безпеки. Дослідження та аналіз SSI створюють і розвивають зти

Сприяння колективній обороні НАТО**:** Безпека та стійкість критичної інфраструктури Посібник НАТО **COE-DAT** Посібник **1**

Керол В. Еванс

Редактор

Кріс Андерсон, Малкольм Бейкер, Рональд Бірс, Саліх Бічакчі, Стів Бібер, Сонгбек Чо, Едріан Двайер, Джеффрі Френч, Девід Харелл, Алессандро Лазарі, Реймонд Мей,

Тереза Сабоніс-Хелф, Дуейн Вернер

Дописувачі

Листопад **2022**

## Зміст

[Передмова **xv**](#_bookmark0)

[Подяки **xix**](#_bookmark1)

[Резюме **xxi**](#_bookmark2)

Розділ **1 -** Розуміння критичної інфраструктури **1**

[Що таке критична інфраструктура? 1](#_bookmark3)

[Чому важлива критична інфраструктура? 5](#_bookmark4)

[У чому різниця між CIP та CISR? 7](#_bookmark5)

[Основні напрямки роботи в плануванні та операціях CISR 8](#_bookmark6)

[Озираючись назад і дивлячись вперед 10](#_bookmark7)

Розділ **2 -** Фізичні загрози критичній інфраструктурі **13**

[Природні загрози 14](#_bookmark8)

[Техногенні загрози 16](#_bookmark9)

[Тематичне дослідження: В Аменасі, Алжир 16](#_bookmark10)

[Внутрішня загроза 18](#_bookmark11)

[РХБЯ загроза 20](#_bookmark12)

[Загроза безпілотників 24](#_bookmark13)

Загрози високоточної ударної зброї 28

[Електромагнітна імпульсна загроза 30](#_bookmark14)

[Аварії та технічні загрози 31](#_bookmark15)

[Більше про що слід подумати: Загрози для портових об'єктів 32](#_bookmark16)

[Зростання витонченості та аутсорсинг фізичних загроз 34](#_bookmark17)

[Зв'язок між загрозою та ризиком 35](#_bookmark18)

[Висновок 38](#_bookmark19)

Розділ **3 -** Кіберзагрози критичній інфраструктурі **41**

[Технічні шари та структури в критичній інфраструктурі 43](#_bookmark20)

[Зв'язок і технічна складність 44](#_bookmark21)

Технологічні шари: Інформаційні технології, операційні технології та промисловий Інтернет речей 47

[Соціальна складність і соціотехнічні структури 50](#_bookmark22)

Пошук прогалин в організації та бізнесі

Рівні управління 52

[Людський капітал, культура та безпека 52](#_bookmark23)

Управління та координація бізнесу

у сфері критичної інфраструктури 54

[Умонастрої та суб'єкти загроз 56](#_bookmark24)

[Різниця в менталітеті: Нападники і захисники 56](#_bookmark25)

[Суб'єкти загроз 58](#_bookmark26)

[Поточні та нові кіберзагрози 60](#_bookmark27)

[Програми-вимагачі 61](#_bookmark28)

[Компрометація ділової електронної пошти (BEC) 66](#_bookmark29)

[Начинка для посвідчення 67](#_bookmark30)

[Атаки на ланцюги поставок 69](#_bookmark31)

[Висновок 72](#_bookmark32)

Розділ **4 -** Гібридні загрози критичній інфраструктурі США і НАТО **75**

[Кібер-кібер-гібридні загрози для критичної інфраструктури 76](#_bookmark33)

Готуємо поле бою: Озброєння критичної інфраструктури Кинути виклик військовій перевазі США і НАТО 80

[Гібридні загрози національній безпеці та боєздатності США](#_bookmark34)

[. 80](#_bookmark34)

Гібридні загрози мобільності США і НАТО

та операції зі сталого розвитку 83

[Гібридні загрози з боку Китайської Народної Республіки 87](#_bookmark35)

[Гібридні загрози оборонно-промисловим базам США та](#_bookmark36) [Європи 92](#_bookmark36)

[Заходи НАТО з усунення вразливості від гібридних загроз 98](#_bookmark37)

Зміст

[Висновок 102](#_bookmark38)

Розділ **5 -** Європейська енергетика та випадок України **103**

[Коротка історія занепокоєння європейською енергетичною](#_bookmark39) [безпекою 105](#_bookmark39)

[Випадок України 111](#_bookmark40)

[Задаючи український контекст: Ранній енергетичний](#_bookmark41) [конфлікт 112](#_bookmark41)

[Російсько-українська війна починається 113](#_bookmark42)

[Кібервійна починається (BlackEnergy та KillDisk) 114](#_bookmark43)

[Кібервійна набирає обертів (CrashOverride) 116](#_bookmark44)

Супутній збиток: Кібератака на українську економіку

(NotPetya) 118

[Атрибуція еволюціонує 120](#_bookmark45)

Вчимося в України: Покращення захисту інфраструктури 122

[Покращуємо Україну: Вразливі місця 125](#_bookmark46)

[Кібер-вразливості 125](#_bookmark47)

[Ядерні вразливості 126](#_bookmark48)

[Improving Ukraine: Допомога 127](#_bookmark49)

[Ключова вразливість зберігається 130](#_bookmark50)

[Висновок 132](#_bookmark51)

[Епілог 134](#_bookmark52)

Розділ **6 -** Цивільна авіація **139**

[Розуміння галузі цивільної авіації 140](#_bookmark53)

[Національна та глобальна критична інфраструктура 140](#_bookmark54)

[Нестабільна галузь 141](#_bookmark55)

[Приваблива мішень 141](#_bookmark56)

[Авіаційна галузь залишається вразливою 143](#_bookmark57)

[Авіаційна безпека є жорсткою 145](#_bookmark58)

[Авіаційна безпека є високо передбачуваною 147](#_bookmark59)

Авіаційна безпека часто намагається не відставати

із загрозою 148

[Тематичні дослідження: Реакція АВСЕК та уроки, які можна](#_bookmark60) [винести 148](#_bookmark60)

[Змова з рідинами, що зірвалася, Велика Британія (2006) 148](#_bookmark61)

[Рідинна ділянка: висновки та аналіз 150](#_bookmark62)

[Комплаєнс чи системи авіаційної безпеки, орієнтовані на](#_bookmark63) [загрози? 155](#_bookmark63)

Потреба в удосконаленні заходів фізичної безпеки

у громадських зонах аеропорту 157

[Рекомендації та кращі практики для зменшення вразливості160](#_bookmark64)

[Розробити більш ризик-орієнтовану систему скринінгу](#_bookmark65)

[AVSEC 160](#_bookmark65)

Розробка та впровадження узгоджених визначень загроз до потенціалу противника 161

Використовуйте дані про подорожі пасажирів авіакомпаній для оцінки ризиків

Цілі скринінгу 162

[Інтеграція програм поведінкового виявлення 163](#_bookmark66)

[Розробка та впровадження програм безпеки в аеропортах](#_bookmark67)

[. 163](#_bookmark67)

[Зміцнити периметр аеропорту 165](#_bookmark68)

[Удосконалення регулювання громадських зон аеропорту165](#_bookmark69)

[Уникайте надмірного покладання на показання та](#_bookmark70) [попереджувальні розвіддані 166](#_bookmark70)

[Пріоритет - людський фактор: Підбір та навчання персоналу](#_bookmark71)

[. 166](#_bookmark71)

[Висновок 167](#_bookmark72)

Розділ **7 -** Залізничні перевезення громадського транспорту**169**

[Залізниці є вразливими за своєю суттю 170](#_bookmark73)

[Внутрішня вразливість та стратегічна оцінка ризиків 170](#_bookmark74)

[Ціль вибору чи можливість? 174](#_bookmark75)

[Багатогранна природа залізниць 176](#_bookmark76)

[Складність 176](#_bookmark77)

[Регулювання та політичне керівництво 178](#_bookmark78)

[Поліція та безпека 178](#_bookmark79)

[Медіа-вплив 180](#_bookmark80)

[Ймовірні методи нападу (MoA) в залізничному середовищі 181](#_bookmark81)

[Страх перед тероризмом 181](#_bookmark82)

Зміст

[Приклад 1: Вибух електронної сигарети в лондонському](#_bookmark83) [метро (2014) 181](#_bookmark83)

[Диверсії та напади на лінію розмежування (ЛР) 182](#_bookmark84)

[Приклад 2: Привид джихадистського дезертира 183](#_bookmark85)

[Приклад 3: Британський досвід атак на ЛЗ 183](#_bookmark86)

[Фізичні напади на людей 184](#_bookmark87)

[Приклад 4: Інцидент у Великій Британії (2018) 185](#_bookmark88)

[Приклад 5: Французький інцидент (2017) 185](#_bookmark89)

[Приклади 6 і 7: німецькі інциденти (2016) 186](#_bookmark90)

[Саморобні вибухові пристрої (СВП) 186](#_bookmark91)

Приклад 8: Низькорівневі/низькотехнологічні СВП, Лондон (2016) 188

[Приклад 9: Експансивна атака, Лондон (2005) 189](#_bookmark92)

[Приклад 10: Експансивна атака, Мадрид (2004) 190](#_bookmark93)

[Швидкодіюча небезпека для здоров'я 191](#_bookmark94)

[Приклад 11: Токійський метрополітен (1995) 191](#_bookmark95)

[Вогнепальна зброя 193](#_bookmark96)

Приклад 12: Напад на потяг Thalys, Бельгія та Франція

(2015) 194

[Соціальна інженерія 194](#_bookmark97)

[Приклад 13: Бінарний тероризм ІРА, Велика Британія.195](#_bookmark98)

[Атаки змішаними методами 196](#_bookmark99)

[Зразок 14: Прилегла до Лондонського мостового вокзалу](#_bookmark100) [територія (2017) 197](#_bookmark100)

[Зразок 15: Центральний вокзал Мумбаї (2008) 197](#_bookmark101)

[Розвиваємо наявні уроки 198](#_bookmark102)

[Висновок 200](#_bookmark103)

Розділ **8 -** Стійкість водного сектору та столиця Вашингтонська справа **203**

Розуміння водного сектору 204

Ризики та загрози для водного сектору 208

Підходи водного сектору до планування стійкості 211

Приклад Вашингтонського регіону 214

Передумови та цілі 214

Оцінка та моделювання ризиків 215

Крок 1: Розробка інвентаризації системи 216

Крок 2: Визначення рівня обслуговування (LOS) 217

Крок 3: Визначення режимів несправностей 218

Крок 4: Визначення ймовірності виникнення (LOO) 219

Крок 5: Визначення наслідків виникнення (COO)

Щоб відповідати рівню сервісу 220

Крок 6: Визначте та перевірте можливі альтернативи 221

Результати 222

Рекомендації та дії для розгляду 224

Розділ **9 -** Стійкість комунікацій **227**

Огляд сектору комунікацій 228

Критично важливий для національної безпеки та готовності до надзвичайних ситуацій 228

Загальні характеристики сектору 230

Сегменти галузі зв'язку 231

Загрози для комунікацій 233

Стихійні лиха 233

Фізичні напади 234

Кібератаки 235

Тематичні дослідження 235

Фізичний напад: Вибух центрального офісу,

Нешвілл, США 236

Фізична аварія та напад: Єгипетські перебої з підводними кабелями

(2008 та 2013) 238

Стихійне лихо: сезон ураганів у США 2017 року 241

Кібератака на системи зв'язку: TV5 Monde 243

Розподілена відмова в обслуговуванні (DDoS): Ботнет Mirai

. 245

Висновок 247

Координація та розбудова відносин у відкритому небі 247

Ідентифікація ризиків та відповідні стратегії пом'якшення

. 248

Інструменти забезпечення стійкості сектору зв'язку 249

Розділ **10 -** Порівняння політичних систем**: CISR** у Сполучених Штатах Америки

та Європейський Союз **253**

Рамкова система CISR США 254

Чим керується політика США у сфері СІСР? 255

Впровадження надійної системи управління ризиками 259

Новий підхід: Управління міжгалузевими ризиками

до об'єктів критичної інфраструктури 261

Хто відповідає за зусилля у сфері СІСР? 261

Ефективна CISR: побудована на співпраці та обміні інформацією 265

Рухаючись вперед: Забезпечення довгострокового успіху СІСР 267

Рамки політики ЄС у сфері СІСР 269

2004: Ембріональна стадія, мотивована боротьбою з тероризмом 272

2005: Від боротьби з тероризмом до захисту від усіх загроз Підхід 276

2006: ЄС офіційно створює EPCIP 278

2008: Ідентифікація, позначення та захист ІВК 279

2013: EPCIP 2.0 - новий підхід 282

2016: Директива про мережеву та інформаційну безпеку .284

2020: Пропозиція щодо Директиви про стійкість критично важливих об'єктів 286

Майбутнє ЄС: Постійне вдосконалення та адаптація

до нових загроз 288

Розділ **11 -** Обмін інформацією та розвідданими **291**

Основоположні концепції обміну інформацією 292

Партнерства з доданою вартістю 292

Важливість довірливих відносин 293

Багатовекторний обмін 294

Своєчасна інформація для тих, хто може діяти 295

Несприятливі умови для обміну інформацією 296

Підкатегорії обміну інформацією 297

Кібербезпека 297

Фізична безпека 298

Аналіз та зменшення ризиків 298

Режими та програми обміну інформацією 299

Тематичні дослідження: Обмін інформацією в дії 304

Робоча група з кібер-здоров'я: Обмін інформацією між державним та приватним секторами 304

Якщо ти щось бачиш, скажи щось® 306

Атака на Капітолій США: Провал в обміні інформацією? 307

Національна дорадча система з питань протидії тероризму

. 309

Національний рейтинг оцінювання спеціальних подій та спеціальних заходів з питань безпеки 311

Підсумки та дії для розгляду 312

Розділ **12 -** Моделювання та аналіз взаємозалежності критичної інфраструктури**:** Вдосконалення стратегій управління відмовостійкістю **315**

Ризик, стійкість та взаємозалежності 317

Таксономії та концепції взаємозалежності критичної інфраструктури 320

Моделювання критичної інфраструктури 326

Структура аналізу взаємозалежності критичної інфраструктури

. 330

Визначення потреб ключових стейкхолдерів 330

Ідентифікація основних активів та систем 331

Зміст

Збір даних 331

Аналіз інфраструктури 332

Визначення стратегій стійкості 332

Операціоналізація взаємозалежностей критичної інфраструктури 333

Висновок 334

Розділ **13 -** Оцінка та управління ризиками для безпеки **337**

Визначення управління ризиками безпеки 338

Системи управління ризиками 339

Національні програми з управління ризиками 341

Управління ризиками безпеки 344

Будуємо знизу догори 346

Формування спільного розуміння ризиків 349

Необхідні характеристики якісних програм управління ризиками 351

Прозорість 351

Інформування про ризики 352

Управління ризиками 353

Розділ **14 -** Посилення кібербезпеки промислових систем управління **355**

Огляд промислових систем керування (ПСК) 357

Проблеми безпеки в ICS 360

Уразливості в компонентах ІКС 361

Компоненти ІКС, що піддаються впливу Інтернету 361

Зв'язок з бізнес-системами 363

Застарілі компоненти 363

Віддалений доступ до мереж управління 363

Небезпечна природа протоколів ICS 363

Основні кіберінциденти 364

Stuxnet (2010) 364

BlackEnergy (2011) 364

Havex (2013) 365

Німецький сталеливарний завод (2014) 365

Відключення електроенергії в Україні (2015) 366

Атомна електростанція RWE, Німеччина (2016) 366

CrashOverride (2016) 367

ТРИТОН (2017) 367

Водоочисна станція, США (2021) 368

Колоніальний трубопровід (2021) 368

Рекомендації з безпеки для ICS 369

Основні практики кібергігієни 369

Основні заходи кібербезпеки для ІКС 370

Управління ризиками для кібербезпеки ІКС 373

Методологія оцінки ризиків для ІКС 375

Підхід до детальної оцінки ризиків 377

Сценарний підхід до визначення базового рівня безпеки378

Захист від кібератак: Погляд у майбутнє 379

Зусилля на національному рівні для CISR 380

Зусилля на міжнародному рівні для CISR 382

Висновок 384

Розділ **15 -** Кризовий менеджмент та реагування **387**

Критична інфраструктура 388

Чому управління кризами та реагування на них є важливим?

. 387

Інциденти, надзвичайні ситуації та кризи: У чому різниця? 390

Розвиваємо спроможність до кризового управління 395

Передбачати та оцінювати 397

Приготуйтеся 398

Реагування та відновлення 399

Команда антикризового менеджменту та лідерство 400

Зміст

Тренінги, навчання та уроки з кризових ситуацій 400

НАТО і врегулювання кризових ситуацій 402

Розвиток антикризового управління та стійкості 402

Підсумки та висновки 404

Про дописувачів 407

## Передмова

Центр передового досвіду питань захисту від тероризму (COE-DAT) надає особам, які приймають рішення, всебічне розуміння тероризму і боротьби з ним з метою трансформації Організації Північноатлантичного договору (НАТО) і країн, що становлять інтерес, для протистояння майбутнім викликам безпеці. Ця трансформація закладена в трьох задекларованих основних завданнях НАТО: колективна оборона, врегулювання криз і безпека на основі співробітництва. COE- DAT визнає, що боротьба з тероризмом є надзвичайно широким викликом безпеці. COE-DAT також визнає, що збройні сили самі по собі не зможуть перемогти тероризм, і що збройні сили не повинні бути провідною силою в боротьбі проти тероризму. Тероризм виникає на ґрунті місцевих невдоволень і тому вимагає загальнодержавного і загальносуспільного підходу, який включає стратегічну співпрацю і колективні дії держав, громадянського суспільства і міжнародного співтовариства.

Як аналітичний центр стратегічного рівня з розвитку діяльності Альянсу із захисту від тероризму, який не входить до офіційної командної структури НАТО, COE-DAT підтримує довгострокову військову трансформацію НАТО, передбачаючи і готуючись до неоднозначного, складного і швидко мінливого майбутнього середовища безпеки. COE-DAT має можливість взаємодіяти з університетами, аналітичними центрами, дослідниками, міжнародними організаціями і глобальними партнерами з метою забезпечення критичного осмислення чутливої за своєю суттю теми боротьби проти тероризму.

Цей проєкт розпочався в середині 2019 року в рамках процесу аналізу наслідків шостої ітерації курсу COE-DAT "Захист критичної інфраструктури від терористичних атак" (CIPATA), який проводився COE-DAT. Рекомендації щодо можливих шляхів трансформації курсу CIPATA задля кращого служіння НАТО і країнам-партнерам дали поштовх низці подій, які зрештою призвели до написання цієї книги. Однією з найважливіших подій стало встановлення офіційного партнерства між Інститутом стратегічних досліджень Військового коледжу армії США (USAWC SSI) і NATO COE-DAT.

USAWC SSI є провідним аналітичним центром стратегічного рівня Армії США, завданням якого є проведення незалежних міждисциплінарних досліджень та аналізу з питань міжнародної безпеки, геостратегії та інших тем для Міністерства оборони США, а також для ширшого кола фахівців з питань національної безпеки та міжвідомчого співробітництва. Це партнерство дозволяє нашим двом організаціям оперативно співпрацювати і взаємодіяти, щоб забезпечити дослідження, аналіз та освітня підтримка з питань безпеки на підтримку НАТО, її членів та країн-партнерів.

Ми визнали, що нові виклики безпековому середовищу ХХІ століття впливають на те, як країни повинні будувати свою концепцію захисту критичної інфраструктури. Дійсно, захист національної критичної інфраструктури перейшов до підходу, що базується на аналізі ризиків і спрямований на розвиток безпеки та стійкості, що зумовило фокус на безпеці та стійкості критичної інфраструктури (CISR).

Члени НАТО розуміють постійну трансформацію захисту критично важливої інфраструктури, тому що стійкість є однією з семи ключових компетенцій НАТО. Хоча CISR - це передусім індивідуальна відповідальність кожного члена Альянсу, захист ключових об'єктів глобальної критично важливої інфраструктури є питанням і викликом стратегічного рівня. Зважаючи на те, що глобальна критична інфраструктура - така як глобальні транспортні, фінансові і телекомунікаційні мережі, а також ланцюги постачання енергоносіїв і медикаментів - становить загрозу міжнародній безпеці, НАТО, разом з Європейським союзом і ООН, має бути залучена до цього процесу.

Хоча НАТО та інші країни наразі розробляють і/або впроваджують власні стратегічні і оперативні підходи до захисту інфраструктури, необхідний комплексний підхід д о посилення безпеки і стійкості національної і глобальної критичної інфраструктури. Щоб відповісти на цю потребу, COE-DAT та USAWC SSI провели дворічне дослідження, залучивши провідних міжнародних експертів з питань захисту критичної інфраструктури з урядових, академічних та промислових кіл. Кульмінацією цієї дослідницької роботи є цей посібник, і хоча існує багато книг про захист критичної інфраструктури, в НАТО не існує спільної публікації з питань критичної інфраструктури.

Тому метою цього проекту є заповнити цю прогалину, підійшовши до теми з військової точки зору і зібравши найкращі практики у сфері КІСБ. У книзі спочатку дається визначення КІСР і численних загроз для неї, наводяться приклади з критичної інфраструктури і, нарешті, надаються інструменти, які країни можуть використати для зміцнення політики і практики КІСР.

Зважаючи на успіх, енергію та зацікавленість, отримані під час написання цієї першої книги, наприкінці 2021 р. у співпраці з Інститутом безпекових досліджень СКУ було розпочато роботу над другою книгою - продовженням, яка вийшла друком наприкінці 2021 р. У той час, як перша книга закладає основу, друга книга буде присвячена Статті 3, що охоплює спроможність і можливості для забезпечення оборонної (військової) та цивільної готовності і стійкості. Мета другого тому - пов'язати зусилля СІСР із сімома цілями НАТО базові вимоги. Обидва томи, кожен окремо і разом, мають стати для членів і партнерів Альянсу ресурсом для розвитку і вдосконалення їхніх зусиль у сфері РМЗС, але вони також можуть бути використані як навчальний посібник.

COE-DAT у співпраці з СБІ СКУ пропонує цю публікацію спільноті НАТО, країнам-партнерам, іншим країнам, що становлять інтерес, та науковим колам з метою поширення "передового досвіду" у глобальній боротьбі з тероризмом. Стратегічні відносини між С Б І СКУ і NATO COE-DAT призвели до того, що ця книга стала реальністю.

Деніел В. Стоун Полковник, ВПС США

Заступник директора

COE-DAT січень 2022

## 

## Подяки

Ця книга була б неможливою без зусиль Інституту стратегічних досліджень Військового коледжу армії США (USAWC SSI), а також моїх співробітників у Центрі передового досвіду з питань захисту від тероризму (COE-DAT).

Я хочу подякувати авторам: Крісу Андерсону, Малкольму Бейкеру, Рональду Бірсу, Саліху Бічакчі, Стіву Біберу, Сонгбеку Чо, Едріану Двайеру, Керол В. Еванс, Джеффрі Френчу, Девіду Харелу, Алессандро Лазарі, Терезі Сабоніс-Хелф і Дуейну Вернеру. Без вашого цінного досвіду та розуміння практичних рішень щодо протидії тероризму в контексті безпеки та стійкості критичної інфраструктури цей проект не був би можливим. Я особливо хочу подякувати Рональду Бірсу, Керол Еванс, Майклу Лоудеру і Джеффрі Френчу, які надали поштовх і початкове натхнення для розробки цієї книги.

COE-DAT вдячний за наукову співпрацю з Інститутом соціальних досліджень СКУ під керівництвом д-ра Керол Еванс, яка забезпечила концептуальну основу, академічну точність та нагляд за цією роботою. Велика подяка д-ру Сарі Ломанн за критичні рецензії та важливі внески, які зробили книгу більш стислою та всебічною. Я також хочу подякувати підполковнику Джеффрі Ван Сіклу за його невтомні зусилля з редагування, щоб привести розділи книги до вчасного, відшліфованого кінцевого стану, та за його допомогу в проведенні серії авторських семінарів. Велика подяка видавництву USAWC Press за підтримку у виданні цієї книги .

Я у великому боргу перед членами мого штабу: полковнику Деніелу В. Стоуну, полковнику Аттілі Чурго, капітану Савашу Айдогду, полковнику Павліну Райнову, полковнику Йоану Прібеку, підполковнику Уве Бергеру, майору Яну Макдональду, майору Майклу Паскуале, майору Джеймсу Каделу і майору Берту Венемі. Дякуємо вам за безмежне терпіння, невтомну працю, критичні зауваження та пристрасть до написання цієї книги. Особлива подяка пані Селві Кахраман, адже без її технічних навичок ми б ніколи не змогли координувати цей проект з членами нашої команди по всьому світу.



Огужан Пехліван, доктор філософії, полковник (TUR A), директор COE-DAT

## 

## Виконавчий директор

## Резюме

У 2014 році Центр передового досвіду НАТО з питань захисту від тероризму (COE-DAT) започаткував перший курс "Захист критичної інфраструктури від терористичних атак (CIPTA)". Оскільки курс CIPTA викликав підвищену відвідуваність і зацікавленість, основна команда лекторів відчула потребу в оновленні курсу з критичної інфраструктури (КІ), беручи до уваги зміщення акценту з "захисту" активів КІ на "безпеку і стійкість". Академічним колам, фахівцям з управління надзвичайними ситуаціями і промисловим практикам бракувало посібника, в якому були б використані колективні знання і досвід основної групи викладачів, посібника, який міг би слугувати для навчання урядових лідерів, власників і операторів об'єктів критичної інфраструктури в державному і приватному секторах, науковців і політиків в НАТО і країнах-партнерах. *Сприяння колективній обороні НАТО: Безпека і стійкість критичної інфраструктури"* є кульмінацією таких зусиль, першим великим спільним дослідницьким проектом в рамках Меморандуму про взаєморозуміння між Інститутом стратегічних досліджень Військового коледжу армії США (SSI) і NATO COE-DAT.

Дослідницький проєкт розпочався у жовтні 2020 року з серії з чотирьох воркшопів, організованих SSI. Наприкінці січня 2022 року було завершено роботу над чернетками розділів книги. Дослідницька група не могла собі уявити російське вторгнення в Україну в лютому цього року. Російська окупація Запорізької атомної електростанції, послідовні ракетні удари по об'єктах генерації та розподілу електроенергії в Україні, залізничному транспорту та кібератаки майже на всі сектори критично важливої інфраструктури країни стали надбанням світової громадськості. Використання Росією своїх газових поставок як засобу економічної війни проти Європи, покликаного підірвати єдність НАТО і підтримку України, є ще одним своєчасним прикладом того, чому вороги, національні держави і терористи однаково обирають об'єкти критичної інфраструктури своєю мішенню. Звідси випливає необхідність партнерства між державним і приватним секторами для захисту цієї інфраструктури і розбудови стійкості, необхідної для забезпечення її життєдіяльності в разі нападу. Україна також наголошує на необхідності розуміння союзниками по НАТО вразливих місць в інфраструктурі приймаючої країни, які можуть підірвати колективну оборону, і приділення більшої уваги усуненню і пом'якшенню цих проблем.

Концептуальна основа цього посібника охоплює ключові аспекти, про які користувачі повинні мати базові знання. Що таке критична інфраструктура і чому вона важлива для НАТО і безпеки окремої країни? Загрози і напади на КІ можуть виникати з багатьох векторів, від кінетичних атак, що здійснюються переважно терористами, до кібератак з боку терористів, національних держав і та їхніх довірених осіб до гібридних загроз. Серед багатьох секторів критичної інфраструктури є визначені "лінії життя", які є життєво важливими через їхню важливість для добробуту суспільства, безперервності роботи уряду, економічних наслідків та згубного каскадного впливу на інші сектори КІ. Останнім часом у спільноті фахівців-практиків у сфері критичної інфраструктури відбувся зсув акценту з простого "захисту" ключових життєво важливих об'єктів інфраструктури на посилення "безпеки та стійкості" цієї інфраструктури. Які ж інструменти можуть використовувати національні держави, власники та оператори КІ для досягнення цих подвійних цілей?

Щоб забезпечити розуміння цих важливих тем у сфері КІ, SSI та COE-DAT зібрали провідних міжнародних експертів. До складу цієї міждисциплінарної команди увійшли фахівці- практики, американські і європейські політики, представники розвідувального співтовариства, експерти науково-дослідних лабораторій і науковці. *Сприяння колективній обороні НАТО: Безпека і стійкість критичної інфраструктури* складається з трьох основних розділів. Перший розділ складається з чотирьох глав, які зосереджуються на тому, що ми розуміємо під "критичною" інфраструктурою і чому і як вона стала мішенню для атак. Відбулася еволюція від фізичних атак, переважно з боку терористів, до витончених кібератак з боку супротивників і більш складних гібридних засобів.

Розділ 1 "Розуміння критичної інфраструктури" (автор Рон Бірс) створює основу для книги, відповідаючи на наступні питання: Що таке критична інфраструктура? Чому вона важлива? Яка різниця між захистом критичної інфраструктури (ЗКІ) і безпекою і стійкістю критичної інфраструктури (БСІ)? Що включає в себе реалізація політики CISR в країнах-членах Організації Північноатлантичного договору і за його межами? Бірс вважає, що CISR є квінтесенцією суспільного завдання з підтримання національної безпеки, економічної життєздатності, громадського здоров'я і безпеки у світі, наповненому зростаючими рівнями ризику. Для країн-членів НАТО розбудова і зміцнення СІСБ на національному рівні необхідна для захисту суспільств, людей і спільних цінностей, а також для забезпечення фундаменту для надійного стримування колективної оборони.

У розділі 2 "Фізичні загрози критичній інфраструктурі" Малкольм Бейкер, Рональд Бірс і Рей Мей детально описують кінетичні загрози для КІ з боку терористів і наводять корисний приклад нападу філії Аль-Каїди на нафтогазовий об'єкт Аменас в Алжирі в 2013 році. Вони також розглядають природні та інші фізичні загрози інфраструктурі, а також майбутні техногенні загрози, які викликають найбільше занепокоєння у НАТО, в тому числі хімічні, біологічні, радіологічні, ядерні, вибухові (ХБРЯ) пристрої, дрони і безпілотні літальні апарати, високоточну ударну зброю і електромагнітні імпульсні атаки.

У розділі 3 "Кіберзагрози для критичної інфраструктури" Саліх Бічакчі досліджує, як зростають ризики для критичної інфраструктури в кіберпросторі. Він пише, що, хоча пандемія COVID-19 змусила бізнес впроваджувати практики, що дозволяють працювати більш віддалено, вона також надала зловмисникам безпрецедентну можливість протестувати системи кібербезпеки та використати вразливості. Пандемія продемонструвала необхідність надійної та безперервної роботи систем електропостачання, природного газу, нафти, водопостачання та водовідведення, а також телекомунікацій. Його розділ містить огляд технічних рівнів і систем критичної інфраструктури та її потенційних організаційних вразливостей до кібератак, пов'язаних з людськими ресурсами і управлінням. Він висвітлює різні категорії суб'єктів загроз (опортуністичні зловмисники, конкуренти, інсайдерські загрози, сучасні постійні загрози і хактивісти) і завершує огляд нещодавніх основних типів атак, які суб'єкти загроз застосовують для використання вразливостей критично важливої інфраструктури.

Четверта і остання глава першого розділу - "Гібридні загрози критичній інфраструктурі США і НАТО" - написана Керол В. Еванс. Вона аналізує кілька основних векторів гібридних загроз для критичної інфраструктури, які можуть атакувати, підірвати або скомпрометувати здатність США і НАТО вести бойові дії, проектувати сили і забезпечувати життєдіяльність. Перший вектор загрози - це навмисне кіберпроникнення супротивника в енергетичну інфраструктуру, яка підтримує американські об'єкти і бази. Таке проникнення дозволяє супротивникам перешкоджати здатності американських збройних сил розгортати і підтримувати передові бойові сили і техніку. Другий вектор гібридних загроз - це ворожі напади н а логістику США і НАТО, що може погіршити здатність США проектувати свої сили за кордоном, а також знизити мобільність і стійкість НАТО на театрі бойових дій. Третя гібридна загроза пов'язана зі стратегічним проникненням, володінням і контролем Китаю над ключовою інфраструктурою оборонних промислових баз і ланцюгами постачання в Європі через його ініціативу "Один пояс, один шлях" і діяльність з прямого іноземного інвестування. Цей вектор надає можливість підірвати оперативну сумісність і політичну єдність США і НАТО. На завершення розділу д-р Еванс висвітлює заходи США і НАТО, спрямовані на усунення і пом'якшення цих загроз шляхом інвестування в СІСР через розбудову організаційної спроможності, розробку політичної бази і виконання базових вимог до стійкості приймаючої країни.

Другий розділ зосереджений на тому, щоб дати читачам уявлення про найважливіші "життєво важливі" сектори інфраструктури, а саме: енергетику, транспорт (включаючи цивільну авіацію та залізничний транспорт), водопостачання та зв'язок. Провідною в цьому розділі є Глава 5 "Європейська енергетика і приклад України".авторства Терези Сабоніс-Хелф. У своїй статті, написаній до російського вторгнення в Україну в лютому 2022 року, д-р Сабоніс-Хелф стверджує, що потенційні перебої в електропостачанні на Заході стають все більш катастрофічними для урбанізованих районів і все більш привабливими для суб'єктів, які прагнуть дезорганізувати роботу систем. Шляхів для підриву стає більше, оскільки енергетичні системи стають більшими, "розумнішими" і більш пов'язаними на міжнародному рівні. Переплетені відносини між енергетичною безпекою і кібербезпекою вимагають розуміння CISR, яке визнає обидва типи вразливостей. Д-р Сабоніс-Хелф стверджує, що приклад України є повчальним. Досвід України в галузі енергетичної безпеки і кібербезпеки виявляє значні ризики і дає уявлення про зусилля НАТО з посилення цивільної готовності і колективної С І С Р серед членів і партнерів Альянсу і країн- партнерів. Він також ілюструє складнощі, з якими Україна і Європа стикаються сьогодні і стикатимуться в майбутньому.

У розділі 6 "Цивільна авіація" Девід Харелл аналізує сектор авіаційної інфраструктури та загрози, з якими він стикається, зокрема, вибухи літаків і наземні атаки терористів на аеропорти. Для розуміння сектору цивільної авіації, пише він, важливо знати, чому авіаційна галузь є такою важливою , що робить її такою нестабільною і чому вона є такою привабливою мішенню для терористів. Він наводить кілька ключових причин вразливості галузі: її негнучкість, непередбачуваність і труднощі з реагуванням на терористичні загрози, що постійно змінюються. Для ілюстрації цих вразливостей Харелл використовує численні тематичні дослідження, які охоплюють 20 років після терактів 11 вересня. Він також аналізує реакцію авіаційної безпеки на ці терористичні атаки і визначає важливі уроки, які слід засвоїти. На завершення він наводить рекомендації та передовий досвід, які можуть допомогти зменшити вразливість міжнародної цивільної авіації.

Розділ 7 "Залізничні операції масового транзиту" Адріана Дуайєра пояснює вразливість відкритих транспортних мереж, таких як залізничні перевезення, до терористичних атак . Він демонструє методи нападів, які найчастіше використовувались, спираючись на дані тематичних досліджень з Великої Британії, континентальної Європи, США, Японії і Індії. З точки зору НАТО, напади на залізничні мережі в країнах-членах можуть порушити військову логістику, цивільний ланцюг постачання і економічне процвітання загалом. Двайер стверджує, що оцінка стратегічних ризиків є важливим засобом управління різноманітними терористичними загрозами і вразливостями, притаманними масовим залізничним перевезенням.

Розділ 8 "Стійкість водного сектору та приклад Вашингтона", автор Стів Бібер, надає відвертий аналіз того, наскільки крихким може бути постачання цього життєво важливого ресурсу і наскільки інші сектори критично важливої інфраструктури залежать від води. Бібер визначає ризики США та загрози для водного сектору; окреслює ключові кроки у плануванні стійкості; ілюструє виклики та рішення для ініціатив з безпеки та стійкості на прикладі Вашингтона, округ Колумбія; та пропонує рекомендації щодо розвитку безпеки та стійкості водного сектору. Він пояснює, що безпека та стійкість водного сектору є ключовим фактором цивільної готовності країни, а також має військові наслідки. Терористичні загрози водопостачанню або забруднення водних джерел можуть вплинути на здатність країни пересувати і утримувати свої збройні сили, а також проектувати військову міць, коли це необхідно. З точки зору Організації Північноатлантичного договору, загрози водному сектору в одній країні-члені можуть мати хвильові ефекти, які обмежують або зменшують військову мобільність і здатність НАТО до застосування сили на підтримку своїх основних завдань.

Розділ 9 " Стійкість комунікацій" Кріса Андерсона завершує другий розділ посібника, присвячений життєво важливим секторам КІ. Зв'язок є критично важливою основою сучасного світу, а стійкий і надійний зв'язок має фундаментальне значення для національної безпеки і готовності до надзвичайних ситуацій. Він пише, що зв'язок відіграє багато важливих ролей для НАТО, в тому числі в командуванні і управлінні, військових операціях, поширенні розвідувальних даних і сигналів оповіщення, врегулюванні криз і координації, а також у забезпеченні готовності громадян. Андерсон надає глибокий огляд сектору зв'язку і пояснює, яким чином цілісність, доступність або конфіденційність систем зв'язку можуть бути порушені або скомпрометовані. Він показує ризики для сектору зв'язку на прикладі нещодавніх природних, техногенних, кібернетичних та кінетичних інцидентів, які вплинули на системи зв'язку та пов'язану з ними інфраструктуру. Він надає важливі рекомендації щодо підвищення стійкості комунікацій до терористичних атак та інших загроз.

Третій розділ "Сприяння *колективній обороні НАТО: Безпека і стійкість критичної інфраструктури"* надає читачам і користувачам посібника інструменти, необхідні для стримування і пом'якшення наслідків атак на критичну інфраструктуру, атакож засоби розбудови довгострокової безпеки і стійкості інфраструктури приймаючої країни, тим самим сприяючи колективній обороні НАТО. Цей розділ складається з шести глав. Він починається з глави 10, написаної Роном Бірсом і Алессандро Лазарі, які, використовуючи свої відповідні політичні погляди, співпрацювали над "Порівнянням політичних рамок: СІСР у Сполучених Штатах та Європейському Союзі". Політика і практика США та ЄС у сфері CISR є найбільш передовими у світі, і багато країн наслідують моделі США та ЄС. У цьому розділі описано ключові засади та характеристики кожної відповідної політичної системи, причини, через які ці системи виникли, і те, як вони були адаптовані з часом. Мета цього розділу - допомогти членам і партнерам Альянсу і партнерам краще розуміти ці дві політичні рамки CISR, щоб вони могли застосовувати ключові принципи та засади для посилення позицій CISR у своїх країнах.

У Розділі 11 "Обмін інформацією та розвідданими" Кріс Андерсон і Реймонд Мей обговорюють важливу роль обміну інформацією та розвідданими між урядами і державними або приватними власниками/операторами об'єктів критичної інфраструктури. Ця діяльність має важливе значення для успіху будь-яких зусиль у сфері РСБІ в рамках Організації Північноатлантичного договору. Вони пояснюють, що ключові зацікавлені сторони інфраструктури повинні обмінюватися інформацією, щоб зрозуміти комплексні інфраструктурні ризики, щоб потім визначити найбільш ефективні і дієві засоби для пом'якшення цих небезпек. Цей процес передбачає розбудову довіри, спільні і практичні методи комунікації, а також структурований, багатовимірний обмін інформацією. Андерсон і Мей наводять приклади найкращих практик державно-приватних програм обміну інформацією зі Сполучених Штатів. Серед них - Консультативна рада з питань партнерства у сфері критичної інфраструктури при Міністерстві внутрішньої безпеки (DHS CIPAC), програма "Захищена інформація про критичну інфраструктуру" (PCII), Програма обміну кіберінформацією та співробітництва, Об'єднана антитерористична цільова група (JTTF) Федерального бюро розслідувань ( ФБР), Рада Альянсу внутрішньої безпеки (DSAC) та InfraGard. Однією з програм обміну інформацією, спільною для США і Європи, є Центр обміну та аналізу інформації (ISAC), який є організацією, що спеціалізується на обміні інформацією про загрози і вразливі місця в секторі критичної інфраструктури.

Розділ 12 "Моделювання і аналіз взаємозалежності критичної інфраструктури: Посилення стратегій управління стійкістю" Дуейна Вернера надає детальний огляд необхідності для країн-членів і партнерів НАТО розуміти взаємозалежність інфраструктури, оскільки вони діють у взаємодії одна з одною. Катастрофічні події можуть каскадом поширюватись на ці взаємопов'язані системи і перешкоджати здатності операторів критично важливої інфраструктури продовжувати свою діяльність. Моделювання та аналіз цих взаємозалежностей є ключовими компонентами ефективної стратегії управління ризиками і визначення того, де потрібні ресурси для розбудови стійкості. Вернер узагальнює загальні підходи до моделювання і оцінювання критично важливої інфраструктури і пропонує гнучку систему CISR для розробки стратегій забезпечення стійкості. Члени і партнери НАТО можуть використовувати ці рамки для зменшення ризиків, що загрожують критично важливій інфраструктурі, і для посилення стійкості за допомогою міжсекторальної співпраці.

Як НАТО може найкраще управляти і оцінювати ризики для безпеки в умовах, що постійно змінюються, є відправною точкою для розділу 13 Джеффрі Френча, "Оцінка та управління безпековими ризиками". Як він зазначає, організації та громади потребують формальних процесів для визначення, пріоритизації та усунення ризиків. Перспективи управління ризиками полягають у тому, що за умови достатньої одноманітності та послідовності лідери уряду чи приватного сектору можуть приймати кращі рішення завдяки здатності агрегувати ризики на різних рівнях. У його главі глибоко досліджуються концепції оцінки ризиків і управління ризиками, а також розглядається н и з к а окремих систем управління ризиками - Міжнародної організації зі стандартизації (ISO), НАТО, Управління державної звітності США (GAO) і Національного плану захисту інфраструктури США ( NIPP), - які були розроблені або адаптовані для управління ризиками безпеки. Далі Френч демонструє, як державна програма управління ризиками на національному рівні може заохочувати і спрямовувати практику управління ризиками, а також координувати діяльність організацій державного і приватного секторів, задіяних в операціях на об'єктах критичної інфраструктури, з метою створення сприятливого середовища для КІСР.

У той час як у попередньому розділі Бічакчі описує різні кіберзагрози для КІ, Сонгбек Чо надає користувачам цього посібника деякі важливі інструменти кібербезпеки для пом'якшення цих самих загроз. У Розділі 14 "Посилення кібербезпеки промислових систем управління" Чо пропонує короткий огляд характеристик промислових систем управління (ПСУ) і причин, чому вони піддаються кібератакам з точки зору вразливості компонентів, а також поширеної в сучасній критичній інфраструктурі практики експлуатації ПСУ в більш відкритих взаємозв'язках з бізнес-мережами. Він висвітлює ці вразливості на прикладах деяких великих кіберподій, зокрема: Stuxnet (2010), BlackEnergy (2011), відключення електроенергії в Україні (2015), атомна електростанція RWE в Німеччині (2016), TRITON (2017) і Колоніальний трубопровід (2021). У розділі пропонуються найкращі практики та інструменти для зацікавлених сторін, власників та операторів об'єктів критичної інфраструктури для захисту своїх систем, підвищення безпеки та стійкості до кібератак. Чо рекомендує використовувати методології управління ризиками, базові гігієнічні практики і основні заходи кібербезпеки. Хоча НАТО вживає заходів для покращення своєї колективної здатності захищати і реагувати на кібератаки на критично важливу інфраструктуру Альянсу, окремі країни-члени формують першу лінію оборони. Чо пропонує національним урядам встановити обов'язкові вимоги з кібербезпеки для об'єктів критичної інфраструктури - забезпечити дотримання цих вимог власниками і операторами - і надавати консультації з питань безпеки в разі потреби. Він також виступає за створення інституційного механізму співпраці (наприклад, державно-приватної ради з питань безпеки критичної інфраструктури та спільної групи кібернетичного реагування), що дозволить інтегрувати унікальні можливості зацікавлених сторін у сфері КІ на національному рівні.

Малкольм Бейкер представляє останню главу в розділі "Інструменти розбудови СІСР", і вона присвячена "Кризовому менеджменту і реагуванню". Кризове управління є важливим компонентом зобов'язань Альянсу щодо посилення стійкості, оголошених у червні 2021 року в рамках ініціативи "НАТО - 2030". Проте Бейкер запитує, чи нинішня філософія Альянсу з врегулювання криз відповідає основним тенденціям розвитку сучасного кризового менеджменту і ідейного лідерства. Крім того, в контексті зусиль CISR, чи підхід НАТО до врегулювання криз все ще відповідає своєму призначенню - чи його можна вдосконалити? На його думку, для НАТО розуміння врегулювання криз виключно в контексті збройних конфліктів та інших бойових дій вже не є доречним або оптимальним (особливо в світлі різних фізичних, кібернетичних і гібридних загроз, про які йшлося раніше в розділах 2-4). Бейкер рекомендує вдосконалити ефективні заходи СІСР шляхом розробки і впровадження надійних структур і процесів управління кризовими ситуаціями. Ключовими елементами ефективного антикризового управління є раннє попередження, ефективна стратегія, хороша комунікація, лідерство і швидке прийняття рішень. Бейкер пропонує перевірену систему антикризового управління, засновану на Британському інституті стандартів, що використовує поетапний підхід до прогнозування та оцінки, підготовки, реагування та управління відновленням. Насамкінець він аналізує нові досягнення в галузі стійкості і врегулювання криз і пропонує пропозиції щодо того, як НАТО може краще узгодити свою діяльність на підтримку НАТО - 2030.

Д-р Керол В. Еванс Редактор

Директор Інституту стратегічних досліджень та прес-служби Військового коледжу армії США

# - 1 –

# Розуміння критичної інфраструктури

## Рональд Бірс

Цей розділ створює підґрунтя для цієї книги, відповідаючи на наступні питання: Що таке критична інфраструктура? Чому вона важлива? Яка різниця між захистом критичної інфраструктури (ЗКІ) та безпекою і стійкістю критичної інфраструктури (БСІ)? Які ключові терміни визначені в національній політиці CISR? Які основні сфери діяльності або напрямки роботи, пов'язані з реалізацією політики CISR в країнах-членах Організації Північноатлантичного договору та за її межами? Відповіді на ці конкретні питання створюють контекстуальну основу для розуміння того, чому СІСР є найважливішим суспільним завданням з підтримання національної безпеки, економічної життєздатності, громадського здоров'я і безпеки у світі, наповненому зростаючими рівнями ризику. Для країн-членів НАТО розбудова і зміцнення СІСБ на національному рівні необхідна для захисту суспільств, людей і спільних цінностей, а також для забезпечення фундаменту для надійного стримування і оборони і здатності Альянсу виконувати свої основні завдання з колективної оборони, врегулювання криз і безпеки на основі співробітництва.1

### Що таке критична інфраструктура**?**

Хоча не існує стандартного або універсального визначення критичної інфраструктури, багато західних країн визначають цей термін як фізичні та кібернетичні системи та активи, які є життєво важливими для країни. що їхня недієздатність або руйнування матиме виснажливий вплив на фізичну чи економічну безпеку країни, а також на здоров'я та безпеку населення.2 Певнісоціально-економічні види діяльності є життєво важливими для повсякденного економічного функціонування та безпеки націй. Хоча немає єдиної думки щодо того, які сектори вважати критично важливими, більшість країн, що мають затверджену національну політику у сфері КІП або КІСР, визначають деякі або всі сектори, перелічені на рис. 1-1, як критично важливі об'єкти інфраструктури.3 Більшість людей повсякденно стикаються з критичною інфраструктурою як з електроенергією, що використовується в їхніх будинках, водою, яку вони п'ють, транспортом, від якого залежить свобода пересування, і системами, які вони використовують для зв'язку з родиною, друзями і колегами по роботі.4



Рисунок **1-1.** Перелік найчастіше визначених секторів критичної інфраструктури

(Діаграма за даними TSAT)

Щоб проілюструвати взаємозв'язки між секторами критичної інфраструктури, на рисунку 1-2 використано сині та червоні рамки для визначення та розмежування різних секторів.5 Червоні квадратики - транспорт, водопостачання, енергетика та зв'язок - відомі як сектори життєзабезпечення. З огляду на їхню унікальну природу, можна виділити чотири основні характеристики, які відрізняють сектори життєзабезпечення від інших секторів критичної інфраструктури.6 По-перше, сектори життєзабезпечення надають необхідні послуги і товари які підтримують більшість домогосподарств, підприємств, громад та рівнів влади. По-друге, вони надають послуги, які є звичними у повсякденному житті, але переривання їх надання може призвести до виникнення небезпечних для життя ситуацій. По- третє, сектори життєзабезпечення включають складні фізичні та електронні мережі, які пов'язані між собою всередині та між кількома секторами. І, нарешті, збій в одному секторі життєзабезпечення може вплинути на інші сектори або вивести їх з ладу, створюючи каскадні або ескалаційні збої. Сині рамки вздовж зовнішнього кільця ілюструють інші сектори критичної інфраструктури, які зазвичай залежать від секторів життєзабезпечення для безперервної роботи.

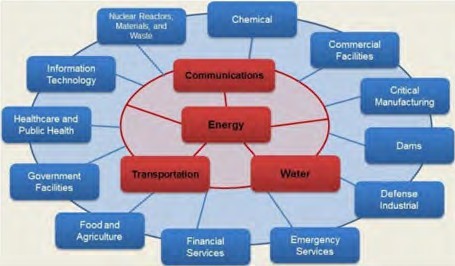


Рисунок **1-2.** Взаємозв**'**язки між секторами критичної інфраструктури

(Діаграма Міністерства внутрішньої безпеки США)

У попередньому розділі було описано, як більшість країн визначають критично важливу інфраструктуру, але як її визначає НАТО? В НАТО Командування об'єднаних збройних сил (ОЗС) використовує декілька визначень для ідентифікації і розуміння типів інфраструктури, наявної в певній зоні відповідальності. ОЗС визначає критичну інфраструктуру як "національні інфраструктурні активи, об'єкти, системи, мережі і процеси, які підтримують військове, економічне, політичне і/або соціальне життя, від яких залежить країна і/або НАТО".7 ACO також описує три підкатегорії критичної інфраструктури на основ і відповідного рівня впливу на національні служби і/або операції НАТО, як показано на наступній сторінці.8

* 1. Критична національна інфраструктура: Активи, об'єкти, системи та мережі, визначені територіальною державою, що приймає, які є невід'ємною частиною безперервного надання та цілісності основних послуг, на які покладається нація, руйнування або компрометація яких може призвести до серйозних військових, економічних, політичних або соціальних наслідків для нації.
  2. Життєво важлива інфраструктура місії: Активи, об'єкти, системи і мережі в районі проведення спільних операцій, на які покладаються сили НАТО/країни, що надають війська, для забезпечення польових сил і засобів, знищення або порушення роботи яких окремо створює вирішальні перешкоди для місії НАТО.
     1. Ключова інфраструктура: Активи, об'єкти, системи і мережі в районі проведення спільних операцій, на які покладається країна, що приймає, або сили НАТО/країни, що надає війська, для забезпечення польових сил і засобів, руйнування або порушення яких, окремо або разом, створює значні перешкоди для країни, що приймає , або місії НАТО.

Важливим питанням, яке має розглянути НАТО, є те, якою мірою її загальна готовність до виконання місій залежить від гарантованої доступності критично важливої інфраструктури, більша частина якої належить компаніям приватного сектора в різних країнах-членах Альянсу. Сьогодні, і вже деякий час, відповідь на це питання полягає в тому, що НАТО значною мірою залежить від такої гарантованої доступності критично важливої інфраструктури. Під час великих операцій або навчань, наприклад, приблизно 90 відсотків військових перевезень покладаються на цивільні кораблі, залізниці і літаки. Про те, як залежність США і НАТО від гарантованого доступу до глобальної судноплавної інфраструктури створює загрози для розгортання сил і військової мобільності Альянсу, див. розділ

4. У цьому розділі ми розглянули, як західні країни визначають критичну інфраструктуру і чому вони це роблять. Простіше кажучи, без товарів і послуг, які надають ці сектори критичної інфраструктури, наслідки можуть бути катастрофічними для здоров'я і безпеки населення, довкілля, національної безпеки та/або економіки країни. Крім того, оскільки багато таких систем і мереж працюють через кордони, будь-яка загроза або напад на них може мати національні, регіональні і навіть глобальні наслідки. Які ще є причини важливості критичної інфраструктури.

**Чому важлива критична інфраструктура ?**

Сьогодні громадяни багатьох країн вимагають або очікують, що системи критичної інфраструктури і функції, які вони виконують, будуть доступні 24 години на добу. Однак зловмисники проникають і виводять з ладу різні частини критично важливої інфраструктури з незначними наслідками або взагалі без них. Один з таких прикладів стався в травні 2021 року, коли невелика група хакерів здійснила атаку з вимогою викупу на Colonial Pipeline, найбільшу трубопровідну мережу в США для постачання нафтопродуктів. Більш детально про випадок з Colonial Pipeline див. у розділі 14. Компанія Colonial перекрила свої магістральні трубопроводи на п'ять днів, перервавши половину поставок пального до східної частини країни. Стурбовані водії вичерпали запаси на заправках у південно-східних штатах, авіакомпанії перенаправили літаки в аеропорти, де було доступне пальне, трейдери зіткнулися з несподіваною волатильністю цін, а компанії намагалися знайти нові джерела пального.

Атака на нафтопровід "Колоніал Пайплайн" демонструє важливість розбудови стійкості. Події, подібні до цієї, надзвичайно складно, якщо не неможливо, передбачити, але багато чого можна зробити, щоб підготуватися до них. Організаціям потрібно не лише підвищити безпеку своїх систем, але й здатність реагувати на інциденти та швидко відновлювати роботу після збоїв. Ці можливості можуть заздалегідь визначити дії, які необхідно вжити у відповідь на велику деструктивну подію. Організації повинні знати, що робити, розвивати можливості для цього, а потім відпрацьовувати свої дії з реагування на кризові ситуації - і все це заздалегідь , до того, як станеться інцидент.

Докази також свідчать про те, що кібератака на Colonial Pipeline не була особливо складною, але їй вдалося паралізувати значну частину паливного постачання найбільшої економіки світу. Атака на Colonial Pipeline і багато подібних атак до і після неї стали можливими завдяки постійній автоматизації традиційного виробництва і промислових практик, що робить ці сфери більш вразливими, хоча і не обов'язково становить для них пряму загрозу. Акцент четвертої промислової революції на сучасних інтелектуальних технологіях спонукає суспільства до більш інтелектуальних і розумних операційних мереж у таких сферах, як енергетика, водопостачання, управління дорожнім рухом, управління повітряним рухом і оборонні системи, якщо назвати лише деякі з них.

Досягнення в автоматизованих технологіях, таких як датчики, Інтернет речей і засоби захисту кібербезпеки, можуть допомогти тим, хто відповідає за захист критичної інфраструктури, зрозуміти потенційні загрози, провести діагностику, спрогнозувати потенційні зміни в своїх системах і більш ефективно зміцнити безпеку і стійкість цих систем критичної інфраструктури. Разом ці характеристики сучасного середовища загроз є однією з найсерйозніших проблем національної безпеки з часів винайдення атомної бомби, і вони демонструють, чому написання такого посібника, як цей, є необхідним для посилення колективної здатності до реагування на кіберзагрози .

Сьогодні країни намагаються зрозуміти, з якими загрозами вони стикаються - видимими і невидимими - і що вони можуть упустити. Ті, хто відповідає за CISR, постійно беруть участь у процесі визначення того, які загрози повинні бути на першому місці в списку, як слід ранжувати інші, і, враховуючи це ранжування, які ресурси слід виділити на боротьбу з цими загрозами. Які моделі та інструменти корисні для кращого розуміння загроз і наслідків атак на критичну інфраструктуру? Які практики або рішення повинні впроваджувати країни для запобігання, стримування, пом'якшення наслідків, реагування та відновлення після подій, що можуть порушити або зруйнувати критичну інфраструктуру? Які існують прогалини в розвідданих і як зацікавлені сторони повинні їх заповнювати?13

Реальність така, що будь-яка кількість факторів може спричинити порушення або руйнування критичної інфраструктури, включаючи погане проектування, помилки операторів, природні причини (такі як землетруси, удари блискавки, космічна погода і зміна клімату) або навмисні дії людини, такі як крадіжки, підпали, тероризм або злочинні напади. Інші фактори, що підвищують ризик для критичної інфраструктури, включають в себе:

* 1. Погана інфраструктура та відсутність належного контролю за безпекою
  2. Більш широке використання інформаційних та

телекомунікаційних технологій для підтримки, моніторингу та контролю функцій критично важливої інфраструктури

* 1. Зростання населення світу та його перехід із сільської місцевості до міст, що призводить до вичерпання можливостей використання старої інфраструктури
  2. Зростаюча залежність і взаємозалежність між секторами критичної інфраструктури (див. розділ 12 для більш поглибленого аналізу цих взаємозв'язків)
  3. Поглиблення розуміння противником того, що успішна атака на системи критичної інфраструктури може спричинити хаос
  4. Залежність країн від критично важливої інфраструктури, яка частково або повністю знаходиться за межами їхньої юрисдикції і над якою вони мають обмежений контроль або взагалі не мають контролю

У кількох розділах цієї книги більш глибоко розглядаються питання вразливості, загроз і ризиків. Огляд загроз і суб'єктів загроз див. у розділах 2-4. Тим не менш, на цьому етапі корисно поділитися гострим спостереженням, зробленим експертом з інформаційної безпеки Беном Ротке, який стверджував у 2013 році: "Найбільша загроза для критичної інфраструктури - це результат десятиліть незахищеності в поєднанні з неадекватним реагуванням на відомі загрози і вразливості". Спостереження Ротке продовжує переслідувати уряди і компанії, оскільки воно підкреслює нагальну потребу для всіх зацікавлених сторін у сфері критичної інфраструктури сприяти співпраці, координації, взаємодії, комунікації та концентрації зусиль, необхідних для використання досвіду, необхідного для наочного посилення колективних позицій у сфері КІСІ.

У чому різниця між **CIP** та **CISR?**

Людство захищає критичну інфраструктуру з часів винайдення колеса, однак за останні 20 років більшість національних політик і стратегій у сфері критичної інфраструктури на Заході еволюціонували від зосередження виключно на захисті критичної інфраструктури до підвищення її безпеки та стійкості. Цей зсув в першу чергу пов'язаний з тим, що перед зацікавленими сторонами стоїть надскладне завдання захистити всі системи критичної інфраструктури від зростаючої кількості факторів ризику, з якими вони стикаються.

Відповідно до концепції CISR, терміни "*безпека"* і "*стійкість",* безумовно, підтримують ідею захисту, але вони мають специфічні значення. *Безпека* означає зменшення ймовірності успішних атак на критичну інфраструктуру або наслідків природних чи техногенних катастроф шляхом застосування фізичних засобів або оборонних заходів кібербезпеки. *Стійкість -* це здатність критичної інфраструктури протистояти, поглинати, відновлюватися або успішно адаптуватися до мінливих умов. Відмовостійка інфраструктура є надійною, гнучкою, адаптивною, здатною протистояти і швидко відновлюватися після збоїв, навмисних атак, аварій або природних загроз чи інцидентів. З огляду на зростання природних і техногенних загроз і вразливостей, з якими стикаються сучасні суспільства і які викривають обмеженість традиційної оцінки ризиків і зусиль зі зниження ризиків, концепція CISR видається особливо корисною для формування політики, спрямованої на пом'якшення наслідків таких подій, і вказує на життєво важливу потребу країн у розробці та впровадженні всеосяжної стратегії управління ризиками. Аналіз і рекомендації щодо стратегій оцінки та управління ризиками див. у розділі 13.

Перехід від мети захисту до мети підвищення безпеки і стійкості вимагає зміни фокусу освіти і навчання, щоб забезпечити завершення і належне управління основними напрямками роботи CISR.

### Основні напрямки роботи в плануванні **CISR** та операціях

Хоча процес створення, впровадження та підтримки ефективної національної політики у сфері КІСБ є складним у будь-якій країні, існує три основні завдання: оцінка ризиків, підвищення безпеки та посилення стійкості. Процес виконання цих трьох завдань є надзвичайно складним і постійним викликом, оскільки вимагає виконання численних потоків робіт усіма зацікавленими сторонами: численними державними установами, власниками і операторами критичної інфраструктури, науковцями, профільними експертами, міжнародними організаціями і постачальниками технологій. Деякі з основних напрямків роботи включають

* Визначення чітких ролей та обов'язків для всіх зацікавлених сторін
* Ідентифікація та визначення критичності

національної інфраструктури

* Картування залежностей та взаємозалежностей критичної інфраструктури
* Визначення вразливостей критичної інфраструктури
* Використання відповідних підходів до оцінки, аналізу та управління ризиками
* Створення потенціалу для управління кризовими ситуаціями
* Налагодження державно-приватного партнерства між державними та приватними власниками та операторами об'єктів критичної інфраструктури
* Створення та впровадження механізмів співпраці та обміну інформацією між урядом та власниками і операторами об'єктів критичної інфраструктури
* Розробка та реалізація планів забезпечення безперервності діяльності та аварійного відновлення інформаційних технологій
* Забезпечення заходів фізичної та кібербезпеки і стійкості
* Забезпечення цілісності, безпеки та безперервності ланцюгів постачання критичної інфраструктури
* Сприяння місцевому, регіональному, національному та міжнародному співробітництву, співпраці, координації, комунікації та концентрації, необхідних для отримання очевидно ефективних результатів
* Розширення можливостей для розвитку та проведення навчання та тренінгів з питань СІСР
* Впровадження надійної програми тестування, навчання та тренувань для визначення того, наскільки поточна політика, законодавство, плани, процедури, системи та науково-дослідницька діяльність у сфері КІСР відповідають, не відповідають або перевищують встановлені вимоги, стандарти та очікування зацікавлених сторін, які стають дедалі жорсткішими

Успішна реалізація національної політики у сфері КІСР потребує сильних лідерів та першокласних менеджерів. Хоча визначені вище напрямки роботи визначають більшу частину того, що необхідно зробити, ступінь ефективності розробки і реалізації "що" залежить від того, наскільки добре люди, відповідальні за керівництво і управління цими напрямками роботи, сприяють співпраці, кооперації, координації, комунікації і концентрації ( 5С), які є необхідними для побудови і підтримки життєздатної, заснованої на ризиках, політики БІСР. Цей факт неможливо переоцінити. Протягом більш ніж 30 років можливості CIP і CISR зростали і слабшали залежно від того, наскільки добре лідери виконують ці 5С.

### Озираючись назад і дивлячись вперед

Важливо дивитися в майбутнє, але країни - члени НАТО також можуть вчитися на досвіді минулого. Одним з повчальних прикладів з Римської імперії є зв'язок між погіршенням стану величезної римської системи акведуків - безумовно, раннього прикладу критично важливої інфраструктури - і остаточним падінням імперії. У третьому столітті до нашої ери римляни побудували акведуки по всій імперії, щоб подавати воду із зовнішніх джерел до міст і містечок для забезпечення громадських лазень, туалетів, фонтанів і приватних домогосподарств, а також для підтримки гірничодобувної промисловості, млинарства, фермерських господарств і садівництва. Однак, оскільки тогочасна адміністрація поступово занедбала акведуки і не вжила достатніх заходів безпеки та стійкості до низки загроз і вразливостей (включаючи загальний знос, навмисну зміну маршрутів місцевими фермерами, навмисне руйнування або перешкоджання з боку ворогів), багато акведуків перестали функціонувати.

У ХХ столітті загрози для критичної інфраструктури були майже виключно матеріальними, фізичними загрозами, яким можна було протистояти за допомогою матеріальних, фізичних засобів захисту. Такі види матеріальних, фізичних загроз існують і сьогодні - як і стихійні лиха, такі як урагани, ліси і лісові пожежі - і вони можуть завдати серйозної шкоди людям і країнам. Однак у двадцять першому столітті критично важливі об'єкти інфраструктури все більше підключаються до Інтернету. Таке посилення зв'язку викликає глобальне занепокоєння, оскільки значна частина критичної інфраструктури, від якої залежить здоров'я, енергетика і безпека країн, вразлива до кіберзагроз. Зловмисники можуть використовувати віртуальні системи управління для реалізації фізичних загроз або створювати віртуальні загрози для фізичної інфраструктури. Таке поєднання віртуальних і фізичних загроз зростає в геометричній прогресії, особливо зважаючи на те, що віртуальні підключення до фізичної інфраструктури через Інтернет речей стають все більш поширеним явищем. Такі атаки стануть більш поширеними і, ймовірно, будуть більш руйнівними. Окрім продовження інвестування в новітні технології для захисту від цих загроз, сильна позиція CISR мінімізує вплив цих атак і зробить цілі менш цінними з точки зору супротивника.

У 2019 році експерт з питань безпеки П'єр Бурже забив на сполох щодо зростання загроз для критично важливої інфраструктури та необхідності реагувати на них шляхом посилення безпеки та стійкості:

Ми стоїмо на порозі світу, який повністю пов'язаний між собою. Від розумних міст до розумних будівель, з використанням машинного навчання та глибокого навчання ми як ніколи близькі до повної конвергенції. Це також є нашою ахіллесовою п'ятою, яка може призвести до катастрофи, яку ми навіть не можемо собі уявити. Необхідність розуміння цих загроз від найнижчих до найвищих ланок наших організацій має вирішальне значення. Однак часу на освіту стає все менше: або ми її отримаємо, або гра закінчиться.

Від зміни клімату до кібератак, інфраструктурні системи повинні працювати в умовах дедалі більшої невизначеності, коли неможливо уникнути або навіть передбачити всі потрясіння і стреси. Тому важливо, щоб суб'єкти критичної інфраструктури були готові до загроз, які вони можуть передбачити, і були здатні реагувати на несподіванки, щоб надавати основні послуги, від яких залежить суспільство. Як сказав Дональд Рамсфельд, тодішній міністр оборони США:

Є відомі речі, які ми знаємо; є речі, які ми знаємо, що знаємо. Ми також знаємо, що є відомі невідомі; ми знаємо, що є речі, яких ми не знаємо. Але є також невідомі невідомі - ті, про які ми не знаємо, що не знаємо. І якщо поглянути на історію вільних країн, то саме остання категорія, як правило, є найскладнішою.

Невідомі невідомі - це ризики, що виникають у ситуаціях, які є настільки несподіваними, що їх не можна було передбачити. Щоб визначити майбутні загрози для критичної інфраструктури, зацікавлені сторони повинні спробувати їх передбачити. Очевидно, що найближчі роки будуть позначені турбулентністю, підживлюваною нетрадиційними конфліктами, що загрожують стихійними лихами та техногенними катастрофами, а також ускладнюється проблемами, що виникають у зв'язку зі зростаючою складністю та залежністю суспільства від критичної інфраструктури.

Як підкреслюється в усіх розділах цього посібника, посилення КІСІ є важливим для здатності НАТО функціонувати в умовах кризового врегулювання, колективної оборони і/або зовнішніх операцій. Захист систем критичної інфраструктури країни і підвищення їх стійкості до широкого спектра нинішніх, нових і майбутніх ризиків є складним і постійним завданням. Насправді, це одна з найскладніших речей, які може зробити країна. Проте нездатність досягти цілей і завдань CISR зменшить спроможність НАТО до виконання місій, а також негативно вплине на колективні суспільства країн-членів, оскільки критична інфраструктура є основою, від якої залежать життєво важливі суспільні і економічні функції. Тому одним з найважливіших суспільних завдань, необхідних для підтримання національної безпеки, економічної життєздатності, громадського здоров'я і безпеки у світі, сповненому ризиків, буде подальший розвиток, створення і підтримання ефективних національних сил і засобів захисту критичної інфраструктури (CISR). Спільна робота та обмін набутим досвідом, передовою практикою, тематичними дослідженнями, методами, інструментами, підходами та досвідом, а також відкриття невідомого сприятимуть розвитку та зміцненню місцевих, регіональних, національних та глобальних КІСР сьогодні та в майбутньому.

# - 2 –

## Фізичні загрози критичній інфраструктурі

Малкольм Бейкер, Рональд Бірс та Рей Мей

Атаки на Сполучені Штати 11 вересня (9/11) продемонстрували вразливість до фізичних і кінетичних загроз з боку терористів. Ці атаки також підтвердили, наскільки рішучими, терплячими і витонченими стали терористи як у плануванні, так і у виконанні своїх операцій. Понад два десятиліття потому наслідки незахищеності критичної інфраструктури залишаються серйозними.

Базова природа вільних суспільств значно полегшує операції і тактику, що застосовуються терористами, конкуруючими державами та іншими зловмисниками, водночас обмежуючи здатність цих суспільств передбачати, стримувати, пом'якшувати наслідки, реагувати на них і відновлюватись після зловмисних атак на них. Тому для країн-членів Організації Північноатлантичного договору (НАТО) вкрай важливо розробити і підтримувати ефективну політику, плани і процедури безпеки і стійкості критичної інфраструктури (CISR), щоб зменшити ризики для критичної інфраструктури, пов'язані з постійно зростаючим переліком реальних загроз, незалежно від того, чи є вони фізичними, кібернетичними або гібридними за своєю природою. Майже щодня суб'єкти загроз здійснюють кібератаки на елементи критичної інфраструктури. Багато з цих кібератак привертають велику суспільну і політичну увагу, оскільки завдають шкоди країнам - членам НАТО і країнам- партнерам, але фізичні напади на критично важливу інфраструктуру також залишаються небезпечними загрозами, що спонукає до планування і зусиль в галузі CISR по обидва боки Атлантичного океану.

Більшість людей мають певний особистий досвід зіткнення з вірусом COVID-19 і були свідками того, як пандемія, біологічна подія, спричинила руйнівні наслідки.

У Сполучених Штатах, країнах-членах НАТО і більшості країн світу стихійні лиха спричинили хаос і завдали шкоди багатьом секторам критично важливої інфраструктури. На жаль, багато людей також на власному досвіді пережили ту чи іншу форму стихійного лиха, яка зрештою завдає мільярдні збитки, негативно впливає на здоров'я і безпеку населення і , можливо, навіть калічить або руйнує певні об'єкти критично важливої інфраструктури. Багато читачів цієї книги також усвідомлюють шкоду і руйнування об'єктів критичної інфраструктури, що сталися внаслідок терактів 11 вересня. Менш відома, але все ж руйнівна подія сталася у 2016 році, коли мавпа вивела з ладу всю енергосистему Кенії, впавши на трансформатор на гідроелектростанції Гітау.1 Такий неймовірний сценарій - разом з прикладами терористичних атак, стихійних лих і біологічних подій - ілюструє, що сучасне середовище ризиків є дуже складним і невизначеним, оскільки загрози, вразливості та наслідки змінилися з початку двадцять першого століття.

У цьому розділі надається загальний огляд існуючих і нових фізичних загроз для критичної інфраструктури у простій і зрозумілій формі, що спонукає до роздумів. Розділ складається з трьох основних розділів. Кожен розділ представляє одну з трьох основних категорій фізичних загроз критичній інфраструктурі:

(1**) природні загрози , (2) зловмисні загрози та (3) випадкові або технічні загрози**. У кожному з цих розділів буде розглянуто природу загроз критичній інфраструктурі, наведено кілька прикладів для кожного типу загроз, а потім проаналізовано відповідні тематичні дослідження, щоб визначити ключові висновки та навчальні моменти, на які слід звернути увагу. У цьому розділі пріоритет надається антропогенним загрозам, який є найдовшим розділом і містить численні приклади та тематичні дослідження різних типів загроз у цій категорії. Розділ завершується оглядом міркувань для членів і партнерів Альянсу і партнерів щодо вдосконалення їхньої політики і практик у сфері КІСР задля протидії викликам, пов'язаним з фізичними загрозами для критичної інфраструктури.

### Природні загрози

Природні явища та катастрофи відбуваються щодня по всьому світу. До цієї категорії належать такі різноманітні природні загрози, як наслідки зміни клімату, землетруси, цунамі, зсуви ґрунту, виверження вулканів, лісові пожежі, урагани, паводки, посухи, а за певних обставин - навіть час і тварини. Природні загрози становлять значний ризик для критичної інфраструктури, як це наочно демонструють наступні приклади. У 1993 році сильна повінь на річці Міссурі поставила під загрозу безпеку атомної електростанції Купер у штаті Небраска. Землетрус у Кобе в Японії в 1995 році зруйнував критично важливі об'єкти транспортної, морської та хімічної інфраструктури. У 1998 році торнадо зі швидкістю вітру від 113 до 156 миль на годину обрушилися на атомну електростанцію Девіс-Бесс в Огайо, і хоча цей конкретний інцидент не мав довгострокових наслідків, він вивів з ладу кілька критично важливих систем, що зробило станцію більш вразливою до катастроф. Масштабні пошкодження енергетичної та хімічної інфраструктури, спричинені ураганами Катріна і Ріта в США у 2005 році, ілюструють загрозу, яку становлять екстремальні погодні умови. Події, пов'язані з екстремальними погодними умовами, зокрема, блискавки і шторми, історично становили найбільшу загрозу для критично важливої енергетичної інфраструктури.

Кліматичні загрози, такі як екстремальні погодні явища, підвищення температури, посухи, лісові пожежі, шторми, підвищення рівня моря, деградація ґрунтів і закислення океанів, посилюються і загрожують інфраструктурі, здоров'ю, водній і продовольчій безпеці. Незворотна шкода екосистемам і середовищам існування - деградація повітря, ґрунту, води і морського забруднення - підірве економічні вигоди, які вони забезпечують. Екстремальні погодні явища, багато з яких погіршуються прискоренням підвищення рівня моря, особливо вплинуть на міські прибережні райони в Південній Азії, Південно-Східній Азії та Західній півкулі. Пошкодження комунікаційної, енергетичної і транспортної інфраструктури може вплинути на військові бази, розташовані в низинних районах, спричинити економічні витрати, а також призвести до переміщення людей і людських жертв.2 Навіть події, які здаються малоймовірними (наприклад, падіння метеорита на велике місто і пошкодження багатьох критично важливих секторів інфраструктури), знаходяться у сфері можливого.

Частота і вартість стихійних лих зростають, і вони часто становлять реальну загрозу для конкретних елементів критичної інфраструктури, розташованих у зоні ураження стихійного лиха. Через взаємопов'язаність об'єктів критичної інфраструктури іноді стихійне лихо в одному регіоні країни може спричинити каскадні наслідки для кількох секторів критичної інфраструктури, деякі з яких знаходяться на іншому кінці країни або навіть у сусідній державі. Суть полягає в тому, що будь-яка методологія оцінки загроз повинна враховувати ймовірність пошкодження або руйнування об'єктів критичної інфраструктури внаслідок природних загроз. Це дозволяє як державним, так і приватним власникам та операторам об'єктів критичної інфраструктури краще розуміти та управляти фізичними ризиками, що загрожують об'єктам критичної інфраструктури.

директора Національної розвідки, 29 січня 2019 року), 23, [https://www.dni.gov/files/ODNI/documents/2019-ATA](https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf)

### Зловмисні Загрози

*Зловмисні сили* - це термін, що використовується для опису людських суб'єктів, які загрожують фізичним нападом, порушенням або знищенням нормальної роботи об'єктів критичної інфраструктури. До таких сил належать іноземні та національні терористичні організації, елементи, що діють від імені конкуруючої іноземної держави, а також окремі особи зі зловмисними намірами щодо уряду або конкретної організації, які мають "надможливості" завдяки інформаційним, комунікаційним та іншим технологічним досягненням.3 Ця категорія загроз включає не лише війну, тероризм і гібридну війну, але й масові заворушення, фінансові злочини, економічне шпигунство, а також можливе використання хімічних, біологічних, радіологічних, ядерних і вибухових матеріалів (ХБРЯ) для завдання великої шкоди. Традиційні акти саботажу і навмисне втручання, модифікація або маніпулювання фізичними системами і процесами - наприклад, фізичне переміщення залізничних стрілочних переводів, відкриття і закриття енергопроводів, придушення сигналів або тривог на критично важливих вузлах енергетичної і транспортної інфраструктури - також залишаються загрозою для критично важливої інфраструктури. З огляду на таке широке розмаїття суб'єктів і методів атак, важливо збалансувати ймовірність і наслідки конкретних векторів загроз. Див. також важливість правдоподібності, описану в розділі 7. У цьому розділі ми розглянемо декілька типів антропогенних загроз, які є найбільш серйозними і викликають найбільше занепокоєння у НАТО, і проілюструємо ключові концепції на конкретних прикладах, починаючи з атаки на нафтогазовий об'єкт в Ін-Аменас, Алжир.

##### 

##### Тематичне дослідження**:** В Аменасі**,** Алжир

16 січня 2013 року близько 32 добре озброєних терористів з угрупування Аль-Каїди напали на нафтогазовий об'єкт Ін Аменас в Алжирі.4 Безпрецедентний, спланований і скоординований напад, що тривав чотири дні, став однією з найбільших терористичних атак, коли-небудь здійснених на нафтогазові об'єкти. Один з найбільших газових проектів в Алжирі, об'єкт в Ін- Аменас експлуатується як спільне підприємство між Statoil, British Petroleum і Sonatrach, національною нафтовою компанією Алжиру. Величезний об'єкт займає понад 2700 квадратних кілометрів - територію, що майже дорівнює розміру Люксембургу - і розташований приблизно за 1300 кілометрів від столиці Алжиру Алжиру і приблизно за 50 кілометрів на захід від Лівійський кордон. З огляду на його стратегічне значення, для захисту нафтогазового об'єкту було створено багаторівневу систему безпеки.

Народна національна армія і жандармерія алжирських збройних сил забезпечували зовнішній рівень безпеки об'єкта, працюючи окремо і підтримуючи один одного. Як і в більшості інших країн, уряд відповідав за захист об'єкта від терористичних атак, включаючи запобігання, збір розвідувальних даних і прикордонний контроль, в тому числі вздовж алжирсько- лівійського кордону і в пустельній зоні навколо об'єкта. Фактично, алжирський уряд створив навколо "Ін Аменас" мілітаризовану зону, де армія відповідає за безпеку ширшої пустельної зони, а жандарми забезпечують безпеку в безпосередній близькості від об'єкту. Що стосується внутрішнього периметру, то компанії Statoil, British Petroleum і Sonatrach відповідали за внутрішню безпеку в In Amenas і надали для цього неозброєну цивільну охорону. Внутрішня охорона забезпечувала контроль доступу та інші захисні заходи безпеки, а також навчання і планування на випадок надзвичайних ситуацій для захисту людей і майна об'єкта. Спочатку терористи напали на автобус, що перевозив робітників на об'єкт, а потім майже одночасно атакували житловий комплекс для робітників та нафтогазовидобувну дільницю. Терористи взяли під контроль об'єкт трохи більше ніж за 15 хвилин. Ситуація перейшла у фазу облоги, оскільки терористи шукали іноземних робітників у житлових та виробничих приміщеннях. Хоча нападники захопили іноземних робітників і оточили їх як заручників, вони не взяли в полон жодного алжирського робітника і не дозволили їм втекти. Терористи вимагали виведення алжирських збройних сил з околиць та вільного і безпечного проїзду до Малі. Терористи також вимагали безпечного проходу від житлового комплексу до виробничих будівель, щоб вони могли перегрупуватися в одному опорному пункті.

Алжирські військові завдали гелікоптерного удару по нападниках у житловому комплексі, що змусило терористів використати заручників як живий щит. Згодом терористи спробували перевезти заручників на автомобілях з житлового комплексу до виробничої зони. Коли алжирські військові зупинили колону нападників, терористи відкрили вогонь у відповідь і підірвали саморобні вибухові пристрої (СВП). Зрештою, військовим вдалося убезпечити житлові приміщення і врегулювати ситуацію, але значною ціною людських життів. Під час штурму терористів і військової відповіді загинули 40 осіб з 10 країн, а також 29 з 32 терористів. Атака в Ін Аменас привернула увагу світових ЗМІ з огляду на характер нападу та тип об'єкту критичної інфраструктури, який став мішенню терористів. Серед багатьох фактів, виявлених під час розслідування після інциденту, у фінальному звіті Statoil було зроблено висновок, що багаторівневі заходи безпеки не змогли захистити житлову зону та виробничі приміщення від терористичної атаки через надмірну довіру до алжирських військових, які захищали об'єкт. Крім того, серед вищого керівництва об'єкту не було високої культури безпеки, яке не вірило в існування реальної загрози і, відповідно, не інвестувало в забезпечення готовності та ресурси для захисту об'єкту. Після публікації звіту Statoil на об'єкті "Ін Аменас" було створено нову службу безпеки, впроваджено програму підвищення рівня безпеки, запроваджено внутрішні структури управління безпекою, а також розроблено та впроваджено новий процес оцінки ризиків та загроз безпеці. В основі всіх цих заходів лежало зобов'язання покращити навчання та міжвідомчу співпрацю.

Як ілюструє напад в Ін-Аменасі, зацікавлені сторони, що займаються критичною інфраструктурою, повинні мати справу з проблемою динамічних супротивників, що еволюціонують. Оскільки ці групи загроз зазвичай мають швидкі цикли планування, постійно адаптують свої стратегії і можуть застосовувати нову тактику для пристосування до оновлених заходів безпеки, країни-члени і партнери НАТО повинні подумати над тим, як випереджати таких супротивників.5 Одна з відповідей на це життєво важливе питання полягає в тому, що члени і партнери Альянсу повинні зосередитись на забезпеченні більшої захищеності і стійкості своїх систем критичної інфраструктури до існуючих і нових загроз і небезпек, з якими вони, найімовірніше, зіткнуться. Хоча перелік загроз з боку зловмисників є досить широким, існує декілька типів цих антропогенних загроз, які викликають найбільше занепокоєння і які ми зараз детально розглянемо в цьому розділі.

##### Інсайдер Загроза

Інсайдерська загроза - це основна штучна фізична загроза для критичної інфраструктури, яку часто не помічають і недооцінюють, незважаючи на зростаючу кількість атак, здійснених таким чином. Насправді, інсайдери становлять найбільшу загрозу - особливо якщо вони працюють з іноземною державою або іншими високопоставленими групами - через їхні детальні знання про роботу системи та практики безпеки. Інсайдери часто є співробітниками компанії або постачальниками, і вони можуть діяти як головні змовники або як спільники та інформатори зовнішнім акторам. На відміну від зовнішніх акторів, які можуть отримати доступ до елементів критичної інфраструктури лише за допомогою насильницьких дій або обману, інсайдери мають беззаперечні переваги. Враховуючи їхній доступ і можливість спостерігати за процесами на об'єкті безперешкодно протягом тривалого часу, знання, якими володіють інсайдери, або легкість, з якою вони можуть їх здобути, мають велику цінність для широкого кола потенційних зловмисників.

В осяжному майбутньому список можливих внутрішніх загроз для критичної інфраструктури включає незадоволених працівників, які прагнуть помститися, хакерів, які випробовують свої навички, злочинців, які прагнуть отримати фінансову вигоду, оперативників іноземних розвідок, які шукають конфіденційну урядову або промислову інформацію, а також терористичні угруповання або ворожі держави, які здійснюють атаки на життєво важливі послуги (такі як електроенергетика, транспорт, енергетика або телекомунікаційні системи). Окрім фізичної загрози, яку інсайдери становлять для об'єктів критичної інфраструктури, інсайдерська загроза також впливає на кіберпростір, де анонімність груп кіберзагроз ускладнює ідентифікацію відповідальних за вторгнення або з'ясування їхніх намірів. З огляду на ці фактори, методології проведення оцінки ризиків конкретних систем і вразливих місць критичної інфраструктури повинні враховувати роль кожного працівника в системі, а також усіх відвідувачів сайту або об'єкта. Наприклад, аналізуючи загрозу використання саморобного вибухового пристрою (СВП) для нападу на літак, персонал, який проводить оцінку, повинен окремо розглядати як СВП, пронесені на борт літака пасажиром, так і СВП, пронесені на борт членами екіпажу та/або іншими працівниками авіакомпанії. Впровадження ефективних процедур найму та перевірки персоналу є ключовим превентивним заходом, якого можуть вжити власники та оператори об'єктів критичної інфраструктури для посилення організаційної безпеки.

Інсайдерська загроза існує з часів найдавніших цивілізацій, а історії про інсайдерські загрози присутні майже в усіх культурах. Приклади з американської історії включають все - від зради Бенедикта Арнольда до нещодавнього несанкціонованого і руйнівного розкриття секретної інформації. У цьому спектрі існує спільний наратив: довірені і здібні люди, які часто стикаються з величезними життєвими викликами, використовують свій доступ і статус довіреної особи, щоб зрадити свою організацію і, в кінцевому рахунку, завдати шкоди нації. Враховуючи ресурси, які іноземні супротивники виділяють на використання або залучення інсайдерів в організаціях, в які вони намагаються проникнути, інсайдерська загрози будуть постійною частиною ландшафту загроз і ризиків для більшості об'єктів критичної інфраструктури на довгі роки.6

Оскільки внутрішні загрози за своєю суттю є людською проблемою, зацікавлені сторони критичної інфраструктури в кінцевому підсумку повинні приймати людські рішення для протидії їм. Див. також главу 3, в якій обговорюється важливість людського капіталу для захисту від кіберзагроз. Хоча технології можуть допомогти організаціям зрозуміти діяльність своїх співробітників у кібер- та віртуальній сферах, найпотужнішою зброєю, яку мають власники та оператори критичної інфраструктури для протидії внутрішнім загрозам, є персонал, який складає робочу силу організації. Щоб допомогти зменшити ці загрози, організаціям необхідно виявляти аномальну або підозрілу активність серед своїх співробітників, а потім реагувати на неї відповідним чином, зміцнюючи довіру і використовуючи робочу силу як партнера.7 Внутрішні загрози стають все більш важливим вектором загроз для критичної інфраструктури в контексті більш широких ризиків безпеки, а також ризиків, пов'язаних з ланцюгами поставок і кібербезпекою. Хоча інсайдерські загрози можуть завдавати шкоди через економічне шпигунство, саботаж, насильство на робочому місці, шахрайство та інші зловживання корпоративними ресурсами, різні види загроз можуть включати навмисні дії інсайдерів, які співпрацюють з іноземними спецслужбами, або інші дії інсайдерів зі зловмисними чи злочинними мотивами. Нарешті, інсайдери можуть несвідомо вчиняти порушення безпеки від легких до серйозних через просту необережність, повну недбалість або повне ігнорування простих правил і процедур безпеки.

Підсумовуючи, можна сказати, що внутрішня загроза є дуже реальною. Вона становить значний ризик для активів критичної інфраструктури і є небезпекою, яку зацікавлені сторони критичної інфраструктури повинні враховувати в процесі оцінки та управління загальним ризиком.

**CBRNE** Загроза

Зловмисне використання ХБРЯ матеріалів є ще одним типом штучної фізичної загрози знищення або пошкодження критично важливої інфраструктури. У руках зловмисників ці матеріали становлять значну загрозу для населення, інфраструктури, економіки і безпеки країн-членів НАТО. Тому захист населення, аварійно - рятувальних служб, сільськогосподарських. Захист ресурсів і критично важливої інфраструктури від цих загроз завжди має бути пріоритетом. У цьому розділі розглядається кожен елемент абревіатури ХБРЯ - хімічні, біологічні, радіологічні, ядерні та високопотужні вибухові речовини - щоб зрозуміти природу загрози і окреслити потенційні заходи для пом'якшення цих загроз і вдосконалення політики і практики КІСР.

Перша категорія ХБРЯ, хімічні матеріали, становить складний виклик, тому що суб'єкти загрози можуть відносно легко отримати доступ до цих матеріалів. Країни-члени і партнери НАТО виробляють і зберігають хімічні речовини у великій кількості через їхню роль як невід'ємної частини сучасного життя. Зловмисники, такі як терористи, екстремісти і диверсанти, можуть використовувати хімічні речовини, поширені в промислово розвинених країнах, для створення саморобних вибухових пристроїв, запалювальних речовин, хімічних агентів або навіть саморобної хімічної зброї. До найпоширеніших типів хімічних речовин, які зловмисники можуть використовувати у саморобній хімічній зброї, належать кислоти, аміак, бензол, хлор і пропан. Ці хімічні речовини виробляються або зберігаються в різних місцях, наприклад, на заводах, промислових об'єктах, автозаправних станціях і дослідницьких лабораторіях. Оскільки хімічні речовини регулярно транспортуються з використанням інших секторів критичної інфраструктури, таких як залізничні мережі, водні шляхи, автомобільні дороги і літаки, вони є легкими мішенями для саботажу і ще більш складними для захисту.

Використання штучного зарину для атаки на токійське метро в 1995 році є протверезним нагадуванням про вразливість і наслідки, пов'язані з використанням небезпечних хімічних речовин у якості зброї. Більш детально про цю атаку див. у розділі 7. Це також яскраве нагадування про потенційну небезпеку, пов'язану з мотивацією зловмисних груп, будь то іноземні чи національні терористи, маріонеткові сили, елементи, що діють від імені ворожої іноземної держави, або зловмисник- одинак зі злим умислом проти уряду, організації чи компанії. Наступна категорія серед ХБРЯ матеріалів - біологічні загрози - передбачає навмисне або випадкове вивільнення чи поширення біологічних агентів, таких як бактерії, віруси, грибки або токсини, що розповсюджуються повітрям, водою або харчовими продуктами і спричиняють хвороби, смерть і паніку. Хоча ймовірність атаки є відносно низькою через проблеми, пов'язані з культивуванням, озброєнням і розгортанням біологічних агентів, акти біотероризму все ж можуть завдати шкоди об'єктам критично важливої інфраструктури. Нещодавні спалахи кишкової палички (E. coli) продемонстрували, наскільки легко біологічна атака на критично важливу сільськогосподарську інфраструктуру може підірвати довіру споживачів і спричинити низку проблем у сфері охорони здоров'я.

Нещодавно компанія-дистриб'ютор м'яса в США була змушена відкликати понад 14 тонн яловичини через потенційне зараження кишковою паличкою. 8 Цей приклад демонструє, що сільське господарство та харчові системи є вразливими до хвороб, шкідників або отруйних речовин, які виникають природним шляхом, ненавмисно занесені або навмисно доставлені суб'єктами загрози. Деякі комахи, наприклад, можуть знищувати ліси або сільськогосподарські зони, завдаючи мільярдні економічні збитки. Отже, науково-дослідні установи, що вивчають інвазивні види, повинні управляти ризиком їх неконтрольованого або несанкціонованого вивільнення.

Нинішня глобальна пандемія, спричинена появою та швидким поширенням вірусу COVID-19 у місті Ухань, Китай, являє собою фізичний вектор біологічної загрози. Біологічні агенти можуть призвести до загибелі мільйонів людей по всьому світу та згубного впливу на критично важливу інфраструктуру, не кажучи вже про трильйони доларів, необхідних для реагування та подолання соціально-економічних збитків, завданих пандемією.9 Вплив COVID-19, а також можливе взяття на озброєння і вивільнення нових вірусів або інших біологічних агентів вимагає від країн посилення їхньої здатності виявляти, стримувати, знищувати або готуватись, пом'якшувати наслідки, реагувати на них і врешті-решт відновлюватись після вивільнення таких токсинів.

Багато "уроків, які слід засвоїти і застосувати" будуть обговорюватися, визначатися і поширюватися по всьому світу, але прикрим фактом залишається те, що уроки, які слід було б засвоїти, часто не засвоюються. Отже, коли ключові уроки ігноруються або не засвоюються на інституційному, колективному рівні, подібні події, що відбуваються в майбутньому, можуть розгортатися в такий самий спосіб і з такими самими результатами. Разом цей широкий спектр можливих біологічних загроз не можна просто ігнорувати, навіть якщо деякі з них більш вірогідні, ніж інші. Як підкреслюється в главі 13, де детально розглядаються питання оцінки та управління ризиками, після того, як уряди визначать, які об'єкти інфраструктури є дійсно критично важливими, всі загрози, що становлять для них значний ризик, повинні бути чітко визначені, оцінені і враховані при визначенні та управлінні ризиками.

Застосування радіологічної та ядерної зброї, третьої та четвертої категорій загроз в рамках ХБРЯ, є ще однією небезпечною фізичною загрозою для критичної інфраструктури. Поганою новиною на цьому фронті є те, що з'являється все більше добре організованих і добре фінансованих терористичних організацій, які тепер мають легкий доступ до знань, необхідних для створення бомби, оголосили про свій намір шукати матеріали, необхідні для створення і використання зброї масового знищення. Хоча ймовірність того, що терористична група створить навіть грубий прозорий пристрій або здійснить диверсію на атомній електростанції, є низькою, міжнародна спільнота не може дозволити собі бути спокійною. Доброю новиною є те, що міжнародні політичні лідери здебільшого поділяють однакове сприйняття загрози ядерного тероризму і все частіше співпрацюють у цьому ключовому політичному питанні, щоб зменшити ризики, що виходять від нього.

Згідно зі звітом Асоціації з контролю над озброєннями та Робочої групи з розщеплюваних матеріалів, в якому зібрані дані за 2010-16 роки, країни досягли значного прогресу у стримуванні ядерного тероризму, а також у зміцненні та підвищенні фізичної ядерної безпеки. Ці добровільні національні зобов'язання є одними з найбільш відчутних та інноваційних протоколів з фізичної ядерної безпеки, і країни активно практикують і впроваджують їх по всьому світу. Не існує достовірних доказів того, що будь-яка терористична група змогла отримати необхідну багатокілограмову критичну масу збройового плутонію, необхідну для створення ядерної зброї. Навіть якби група володіла кількома кілограмами матеріалу, щ о розщеплюється, груба конструкція, створена терористами, потребувала б набагато більше матеріалу і становила б величезний технічний виклик. В той же час, фахівці з безпеки не можуть просто відкидати таку можливість.

Імовірність того, що терористи або інші зловмисники створять і підірвуть так звану "брудну бомбу" - інакше відому як радіологічний пристрій розсіювання (РПР) - значно вища, оскільки виготовлення РПР не складніше, ніж виготовлення СВП. РРП поєднує звичайні вибухові речовини з матеріалами, що містять радіоактивні ізотопи, деякі з яких можна знайти в таких виробах, як обладнання для лікування раку, ксерокси, годинники і навіть побутові детектори диму, що містять радіоактивний ізотоп америцій 241. Детонація RDD, ймовірно, матиме більший психологічний вплив на постраждале населення, ніж фізична шкода, яку вона може спричинити. З огляду на ймовірність нападу з використанням СЗР, зацікавлені сторони критичної інфраструктури повинні розглянути, наскільки сили реагування готові пом'якшити фізичні і психологічні наслідки вибуху, а також який вплив така подія матиме на об'єкти і системи.

Окрім шкоди майну та критичній інфраструктурі, зловмисне використання ХБРЯ матеріалів може мати довготривалий вплив на психічне здоров'я та психіку громадян та осіб, які здійснюють перше реагування на надзвичайні ситуації. у такому інциденті. Наприклад, фізична і психологічна травма від вибуху федеральної будівлі Альфреда П. Мурри в Оклахома-Сіті і терактів 11 вересня в США призвела до посттравматичного стресового розладу (ПТСР) і збільшила використання і залежність від ліків від тривоги. Серед майже 37 000 членів Реєстру здоров'я Всесвітнього торгового центру приблизно 14 відсотків страждали від ПТСР і 15 відсотків від депресії більш ніж через десять років після терактів, а дослідження показують, що приблизно 10 відсотків тих, хто першими реагував на теракти, все ще страждали від ПТСР більш ніж десять років потому. Аналогічно, негативні психічні і психологічні наслідки пандемії COVID-19 свідчать про важкі втрати для суспільства, які можуть бути спричинені фізичними атаками на об'єкти критичної інфраструктури. Противники зробили висновки з цих та інших катастрофічних подій і, безумовно, враховують ці наслідки у своїх переслідуваннях фізичних атак і використанні гібридних векторів загроз для розколу західних суспільств.

Остання категорія загроз у сімействі ХБРЯ, вибухові речовини, є найпоширенішим типом антропогенної фізичної загрози для критичної інфраструктури. Ця категорія передбачає використання вибухових речовин, таких як саморобні вибухові пристрої, ракети і гранати, для завдання шкоди, виведення з ладу або знищення об'єктів критичної інфраструктури. Окрім звичайних вибухових речовин, до цієї категорії також належать такі прості інструменти, як запальнички та сірники, саморобні запалювальні пристрої, СВП, встановлені на транспортних засобах, та саморобні вибухові жилети. У цьому сенсі такі прості речі, як бензинова бомба або коктейль Молотова, у поєднанні зі злим умислом суб'єкта загрози можуть призвести до катастрофічних наслідків, пошкодивши або зруйнувавши фізичні об'єкти критичної інфраструктури, а також порушивши або припинивши надання основних послуг, які вони забезпечують. Тому заходи безпеки для об'єктів критичної інфраструктури повинні враховувати більше, ніж просто захист від звичайних СВП . Деякі потенційні заходи захисту включають своєчасне отримання точної інформації; сучасне автоматизоване спостереження (наприклад, відеоспостереження); пристрої виявлення для внутрішнього і зовнішнього використання; визначення пріоритетності загроз встановленими системами (щоб уникнути постійних хибних тривог); сумісність комунікацій; і, що набуває все більшого значення, стійкість організації або об'єкта після нападу.

##### Безпілотник Загроза

Ще одним видом антропогенної фізичної загрози для критичної інфраструктури є зловмисне використання дронів. Дрони - це будь-який транспортний засіб, що може пересуватися автономно; хоча зазвичай дрони і безпілотні літальні апарати (БПЛА) не зовсім однакові. Автономний безпілотник не потребує втручання людини, але може літати за допомогою бортового автопілота, комп'ютера та набору датчиків. Хоча БПЛА не потребує присутності людини-пілота або членів екіпажу на борту літального апарату для здійснення польоту, люди-оператори зазвичай керують БПЛА дистанційно з землі.12 БПЛА є компонентом безпілотної авіаційної системи, яка включає не лише БПЛА, але й усе необхідне для його функціонування: наземний модуль управління, модуль системи глобального позиціонування, систему зв'язку з БПЛА, а також людину на землі, яка керує БПЛА. Незважаючи на ці нюанси, в цьому розділі ми будемо використовувати загальний термін "*дрон"* для позначення категорії фізичної загрози, яку становить весь спектр повністю і напівавтономних повітряних систем.

Коли дрони використовуються технічно підкованими особами-одинаками, терористичними угрупованнями, національними і транснаціональними злочинними організаціями або підконтрольними їм маріонетками, що діють у місцях бойових дій, на спірних територіях або навіть над вразливими об'єктами критичної інфраструктури, вони становлять значну загрозу для критичної інфраструктури. Тому процеси оцінки та управління ризиками для безпеки критичної інфраструктури повинні включати цей вектор фізичної загрози в загальну концепцію CISR. Залежно від потужності і розміру, дрон може перевозити контрабанду, хімічні речовини, інші вибухові речовини чи озброєні вантажі. Ці системи також здатні безшумно вести спостереження з неба за великою територією з метою підступної або стратегічної розвідки і навіть можуть використовуватися для здійснення кібератак, пов'язаних з викраденням комерційної таємниці, технологій або конфіденційної інформації, що впливає на критично важливу інфраструктуру. Існують численні приклади зловмисної діяльності з використанням дронів для нападів на об'єкти критичної інфраструктури та інші чутливі об'єкти або персонал. У Франції сім атомних електростанцій підтвердили несанкціоновані польоти дронів над своїми об'єктами у 2014 році, а активісти Грінпіс навмисно врізалися дроном у французьку атомну електростанцію поблизу Ліона у 2018 році.14 Ці приклади показують, що атаки з дронів є новим вектором фізичної загрози для здійснення атак на об'єкти критичної інфраструктури - тенденція, яка, ймовірно, посилюватиметься в найближчі роки.

Найпопулярніші квадрокоптери, що коштують всього 1200 доларів, можуть перевозити предмети вагою до одного кілограма. Зловмисники можуть скористатися доступністю і мобільність квадрокоптерів для транспортування камери, щоб знімати мости, урядові будівлі, стадіони або кортежі, шукати порушення правил безпеки або навіть здійснювати атаки з використанням легких вибухових пристроїв. Через свої фізичні та експлуатаційні характеристики багато типів дронів можуть уникати виявлення і створювати проблеми для власників та операторів об'єктів критичної інфраструктури. З огляду на постійну доступність і універсальність дронів, зловмисники, ймовірно, використовуватимуть їх у будь-якій з наступних якостей. По-перше, вони можуть використовувати дрони для розвідки критично важливих об'єктів з метою збору розвідувальних даних про розташування об'єкта, переміщення охорони або іншої інформації, яка може допомогти у здійсненні фізичної атаки. По-друге, групи загроз можуть використовувати дрони для скидання вибухівки, призначеної для пошкодження критично важливої або чутливої інфраструктури в транспортних вузлах та інших місцях масового скупчення людей. По-третє, дрони можуть доставляти зброю або інші матеріали для використання в атаці. І нарешті, дрони можуть забезпечувати повітряну підтримку і спостереження для підтримки наземної атаки. Щоб продемонструвати смертоносність атак безпілотників на об'єкти критичної інфраструктури, зараз доречно розглянути приклад атаки на Saudi Aramco.

14 вересня 2019 року повстанці-хусити, що базуються в Ємені, взяли на себе відповідальність за використання комбінації дронів і крилатих ракет для атаки на два стратегічні нафтові об'єкти в Саудівській Аравії, якими керує державна компанія Saudi Aramco. За повідомленнями, було зафіксовано 19 точок ураження на нафтопереробному заводі в Абкаїку - найбільшому в світі - і на нафтовому родовищі Хурайс, що спричинило пожежі, які призвели до значних руйнувань і перебоїв у роботі об’єктів Хоча повстанці Хуті взяли на себе відповідальність за атаку, деякі західні розвідувальні служби заперечують це твердження. Передові технології безпілотників, які використовувалися в цих атаках, свідчать про різку ескалацію конфлікту і про здатність повстанців здійснювати такі напади , що дозволяє припустити, що ця атака була терористичним актом у регіоні, спонсорованим державою або за її сприяння.

Незважаючи на невизначеність щодо конкретних суб'єктів загрози, які стояли за атакою, шкода, завдана самому серцю нафтової інфраструктури Саудівської Аравії, була беззаперечною. Атаки пошкодили більше половини установок для розгерметизації і три стабілізаційні колони на нафтових об'єктах в Абкаїку, що призвело до зниження щоденного видобутку нафти в Саудівській Аравії приблизно на п'ять мільйонів барелів на добу протягом 10 днів.1 Ця втрата, яка становить близько п'яти відсотків світового

Внаслідок цього світові ціни на нафту підскочили до 20-річного максимуму. Рівень безпеки на заводі в Абкаїку вважався надзвичайно високим, тому руйнування, спричинені атаками, посилили занепокоєння щодо ширшого регіонального конфлікту і збільшили глобальну напруженість, яку можуть посилити подібні або подальші атаки на критично важливі об'єкти інфраструктури. Можливо, найбільш тривожним є те, що атаки на завод в Абкаїку, який деякі експерти називають перлиною саудівської нафтової інфраструктури і серцем світової нафтової системи, поставили під сумнів цінну репутацію Саудівської Аравії як надійного, стабільного постачальника нафти на світовий ринок.

Значний досвід, отриманий після інциденту, включає баланс загроз, ризиків і шкоди при розгляді питання про те, як зробити критичну інфраструктуру більш безпечною. Природа видобутку нафти, газу та енергії ілюструє значну взаємозалежність з іншими інфраструктурними секторами, економічним майбутнім і глобальними ринками. Оператори критичної інфраструктури надають послуги, які важко захистити з повітря без підтримки військових або сил безпеки. Зменшення загроз нафтогазовим об'єктам суттєво відрізняється від протидії загрозам іншим видам критичної інфраструктури, зокрема, таким видам транспорту, як авіація та залізниця. Розділи 6 і 7 містять більш детальну інформацію про захист від загроз цивільній авіації та залізниці. Ці тематичні дослідження наочно демонструють, що фахівці з безпеки не можуть вживати заходів і зусиль для зменшення загроз у конкретному секторі, а потім застосовувати їх однаково в усіх секторах критичної інфраструктури. Необхідно мати баланс, заснований на загрозах, правдоподібності, достовірності та пропорційності. Розділи 7 і 1 присвячені обговоренню цих концепцій в рамках ширшої системи стратегічної оцінки ризиків.

Цей короткий огляд того, як зловмисники використовували дрони в минулому, змушує замислитися над тим, скільки часу пройде, перш ніж суб'єкти загрози посилять свою тактику і почнуть ширше використовувати дрони для атак на об'єкти критичної інфраструктури. Однією з таких небезпек є роїння дронів - тактика, яка передбачає одночасне використання декількох дронів для координації операцій і виконання завдань, які не під силу одному дрону. У такій конфігурації кожен дрон може виконувати схожу функцію або мати унікальну, спеціалізовану роль, наприклад, збирати інформацію, нести зброю чи вибухівку або передавати повідомлення. Рой безпілотників вимагає розширених можливостей, в тому числі здатності окремих дронів дотримуватися дистанції, уникати зіткнень на близькій відстані і передбачати, де перебуватимуть інші дрони в рої в певний момент часу. Щоб досягти такого рівня складних можливостей, рої дронів зазвичай покладаються на зондування в реальному часі, штучний інтелект, алгоритми комп'ютерного зору і зв'язок на основі радіочастотного, стільникового або супутникового зв'язку. Використовуючи єдину наземну станцію управління для контролю над роєм безпілотників, суб'єкти загрози можуть спростити розгортання і вимоги до обладнання, а також ефективно керувати безпілотниками автономно, щоб оператору не доводилося контролювати кілька безпілотників в реальному часі.21 Без зайвих фантазій можна уявити собі рої безпілотників, здатних маневрувати в умовах активних оборонних заходів, виявляти цілі і доставляти такі різноманітні вантажі, як хімічні агенти над населеними пунктами або вибухівку проти таких цілей, як нафтові родовища або водоочисні споруди.22

Вивчення загрози, яку дрони і зграї дронів становлять для критично важливої інфраструктури, підкреслює необхідність для країн - членів і партнерів НАТО вжити життєво важливих заходів для посилення своїх сил і засобів СІСР. Одним з таких прикладів є те, що Агентство зв'язку і інформації НАТО розробило недорогий прототип рішення для швидкого виявлення, ідентифікації і локалізації малих дронів, які можуть становити загрозу. Цей прототип, відомий як система ARTEMIS, використовує електромагнітні хвилі для ідентифікації дронів і передові технології виявлення і класифікації радіочастотних сигналів, які використовують дрони. Обладнання успішно пройшло випробування у відкритих польових умовах, показавши дуже багатообіцяючі результати для використання у зменшенні загрози, яку становлять комерційні дрони.

##### Загроза високоточної ударної зброї

Хоча високоточні атаки з використанням ракет, які традиційно вважаються звичайними озброєннями, рідко беруться до уваги під час оцінювання національної безпеки, вони становлять загрозу основним системам критично важливої інфраструктури в усьому НАТО. Високоточні ракети можуть вражати цілі на великих відстанях, від 100 метрів до тисяч миль. Хоча військові вже застосовують певні заходи.

Для запобігання таким прихованим атакам за кордоном і захисту ключових військових об'єктів, інші вузли критичної інфраструктури погано захищені або не захищені взагалі, що робить їх відносно легкими цілями. З огляду на постійно зростаючі можливості терористів придбати ракетні технології і зброю, високоточні ракетні удари можуть становити постійну загрозу як з боку терористів, так і з боку держав-ізгоїв. Для розуміння численних високоточних озброєнь, які можуть загрожувати критично важливим об'єктам інфраструктури в країнах - членах НАТО, в цьому розділі розглядаються загрози, які становлять системи малої і великої дальності.

У категорії систем малої дальності найпоширенішою зброєю є переносні зенітно-ракетні комплекси (ПЗРК), які спочатку були розроблені для захисту від військових літаків. Оскільки ПЗРК здатні завдавати високоточних ударів, доступні в усьому світі і бувають різних конфігурацій, терористи традиційно використовують їх для нападів на пасажирські літаки. Приклади терористичних атак проти цивільної авіації з використанням ПЗРК див. у розділі 6. Зважаючи на відносно невеликі розміри - деякі системи важать лише 35 фунтів і мають довжину 6 футів - ПЗРК легко приховувати і транспортувати, що робить їх ідеальною зброєю для зловмисників, які шукають вразливі місця на наземних об'єктах, таких як електростанції або нафтогазові об'єкти. Аналогічно, протитанкові керовані ракети (ПТРК) легко доступні на чорному ринку зброї, їх так само легко приховати і транспортувати. Зловмисники можуть легко зберігати ПТРК разом з системою наведення і боєприпасами в багажнику автомобіля і використовувати їх для ураження будь- якої кількості об'єктів критичної інфраструктури, таких як великі фінансові установи, водоочисні споруди і навіть основні урядові будівлі.

Серед систем високоточної зброї великої дальності загроза, яку крилаті ракети становлять для критичної інфраструктури, також зростає. Хоча відносно небагато країн мають крилаті ракети наземного базування, багато хто має протикорабельні крилаті ракети. Хоча основною функцією цих систем є ураження кораблів у морі, зловмисники можуть також модифікувати їх для ураження об'єктів критичної інфраструктури або просто використовувати як зброю терору, запускаючи їх без розбору по населених районах. Так само балістичні ракети стають все більш поширеною загрозою. Хоча лише кілька країн володіють міжконтинентальними балістичними ракетами, багато хто має балістичні ракети, здатні діяти на менших відстанях. Зловмисники можуть контрабандою перевозити ці ракети на вантажних суднах і транспортувати їх по всьому світу для застосування проти об'єктів критичної інфраструктури або населених пунктів в країнах-членах і партнерах Альянсу.

##### Електромагнітний імпульс Загроза

Іншим вектором фізичної загрози є електромагнітний імпульс (ЕМІ) і катастрофічні наслідки, які він може спричинити. ЕМІ - це короткий сплеск високоенергетичного електромагнетизму, який за певних обставин може вивести з ладу або зруйнувати електричні та електронні системи. Оскільки значна частина сучасного життя залежить від електрики та електроніки, широкомасштабна атака ЕМІ може спричинити велику катастрофу. При взаємодії з магнітним полем Землі ці потужні імпульси можуть пошкодити електронне та електричне обладнання, таке як комп'ютери, мобільні телефони, трансформатори, лінії електропередач і більш широку критично важливу комунікаційну інфраструктуру. Огляд мережі зв'язку як життєво важливого сектору див. у главі 9. Навіть гірше, конструкція багатьох електричних мереж означає, що пошкодження певних електричних систем, які є життєзабезпеченням будь-якого сучасного суспільства, може спричинити збої в роботі цілої низки систем - банківської, енергетичної, транспортної, виробництва і доставки продуктів харчування, водопостачання, аварійних служб і кіберпростору - в усій країні або регіоні.

Екстремальні електромагнітні інциденти, спричинені навмисною, штучною атакою ЕМІ або природними геомагнітними збуреннями (також званими космічною погодою), можуть завдати значної шкоди критично важливим секторам інфраструктури, таким як електромережі, зв'язок і транспорт, мережі, а також системи водопостачання і водовідведення. Ймовірно, що наслідки атаки матимуть каскадний характер, коли спочатку буде порушено один або кілька елементів критично важливої інфраструктури, а потім вони поширяться на інші сектори і вийдуть за межі початкових географічних регіонів. Навмисні атаки з використанням висотних ядерних вибухів, спеціальних звичайних боєприпасів або неядерних пристроїв спрямованої енергії можуть призвести до подій ЕМІ. Залежно від специфічних характеристик зброї і профілю атаки, наслідки події ЕМІ можуть варіюватися в масштабах від локальних до регіональних і континентальних.

Уряди всього світу, і особливо їхні збройні сили, займаються оцінкою загрози ЕМІ з перших років холодної війни. Цей процес є складним завданням, оскільки необхідна технічна інформація може змінюватися - особливо у випадку неядерного ЕМІ - і мотиваційні аспекти, що випливають з політичних міркувань і економічну ситуацію важко оцінити і передбачити. Військовий аналітик Пітер Прай, який раніше очолював Комісію Конгресу США з питань ЕМІ, зазначає, що вибух ядерної зброї приблизно за 200 миль над Сполученими Штатами може спричинити подію ЕМІ, яка охопить майже увесь північноамериканський континент, а зловмисники або групи можуть створити і використати генератор ЕМІ, достатньо потужний для того, щоб вивести з ладу великий мегаполіс. Незалежно від того, чи є це наслідком нападу, чи природної події , ризики, пов'язані з ЕМІ, є значними і вони заслуговують на постійну увагу і дії з боку зацікавлених сторін, які займаються критично важливою інфраструктурою в країнах НАТО.

### Аварії та технічні загрози

Остання категорія фізичних загроз, що розглядається в цьому розділі, - аварії та технічні загрози - включає в себе безліч катастроф, спричинених діями або бездіяльністю людей, технічними або інфраструктурними збоями різного роду, а також ситуаціями або подіями, що виникають безпосередньо через людські помилки. Серед цих загроз - технічні збої в електромережах і водоочисних спорудах, несправні системи безпеки, старіння інфраструктури, що призводить до прориву водогону або витоку небезпечних матеріалів, і навіть мавпи (або інші істоти), що потрапляють туди, куди їм не слід потрапляти. Наслідки цих загроз варіюються від легких до тяжких.

Прикладами таких інцидентів є витоки радіації на атомних електростанціях, викиди токсичних газів з хімічних заводів, смертельні викиди з заводів з виробництва добрив, а також людські жертви і руйнування довкілля, спричинені катастрофами нафтових і газових платформ. Викид смертоносних радіоактивних матеріалів після аварій на Чорнобильській АЕС у 1986 році та на АЕС у Фукусімі у 2011 році - це два конкретні приклади з недавньої історії. Катастрофічні наслідки цих двох інцидентів також підкреслюють руйнівний потенціал використання цих матеріалів у руках зловмисників. Зі зростанням використання ядерної енергії та залежності від неї, крадіжка ядерних матеріалів і терористичні мотиви для нападу і вивільнення радіоактивних матеріалів є реальністю, яка вимагає надійної безпеки, підтримки безпеки і регуляторного нагляду для протидії.

Темпи, з якими сучасні економіки стали нерозривно пов'язаними протягом останніх двох десятиліть, особливо завдяки значним досягненням у сфері інформаційно- комунікаційних технологій, піддали суспільства і критичну інфраструктуру країн-членів НАТО до безпрецедентних загроз і вразливостей. Навіть простий знос створює постійні проблеми для критичної інфраструктури. Хоча об'єкти критичної інфраструктури не виходять з ладу лише через похилий вік або запізніле технічне обслуговування, старіння активів може погіршити продуктивність і призвести до функціональної застарілості, і обидва ці фактори підвищують ризик виходу з ладу. До речі, нещасні випадки, пов'язані з використанням сільськогосподарської техніки, наприклад, використання екскаватора для копання землі, спричиняють більше збоїв у роботі систем зв'язку на день, ніж будь-яка інша фізична подія. Загрози, пов'язані з аваріями і технічними несправностями, прикро вражають тим, що будь-яка з них може призвести до неприйнятних втрат у вигляді людських жертв, знищення майна, економічних наслідків, а також підриву суспільної моралі і довіри до влади. Саме тому всі три категорії фізичних загроз - стихійні лиха, техногенні катастрофи, аварії та технічні збої - необхідно брати до уваги при визначенні ризику для конкретних елементів критичної інфраструктури в будь-якому секторі.

### Більше про що слід подумати**:** Загрози для портових об**'**єктів

На морський транспорт - суховантажі, контейнеровози і нафтові танкери - припадає 80 відсотків обсягу світової торгівлі і 70 відсотків її вартості, що робить великі морські порти центрами усієї глобальної економічної діяльності. Багато об'єктів критичної інфраструктури в країнах - членах НАТО розташовані вздовж узбережжя, в тому числі нафтогазові термінали, опріснювальні установки і атомні електростанції, які потребують великої кількості води для процесу охолодження. Ці великі порти являють собою багате на мішені середовище для зловмисників; правильна ціль, в правильному місці, в правильний час, використовуючи правильний вектор загрози, може завдати величезної шкоди портовим об'єктам, а також суспільству і економіці, які вони підтримують. Планувальникам безпеки і стійкості, а також власникам і операторам портових об'єктів необхідно враховувати багато факторів, коли вони думають про фізичні загрози для великих портів. Щоб краще зрозуміти виклики, пов'язані із захистом цих життєво важливих об'єктів, зацікавлені сторони в морських портах повинні розглядати порт з геопросторової точки зору, що вимагає вивчення водного простору навколо порту - як на рівні поверхні, так і під водою, а також портових об'єктів на суші і повітряного простору над ними.

Що стосується фізичних загроз з боку води, яка оточує портові споруди, то кілька терористичних організацій продемонстрували наміри розвивати можливості для нанесення кінетичних ударів з моря, зокрема ті, що поєднують використання аквалангістів і вибухівки. Існує два основних методи, які водолази використовують для атак на порти: вони або прикріплюють міну до судна, що стоїть поруч з портом, або встановлюють міну на д н о портового каналу. Водолазам може бути складно транспортувати і встановлювати велику кількість вибухівки, яка була б необхідна для значного впливу при атаці на більшість великих суден. Проте, стратегічно розміщений заряд може завдати значної шкоди і створити труднощі для круїзних лайнерів, військових кораблів або однокорпусного танкера, наповненого компонентами, які підтримують широкий спектр критично важливої інфраструктури. Ця ідея не є надуманою, про що свідчить приклад з грудня 2014 року. Тоді єгипетські сили безпеки заарештували членів терористичного осередку на Синаї за спробу здійснити напад на єгипетські військові кораблі. Під час арешту у членів терористичного угруповання, яке вже було причетне до попередніх нападів із застосуванням стрілецької зброї і ракет для влаштування засідок і захоплень єгипетських військових кораблів, було знайдено водолазне спорядження.

Аналогічно, охорона водних портів повинна враховувати атаки з різних платформ, які можуть використовувати зловмисники, включаючи швидкісні катери, водні мотоцикли, морські контейнери і дистанційно керовані човни. При розгляді того, які типи атак є ймовірними, особливо корисними є два конкретні приклади. Перший вектор атаки, який переслідують терористичні групи, такі як Аль-Каїда, полягає в контрабанді СВП в корабельний контейнер для детонації проти цілей, віддалених від місця запуску, як форма проекції сили для терористичних груп.

Другим потенційним способом атаки є створення рою, який поєднує безпілотники з човнами-смертниками і пілотовані човни-смертники - фактично, морська версія повітряних дронів і роїв дронів, описаних в попередньому розділі. Цей вектор атаки схожий на те, як Японський імператорський флот і армія використовували катери-смертники *Shinyo*, здатні перевозити понад 500 фунтів вибухівки і рухатися зі швидкістю майже 30 миль на годину, щоб завдати значної шкоди американським кораблям під час Другої світової війни. У сучасному контексті повстанці Хуті використали дистанційно керований човен, навантажений вибухівкою - ймовірно, наданий Корпусом вартових ісламської революції Ірану - для нападу на Королівський

Фрегат ВМС Саудівської Аравії "*Аль-Мадіна"* в січні 2017 року. Хоча цей вектор атаки схожий на атаку човна-смертника на есмінець ВМС США "*Коул" у* 2000 році, можливість проведення безпілотних атак становить більш небезпечну загрозу, оскільки зловмисники можуть діяти сміливіше і смертоносніше, коли їхнє власне життя не знаходиться під прямим загрозою. Що стосується фізичних загроз для наземних портових об'єктів, то для більшості терористів небезпідставно залишаються улюбленою зброєю саморобні вибухові пристрої, що встановлюються на транспортних засобах. Ця мобільна зброя може містити велику кількість вибухівки в транспортному засобі, і чим більший транспортний засіб, тим потужніший вибух. Зловмисники можуть не лише доставити СВП безпосередньо до місця призначення, але й виявити і запобігти таким атакам може бути складно.

Як уже зазначалося в цьому розділі, зловмисники можуть скористатися доступністю і мобільністю дронів, щоб атакувати наземні портові об'єкти зверху з метою виведення з ладу ключового обладнання або нейтралізації робочої сили, тимчасово або назавжди. Такі атаки можуть бути досить руйнівними під час рутинних портових операцій і повсякденної роботи. Вони можуть завдати ще більшої шкоди, коли країни- члени НАТО перебувають у процесі мобілізації військових сил і засобів на підтримку колективної оборони, врегулювання кризових ситуацій або інших зовнішніх операцій. У розділі 4 детально обговорюється важливість морських перевезень для операцій НАТО і виклики, які створюють гібридні загрози. Труднощі будівництва і утримання безпечних, стійких портів, безумовно, величезні. Проте значні інтелектуальні зусилля і ресурси, розвиток передових засобів ситуаційної обізнаності для забезпечення загальної оперативної картини, розгортання ефективних заходів протидії загрозам і найсучасніших систем захисту допомагають убезпечити великі порти. Це досягнення є одним з найкращих прикладів найкращих зусиль CISR в ряді країн.

### 

### Зростання складності та

аутсорсинг фізичних загроз

Після терактів 11 вересня можливості моніторингу, виявлення та захисту від широкого спектру фізичних загроз для критичної інфраструктури значно зросли, про що свідчить величезна кількість камер відеоспостереження, а також супутнього програмного забезпечення і людей-контролерів, які оточують майже всі об'єкти критичної інфраструктури в багатьох західних країнах.

На жаль, оскільки захисники стали більш витонченими, зловмисники також стали більш витонченими і їхні можливості зросли.

Оскільки приватний сектор володіє і управляє більшою частиною критичної інфраструктури на Заході, дорогі заходи безпеки неминуче конкурують з цілою низкою економічних міркувань, створюючи реальність, в якій безпека сама по собі ніколи не є вирішальним фактором. Така динаміка створює дві унікальні вразливості. Перша - нестача ресурсів - полягає в тому, що захист критичної інфраструктури від фізичних загроз може бути дорогою справою, яка вимагає виділення значних ресурсів, але при цьому має конкурувати з іншими пріоритетами, що конкурують між собою. Часто не вистачає ресурсів для вирішення всіх потенційних проблем безпеки, або немає достатньо вагомих підстав, щоб виправдати витрачання коштів на безпеку замість підвищення ефективності бізнесу чи покращення операцій. Великі компанії та організації з більшою ймовірністю, ніж малі, можуть дозволити собі такі витрати. Друга вразливість - складність аутсорсингу - підкреслює тенденцію компаній та організацій зосереджуватися на ключових компетенціях, а все інше передавати на аутсорсинг зовнішнім постачальникам, включаючи такі сфери, як транспорт, комунальні послуги, охорона здоров'я та постачальники фінансових послуг. Досить часто послуги фізичного та кіберзахисту також передаються на аутсорсинг, що ускладнює оптимізацію захисту.

З огляду на тенденцію до появи нових фізичних загроз для критичної інфраструктури, уряди і приватний бізнес повинні усвідомлювати відповідальність, яку вони несуть, і тому залишатися пильними в своїх зусиллях щодо передбачення і протидії фізичним загрозам в максимально можливій мірі. Важливо, щоб менеджери з безпеки навчилися відстежувати фізичні загрози і постійно впроваджувати інновації для забезпечення максимальної стійкості, оскільки ціна невдачі занадто висока.

### Зв**'**язок між загрозою та ризиком

Точна оцінка загроз ґрунтується на детальному знанні та розумінні намірів і можливостей потенційних суб'єктів загрози, будь то стихійні лиха, маріонеткові сили, зловмисні недержавні суб'єкти, терористи або інсайдери зі зловмисними намірами. Якісна оцінка ризиків безпеці враховує ймовірність - включаючи як загрозу, так і вразливість - і наслідки небажаних подій, спричинених різноманітними суб'єктами загроз.

Програма CISR - це здатність зіставити певну загрозу з ризиками і вразливостями в системах критичної інфраструктури та поточними можливостями відповідних зацікавлених сторін. Без стратегічної прихильності до програми безпеки, заснованої на загрозах і ризиках для критичної інфраструктури, буде практично неможливо створити ефективну національну архітектуру, культуру і політику КІСБ, яка б демонструвала її ефективність.

Розуміння намірів суб'єкта загрози вимагає детального знання і розуміння його переконань, досвіду, світогляду, цілей і можливостей реалізувати будь-який зловмисний намір шляхом здійснення фізичної атаки. У випадку природних загроз або загроз, пов'язаних з аваріями чи технічними збоями, такі знання включають наукові прогнози ймовірності стихійних лих або виходу з ладу компонентів інфраструктури під впливом таких факторів, як час і стрес. Експерти з безпеки погоджуються, що безліч виснажливих і шкідливих дій, які зловмисники можуть вчинити проти об'єктів критичної інфраструктури, є різноманітними, постійно змінюються, стають все більш витонченими і їм важко запобігти. Однак, якщо ми хочемо ефективно захистити критичну інфраструктуру і зробити її більш стійкою, то зацікавлені сторони, на яких покладено цей обов'язок, повинні глибоко розуміти спектр ймовірних фізичних загроз, які існують сьогодні або лежать просто за горизонтом - місце, де часто з'являються невідомі невідомі, про які йшлося в розділі 1.

*Ризик -* це потенційна можливість небажаного результату в результаті інциденту, події або явища, що визначається його ймовірністю - функцією загроз і вразливостей - і пов'язаними з ним наслідками. *Управління ризиками - це* процес виявлення, аналізу та інформування про ризики з метою їх прийняття, уникнення, передачі або контролю до прийнятного рівня та вартості. Управління ризиками зосереджує ресурси на тих загрозах і небезпеках, які з найбільшою ймовірністю можуть спричинити значні небажані наслідки для конкретної системи або сектору критичної інфраструктури, і визначає дії, спрямовані на запобігання або пом'якшення наслідків цих інцидентів. Воно також підвищує безпеку і зміцнює стійкість шляхом визначення і пріоритизації дій, спрямованих на забезпечення безперервності основних функцій і послуг, а також на підтримку посиленого реагування і відновлення. Управління ризиками полегшує прийняття рішень і визначення пріоритетів серед усіх зацікавлених сторін.

Система управління ризиками визначає підхід до послідовного виконання трьох ключових функцій. По-перше, вона спрямована на виявлення, аналіз і розподіл ресурсів для запобігання, виявлення, припинення і підготовки до загроз і небезпек для критичної інфраструктури. По-друге, система управління ризиками дозволяє особам, які приймають рішення, визначати пріоритети і спрямовувати зусилля на зменшення вразливостей і усунення фізичних особливостей або експлуатаційні характеристики систем критичної інфраструктури, які є вразливими до експлуатації або схильні до певної загрози. Нарешті, вона допомагає зацікавленим сторонам проактивно пом'якшити потенційні наслідки інцидентів або підготуватися до їх ефективного обмеження, якщо вони все ж таки відбудуться. Система управління ризиками може бути застосована на всіх рівнях державного або приватного сектору. Вона повинна охоплювати всі загрози і небезпеки, а також різні фактори в усіх секторах критичної інфраструктури, на додаток до окремих активів і систем. Поглиблене пояснення суті оцінки та управління ризиками для безпеки, а також відповідні кращі практики наведені в главі 13.

Типи фізичних загроз, визначені в цій главі, можуть завдати шкоди, пошкодити, вивести з ладу або знищити об'єкти критичної інфраструктури. Наміри і можливості супротивника, доступ супротивника до об'єкта критичної інфраструктури і можливість діяти, керуючись цими мотивами загрози, впливають на те, чи здійснять групи, що загрожують, атаку, коли і як саме. Загрози критичній інфраструктурі відрізняються за намірами, можливостями, потенційними або запланованими цілями, методологіями атак і можливостями. Замість того, щоб зосереджуватися на одному типі загрози чи небезпеки, державам слід визначити всі загрози і небезпеки, які становлять найбільші ризики для їхньої критичної інфраструктури. Цей процес дозволяє більш ефективно і раціонально планувати і розподіляти ресурси.

Критична інфраструктура вже давно піддається ризикам, пов'язаним з багатьма фізичними загрозами, про які йшлося в цьому розділі, але зараз серйозні ризики і загрози також походять з кіберпростору. Ці ризики виникають через зростаючу інтеграцію інформаційно-комунікаційних технологій з критичною інфраструктурою, а також через дії супротивників, які зосереджуються на використанні потенційних кібервразливостей. Оскільки фізичні об'єкти стають все більш залежними від складних кіберсистем, критично важлива інфраструктура буде ставати все більш вразливою до певних кіберзагроз. Багато з цих кіберзагроз можуть спричинити подібний рівень шкоди, виведення з ладу та руйнування, як і низка фізичних загроз. Див. розділи 3 і 4, в яких розглядається природа загроз у кіберпросторі і гібридне поєднання фізичних і кіберзагроз.

Зв'язки та взаємозалежності між елементами та секторами інфраструктури означають, що пошкодження, порушення або знищення одного елемента інфраструктури внаслідок фізичної (або кібернетичної) події може спричинити каскадні ефекти, які впливають на безперервність операцій в інших секторах або системах. Виявлення і розуміння взаємозалежностей (двосторонніх) або залежностей (односторонніх) між елементами і секторами інфраструктури є важливими для оцінки ризиків і вразливостей, а також для визначення того, які кроки можуть бути вжиті для підвищення безпеки та стійкості. У главі 12 наведено додаткові пояснення залежностей і взаємозалежностей між секторами критичної інфраструктури, а також потенціалу для каскадних або ескалаційних ефектів. Наприклад, функціонування електромережі залежить від інтегрованих інформаційно-комунікаційних систем інших секторів критичної інфраструктури, в той час як електромережа також живить сектори життєзабезпечення (наприклад, транспорт і системи водоочищення).

### Висновок

Сучасне середовище загроз змінюється таким чином, що вимагає нових видів і рівнів уваги. Критична інфраструктура в країнах-членах НАТО є водночас і ареною геополітичної боротьби, і об'єктом широкої злочинної діяльності. Загроза з боку зовнішньої розвідки ще ніколи не була такою складною і динамічною, як сьогодні. Суб'єкти зовнішньої розвідки розвивають спроможність експлуатувати, підривати або деградувати системи критичної інфраструктури, які лежать в основі глобальних енергетичних і фінансових ринків, телекомунікаційних послуг, урядових функцій і оборонних можливостей. У такий спосіб іноземні спецслужби намагаються впливати на осіб, які приймають рішення, або чинити на них тиск під час кризових ситуацій, ставлячи під загрозу критично важливу інфраструктуру. Порівняно з рештою світу країни- члени НАТО загалом мають величезний привілей сприймати функціонуючу критично важливу інфраструктуру як належне. Чиста вода, надійні дороги, якісна охорона здоров'я, надійне електропостачання, телефони і електронна пошта - все це настільки важливо для сучасного життя на Заході, що неможливо уявити життя без них. Проте події перших десятиліть ХХІ століття демонструють необхідність переоцінки будь-яких припущень щодо безперешкодного доступу до цих послуг. Елементи загрози, швидше за все, плануватимуть уникати збройних сил Альянсу і натомість намагатимуться завдати шкоди тим об'єктам, які погано захищені і можуть завдати найбільшої фізичної і психологічної шкоди. Зловмисники націлені на інфраструктуру, яка підтримує країни-члени НАТО і їхні збройні сили.

Для країн НАТО життєво важливо розуміти природу цих критично важливих об'єктів інфраструктури, притаманні їм вразливості і ризики, а також загрози, з якими вони стикаються. Оскільки нові технології підвищують швидкість операцій, обсяг інформації або своєчасність розробки загальної оперативної картини, можливості суб'єктів загроз пошкодити або зруйнувати критично важливу інфраструктуру також зростають. При впровадженні нових систем або будуючи нові об'єкти критичної інфраструктури, члени і партнери Альянсу повинні постійно оцінювати ризики і вразливості, притаманні цим системам, а також шляхи, якими зловмисники можуть їм загрожувати. Така пильна оцінка допомагає гарантувати, що кожен крок уперед не викриє слабку ланку, яку можуть використати і атакувати групи, що загрожують.

З огляду на мінливе середовище загроз, зацікавлені сторони критичної інфраструктури в приватному і державному секторах та на всіх рівнях влади повинні постійно оцінювати свою безпеку з огляду на спектр фізичних суб'єктів загроз і векторів загроз, з якими вони стикаються. Оцінка загального стану корпоративної безпеки організації та облік нещодавніх інвестицій або змін в організаційній безпеці є ключовими кроками, які необхідно здійснити. Крім того, організації повинні оцінити, наскільки їхня система безпеки відповідає поточним та новим загрозам. Якщо стан безпеки та процедури не відповідають характеру загрози, дуже важливо, щоб організації визначили причину невідповідності та знали, хто з керівників організації відповідає за виправлення такого недоліку в програмі безпеки, і як вони повинні це зробити. Якщо існуючі політики і практики не можуть дати відповіді на ці питання, організаціям критичної інфраструктури необхідно провести огляд і оцінку стану безпеки. Завдяки такому рішучому прагненню оцінювати ризики і загрози і вживати заходів для їх пом'якшення країни-члени і партнери НАТО можуть посилити культуру безпеки і стійкості, необхідну для пом'якшення широкого спектра фізичних загроз критично важливим об'єктам інфраструктури. Такі заходи сприятимуть безпеці і процвітанню окремих країн, а також допоможуть Альянсу в цілому краще виконувати основні завдання НАТО.

# - 3 -

## Кіберзагрози для критичної інфраструктури

Саліх Бічакчі

Ризики для критичної інфраструктури зростають, особливо в кіберпросторі. Хоча пандемія COVID-19 збільшила середню активність домогосподарств в Інтернеті та змусила бізнес впроваджувати практики, що дозволяють працювати віддалено, вона також надала зловмисникам безпрецедентну можливість протестувати системи кібербезпеки та використати вразливі місця. Протягом перших шести місяців пандемії Кіберпідрозділ Федерального бюро розслідувань (ФБР) США повідомив про 400-відсоткове збільшення загальної кількості кібератак порівняно з допандемічним рівнем, а Інтерпол відзначив "тривожний рівень кібератак, спрямованих на великі корпорації, уряди та об'єкти критичної інфраструктури". Пандемія також продемонструвала важливість цифрової інфраструктури для безперервності сучасного життя. Надійна робота систем постачання електроенергії, природного газу, нафти, водопостачання та водовідведення, а також телекомунікацій є життєво важливою для функціонування держави та надання нею основних послуг. У цьому сенсі зацікавлені сторони критичної інфраструктури несуть відповідальність за створення системи кібербезпеки, що впливає н а національну безпеку.

У кіберпросторі переважають дві точки зору: наступальна та оборонна. З оборонної точки зору, відповідальні особи для захисту своїх систем стикаються з великою невизначеністю, оскільки вони намагаються протистояти та пом'якшити складний спектр загроз у кіберпросторі. У певному сенсі наступальний підхід є простішим, оскільки зловмисники зосереджуються виключно на пошуку вразливостей системи, які можна зламати і використати. У цьому розділі пріоритетним є наступальний підхід, а отже, ми розглядатимемо вразливості, ризики та загрози для критичної інфраструктури в кіберпросторі з точки зору супротивника. Для ознайомлення з оборонним мисленням див. главу 14, в якій розглядаються інструменти кібербезпеки та найкращі практики захисту критичної інфраструктури.

Щоб спланувати успішну атаку, зловмисники повинні розуміти природу об'єкта та його відповідні компоненти і взаємозв'язки. З точки зору наступального підходу, кінцева мета полягає в тому, щоб спочатку знайти одну вразливість для отримання доступу до комп'ютерних систем, яку зловмисник згодом використає для підвищення привілеїв у системі. Наступальний менталітет відображає практики безпеки, які широко розповсюджені в природному світі. Наприклад, у природі хижаки використовують два основні інструменти - хитрість і стратегію - для захоплення здобичі.2 У секторі кібербезпеки і пов'язаній з ним літературі одним з корисних прикладів такого наступального мислення є модель Cyber Kill Chain® компанії Lockheed Martin, яка визначає сім кроків, які повинні зробити суб'єкти кіберзагроз для досягнення своїх цілей.3 Спираючись на базу знань про тактику, методи і процедури, які супротивники застосовували під час кібератак, методологія ATT&CK® від MITRE детально описує ці сім кроків у рамках, які ретельно окреслюють можливий підхід супротивника.4 Матриця окреслює фази кібератаки, починаючи з початкового періоду підготовки, що складається з розвідки і озброєння, і продовжуючи ключовими етапами, такими як виконання, наполегливість, ескалація привілеїв, ухилення від оборони і бічний рух.

Оскільки кожна система критичної інфраструктури знаходиться в унікальному операційному середовищі, зловмисники повинні спочатку зрозуміти ландшафт і організацію, на яку спрямована атака. Критичну інфраструктуру можна уявити як колосальний зубчастий механізм, який виконує свою специфічну функцію лише тоді, коли всі шестерні працюють належним чином; тому будь-яка помилка в дизайні чи організації швидко стає вразливим місцем. По-друге, більшість об'єктів і систем критичної інфраструктури належать і експлуатуються приватним сектором. Таким чином, вони, як правило, є бізнес- орієнтованими об'єктами, які повинні працювати в умовах певних економічних обмежень. Нарешті, критична інфраструктура за своєю суттю пов'язана з людським фактором, оскільки об'єкти та системи критичної інфраструктури (1) належать і експлуатуються людським ресурсом і (2) надають основні послуги кінцевим користувачам, тому будь-яке порушення їхньої роботи вплине на повсякденне життя.

У цьому розділі буде надано огляд технічних рівнів і систем критичної інфраструктури, після чого буде розглянуто різні технологічні рівні, а потім обговорено потенційні організаційні вразливості, пов'язані з людськими ресурсами та управлінням. Далі в розділі буде представлено різницю в менталітеті між кібератаками і захисниками, висвітлено різні категорії суб'єктів загрози, а на завершення - огляд нових і нещодавніх основних типів атак, щоб продемонструвати різні підходи, які застосовують суб'єкти кіберзагроз для використання вразливостей в критичній інфраструктурі.

### Технічні шари та структури в критичній інфраструктурі

Інфраструктура - це великомасштабні промислові системи, які взаємозалежно функціонують для виробництва та розподілу основних товарів, таких як енергія, вода та дані, а також послуг, включаючи транспорт, банківські послуги та охорону здоров'я.5 Критична інфраструктура відіграє важливу роль у життєдіяльності суспільства та функціонуванні держави. Огляд взаємозв'язку між секторами життєзабезпечення та іншими секторами критичної інфраструктури див. у розділі 1. Залежно від таких факторів, як географічне розташування, природні ресурси та економіка, держави по-різному визначають, які інфраструктурні системи вони вважають критично важливими. У розділі 12 наведено порівняння секторів, які деякі країни відносять до критично важливої інфраструктури. Наприклад, у нафтовидобувній країні пріоритет захисту нафтопереробних заводів набагато вищий, ніж в інших. Кожен сектор критичної інфраструктури має унікальні вимоги та практики, враховуючи різні послуги та товари, які ці сектори надають. Серед різних типів об'єктів критичної інфраструктури існують відмінності в дизайні, плануванні, функціональності, організації та технічних характеристиках залежно від сектору. Наприклад, конструкція і функції атомних електростанцій помітно відрізняються від телекомунікаційних або водопровідних систем. Для кращого розуміння кібербезпеки об'єктів критичної інфраструктури важливо зазначити, що, незважаючи на описані вище відмінності, системи також мають схожість на організаційному і технічному рівнях, які заслуговують на подальше вивчення.

##### Підключення та технічна складність

За своєю природою критичні інфраструктури є складними, розподіленими системами, що нагадують дерево, коріння якого заглиблене в ґрунт, а гілки знаходяться на видноті. Тому доречніше моделювати взаємозв'язок цих структур як систему систем, яка складається з "множинних, гетерогенних, оперативно розподілених, іноді незалежно функціонуючих систем, вбудованих в мережі на багатьох рівнях, які розвиваються з часом". Складність системи систем впливає як на вимоги до захисту, так і на процедури кризового управління. Існує два основних типи складності, притаманних цим системам критичної інфраструктури. По-перше, рівень взаємозв'язку між системами означає, що будь-яка несправність може створити каскадний ефект серед подібних об'єктів. По-друге, взаємозв'язок також впливає на інші сектори, які не є схожими за своєю природою, але, тим не менш, є залежними. У розділі 12 детально розглянуто каскадні та ескалаційні збої, що виникають внаслідок залежностей і взаємозалежностей між системами критичної інфраструктури. Наприклад, будь-який збій у телекомунікаційному секторі швидко вплине на всі сектори, що залежать від телекомунікацій у своїй роботі. Щоб проілюструвати цю концепцію взаємозв'язку, на рисунку 3-1 показано, як відключення електроенергії в Італії в 2003 році вплинуло на кілька інших секторів критичної інфраструктури в Італії та за її межами.

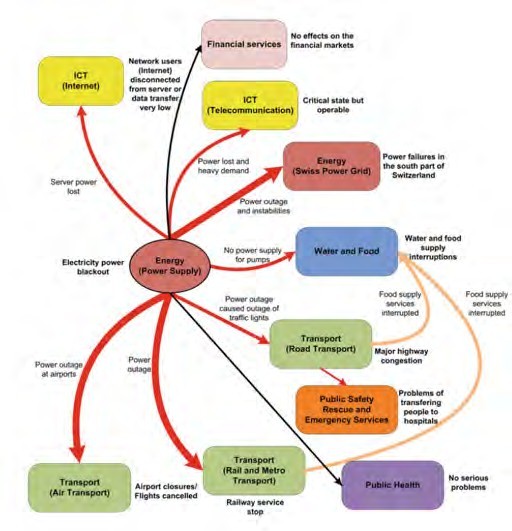


Рисунок **3-1.** Вплив відключення електроенергії в Італії на інші сектори

(Діаграма від Springer)

Складний характер цих залежностей, що збільшує потенціал для виникнення значних криз і каскадних або ескалаційних збоїв, підкреслює необхідність міжсекторальної координації, планування і навчань до того, як відбудуться кібератаки. На жаль, загальний брак співпраці, комунікації та участі в комплексних навчаннях у всіх секторах критичної інфраструктури є вразливістю, якою можуть скористатися зловмисники. Як зазначає один експерт з питань безпеки: складні системи, такі як електромережі, водопровідні мережі, транспортні мережі та мережі зв'язку, мають тенденцію до самоорганізації до критичного стану, і, потрапивши в цей стан, будь- яка зміна в системі може запустити ланцюгову реакцію. Ці ланцюгові реакції проявляються у вигляді каскадних лавин, аварій на атомних електростанціях та колапсів в електромережах. Коли купа піску досягає критичного стану, додавання однієї піщинки може призвести до лавини непередбачуваного розміру - навіть до екстремальних лавин, які повністю знищують купу піску.9

Таким чином, комунікація між державними органами та власниками і операторами об'єктів критичної інфраструктури є важливим елементом політики і практики CISR. Приклади багатовекторного обміну інформацією та координації між державним і приватним секторами див. у главі 11. На об'єкті критичної інфраструктури існує кілька унікальних рівнів функціонування, включаючи бізнес, управління, основне виробництво, ланцюг постачання (треті сторони) та охорону периметру. Для підтримання належної функціональності об'єктів критично важливими є координація та комунікація між цими рівнями. На рівні основного виробництва важливими є два типи технологій: інформаційні технології (ІТ) та операційні технології (ОТ). Хоча в чомусь вони схожі, ІТ та ОТ є достатньо унікальними, щоб вимагати від операторів і захисників певних знань і особливого розуміння для роботи з ними. Інтеграція цих технологій є життєво важливим елементом надійних кіберсистем.

На додаток до операційної складності підключення до мережі, існує часовий вплив на ці об'єкти. Архітектура промислової системи управління (ПСУ) складається з рівнів рішень, процесів іпроцедур. В основі та забезпеченні безперебійної роботи критичної інфраструктури лежить структура ІКС, яка складається з декількох типів систем управління, таких як диспетчерське управління та збір даних (SCADA), розподілені системи управління та програмовані логічні контролери. Характерною рисою Індустрії 4.0 є переважання компонентів Інтернету речей (IoT) у сфері критичної інфраструктури. Збільшення бездротового зв'язку між нелюдськими компонентами також розширює межі протоколів бездротового зв'язку і створює додаткові обов'язки в сфері кібербезпеки.

В управлінні ICS кілька компонентів повинні функціонувати разом, щоб підтримувати роботу критично важливої інфраструктури. Складність ICS полягає в тому, що мережа критичної інфраструктури складається з декількох ІТ- та ОТ- компонентів, виготовлених різними виробниками, які, як правило, мають різний термін служби, не схожі оновлення та різні вимоги до технічної підтримки. Коли власники та оператори критичної інфраструктури визначають пріоритети

В умовах переважання функціональності та продуктивності над безпекою компонентів ІКС ризики кібербезпеки в екосфері критичної інфраструктури зростають. Таким чином, коли йдеться про впровадження політики CISR та забезпечення безперервної роботи об'єктів критичної інфраструктури, керівник служби безпеки об'єкта відіграє вирішальну роль у зменшенні вразливостей, ризиків та загроз у кіберпросторі. Компоненти ІКС не є загальнодоступними пристроями або компонентами, тому їх атака вимагає від зловмисників глибоких знань про ці компоненти - реальність, яка зменшує кількість супротивників, що володіють необхідним ступенем специфічності для атаки на компоненти ОТ. З іншого боку, атаки, спрямовані на компоненти ІКС, здебільшого походять від передових груп постійних загроз або груп, що мають державну підтримку.

Структура ICS, побудована з компонентів різних постачальників, вимагає ретельного планування для інтеграції необхідних оновлень, модернізацій та виправлень безпеки, а також для забезпечення того, щоб цей процес оновлення не заважав загальному функціонуванню системи. Оскільки важко передбачити, як будуть функціонувати різні компоненти після завершення процесу оновлення, особи, відповідальні за ці оновлення, можуть не наважуватися впроваджувати будь-які зміни, які можуть загрожувати здатності системи працювати так, як це було заплановано. Як наслідок, компоненти SCADA та ICS, які забезпечують роботу критично важливої інфраструктури, часто не отримують більшість оновлень та виправлень безпеки, яких вони потребують.

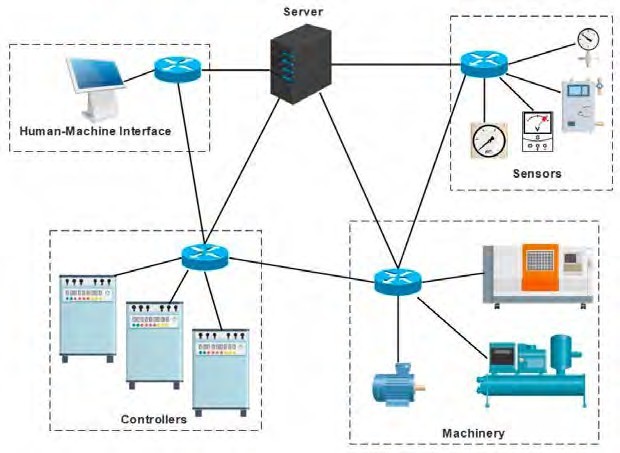
##### Технологічні шари**:** Інформаційні технології**,** Операційні технології та промисловий Інтернет речей

Функціональність різних комп'ютерних протоколів в межах певної критичної інфраструктури підвищує продуктивність системи, але ускладнює безпеку. ІТ-системи та системи оперативного управління в основній виробничій зоні критичної інфраструктури з'єднані та синхронізовані для підтримки виробництва або обслуговування об'єкта. Як випливає з назви, розробники OT мають на увазі здатність виконувати певні дії, що забезпечують безперервність роботи критичної інфраструктури. Як наслідок, під час операційного проектування систем OT пріоритетом є функціональність, а не безпека. Інженери, в принципі, не підключають системи ОТ безпосередньо до Інтернету на етапі проектування, а використовують брандмауери, щоб відокремити системи ОТ. Оскільки інформаційні технології зосереджені на комп'ютерних і телекомунікаційних системах, які виконують введення, зберігання, відновлення, передачу, обробку і захист даних, вони ставлять на перше місце дані і належні процедури роботи з ними. Інновації в ІТ-сфері швидко змінюються і вдосконалюються, і більшість ІТ-інфраструктур можуть швидко прийняти і впровадити останні технологічні досягнення без особливих зусиль. У критичній інфраструктурі ІТ-мережа є основою для бізнес-рівня та рівня підприємства, тоді як тісний взаємозв'язок між ІТ- та OT-системами в основній виробничій сфері є важливою вразливістю.

55

У 1980-х роках операційні та ІТ-системи функціонували переважно незалежно один від одного. У 1990-х роках системи ОТ почали підключатися до ІТ-систем для централізації управління. У 2000-х роках інженери ОТ створили сумісні з ІТ-системами системи, щоб поліпшити комунікаційні проблеми між двома системами. Таким чином, у мережах почали розмиватися межі між ІТ- та ОТ-системами. Сьогодні системи OT також співпрацюють з хмарними обчисленнями та бездротовими технологіями.

Простіше кажучи, операційна технологія - це обчислювальна потужність для виконання операцій і моніторингу пристроїв, різних промислових процесів і деяких галузевих подій. Типова мережева архітектура для промислових систем OT показана на рисунку 3-2. Системи OT виконують важливі функції, включаючи управління виробничими лініями, контроль гірничодобувних операцій і моніторинг нафти і газу. Операційна технологія надає пріоритет процесам, необхідним для підтримання функціонування системи, тому підвищення доступності, точності та надійності послуг наземної обробки даних має важливе значення. У секторі критичної інфраструктури системи OT регулярно контролюють процеси і підтримують виробничі та оборонні підприємства.



Малюнок **3-2.** Типова мережева архітектура промислових систем ОТ

(Діаграма за прикладними науками)

На відміну від більшості ІТ-систем, які суворо контролюються і регулюються системними адміністраторами, системи відкритого доступу, як правило, не мають таких обмежень чи правил доступу. Щоб захистити функціональність систем відкритого доступу, вони не повинні бути настільки ж доступними, як ІТ- системи. Порівняно з ІТ - системами, ОТ-системи набагато складніше відновлювати і відновлювати в разі збою, і будь-який збій в ОТ-мережі може призвести до катастрофічних наслідків або до сценарію "кінця життя".

З часом ОТ-системи поступово стають більш захищеними, хоча цей прогрес не відповідає значним зусиллям, спрямованим на захист ІТ-систем. За умови обмеженого оновлення прошивки, підтримуваний термін служби компонентів ОТ становить від 10 до 20 років. На противагу цьому, апаратне, програмне забезпечення та протоколи ІТ-систем швидко змінюються. Ця різниця в темпах і типах змін між цими двома системами створює проблеми сумісності та комунікації. Технологічні зміни в ІТ- та ОТ-системах можуть поставити під сумнів здатність операторів критичної інфраструктури адаптуватися до змін та керувати процесом встановлення оновлень і патчів. З огляду на ці виклики, об'єкти критичної інфраструктури потребують стратегічних планів для управління цим процесом і забезпечення належного поєднання модернізації системи безпеки з безперервною роботою бізнесу.

Значним сегментом систем ОТ є архітектура ICS, яка складається з систем, що здійснюють моніторинг та управління промисловими процесами за допомогою програмованих логічних контролерів або дискретних систем управління технологічними процесами. SCADA-системи, які відповідають за управління ІКС, мають два основних компоненти. Перший - це людино-машинний інтерфейс. Другий - історик, який забезпечує графічний інтерфейс користувача, щ о дозволяє операторам легко спостерігати за станом системи, отримувати будь-які сигнали тривоги, що вказують на роботу за межами діапазону, або вводити системні налаштування для управління контрольованим процесом. На додаток до SCADA, ключові програми в категорії систем OT включають комп'ютерне числове програмне забезпечення, системи управління будівлями та системи автоматизації будівель. Системи OT також мають власні протоколи зв'язку, які відрізняються від тих, що використовуються в ІТ-системах. Системи OT також часто використовують віддалені термінальні пристрої (RTU) для підключення одного або декількох пристроїв (виконавчих механізмів і моніторів) для управління або моніторингу процесу з безпосередньої близькості або за тисячі кілометрів від штаб- квартири.

Окрім систем ІТ і ОТ, новітнім елементом, що впливає н а роботу і кібербезпеку критичної інфраструктури, є Індустрія 4.0, яка дозволяє об'єднати в інтелектуальну мережу машини і процеси для підвищення ефективності. Промисловий Інтернет речей (IIoT) відноситься до використання Інтернету речей у промислових секторах, і це дає змогу застосовувати міжмашинну взаємодію та штучний інтелект у кількох категоріях. Хоча і не без ризиків, ці міжмашинні додатки можуть спростити складні виробничі або контрольні процеси. У критично важливих інфраструктурах основна відмінність між пристроями IIoT лежить на перетині рівнів ІТ і OT. IIoT також може оптимізувати прозорість ланцюга поставок і логістики, використовуючи розумні датчики і виконавчі механізми. Така мережева структура може також підвищити рівень знань і розуміння спільнотою безпеки OT своїх мереж.11 У середовищі OT завдання полягає в тому, щоб визначити, чи є проблема незвичайним інцидентом, що виник в результаті атаки, або просто базовою помилкою в програмному забезпеченні.

##### Соціальна складність та соціально**-**технічні структури

У той час як технічна складність комп'ютерних систем є предметом вивчення протягом багатьох років, концепція соціальної складності є унікальною і порівняно новою. Традиційне розуміння безпеки зосереджується на захисті нелюдських компонентів в зоні операції і розглядає автоматизацію як ідеальний інструмент для контролю всіх можливих наслідків. Автоматизація та обмеження нелюдських компонентів вимагають менше зусиль, ніж боротьба з соціальною непередбачуваністю. Проблема полягає в тому, що критична інфраструктура є бізнес-орієнтованим сектором послуг і повинна співпрацювати з кількома сторонніми партнерами. Можна використовувати автоматизацію як засіб мінімізації людської робочої сили, але не без того, щоб не наражати критичну інфраструктуру на інші вразливості. Сучасний підхід до соціальної складності, однак, розуміє всю мережу і її людські та автоматизовані компоненти в межах об'єкта. Інженери, разом з їхніми мобільними телефонами, картками доступу, токенами і серверними кімнатами, повинні розглядатися з точки зору мережевого мислення. Така перспектива покаже, скільки компонентів пов'язані між собою, і продемонструє рівень складності об'єкта.

Акторно-мережева теорія (АМТ) розуміє кожен елемент як вузол у певній організації або структурі.

Аналіз критичної інфраструктури в мережевому режимі може допомогти рівню захисту легше побачити і оцінити вразливості і слабкі місця, даючи підказки про специфічні взаємодії між різними елементами об'єкта. Підхід ANT також може представити цілісний погляд на безпеку критичної інфраструктури. Коли зловмисник вирішує атакувати певний об'єкт критичної інфраструктури, наступним кроком буде пошук вразливостей, які можна використати і таким чином отримати початковий доступ до системи. Зловмисники переслідують цю мету за допомогою апаратних доповнень, довірчих відносин, реплікації через знімні носії та зовнішні віддалені сервіси. У цьому контексті крадіжка мобільного пристрою інженера або несанкціонований доступ до облікових записів віртуальної приватної мережі менеджера можуть швидко стати вразливими місцями, які ставлять під загрозу функціональність всієї системи. Практика ANT також може допомогти операторам критичної інфраструктури та командам кібербезпеки визначити потенційні наслідки, якщо і коли вони трапляться.

Крім того, тимчасові зміни також можуть впливати на системи критичної інфраструктури. Бувають випадки, коли економічні та політичні міркування або стихійні лиха змушують операторів об'єктів критичної інфраструктури на певний час розширювати виробничі потужності об'єкта, щоб задовольнити нові потреби в послугах. Бувають також ситуації, коли об'єкт спочатку перебуває у державній власності, але потім переходить під управління приватного сектору, або коли планування об'єкта змінюється з таких причин, як реконструкція чи додаткове будівництво. Висока плинність кадрів на таких об'єктах може вплинути на наявність необхідних експертних знань для забезпечення ефективної роботи, навіть якщо нові працівники мають у своєму розпорядженні конкретні креслення і записи.

У більшості критично важливих об'єктів інфраструктури характер операцій, а саме безперебійне обслуговування, означає знижену видимість і контроль під час функціонування системи. Об'єкти, як правило, координують свої виробничі потужності з об'єктами в натуральному вираженні, щоб організувати розподіл продукту, якого потребують споживачі. Електропостачання, водопостачання, каналізація та телекомунікації переважно працюють за схожими принципами. З точки зору організаційної структури, об'єкти критичної інфраструктури в основному поділяються на дві частини: (1) виробничі підприємства та управлінська ланка, а також послуги та лінії розподілу. До першої категорії відноситься різне обладнання та інструменти обмежують фізичний доступ до об'єкту, де відбувається виробництво. Усередині заводу команди фізичної та кібербезпеки працюють над контролем будь-яких аномалій, щоб запобігти порушенням, а оператори стежать за датчиками, щоб керувати роботою об'єкта. У другій категорії розподільчі лінії та служби мають обмежений захист від будь-яких загроз, оскільки поверхня атаки є значною через їхні величезні розміри. У деяких секторах безпека цих різних ліній та послуг залежить від таких незначних речей, як накладка на замок або захищений ящик, щоб утримати потенційного супротивника від нападу на систему або націлити його на неї. Експерт може легко використати ці вузли, щоб завдати шкоди або вивести з ладу критичну інфраструктуру і послуги, які вона надає.

Наприклад, багато електроенергетичних і телекомунікаційних компаній використовують службові легкові та вантажні автомобілі, які зазвичай залишаються припаркованими в гаражі підприємства під обмеженою охороною по периметру або спостереженням у неробочий час. З точки зору бізнесу, ці компанії шукають економічно ефективні засоби для роботи та зберігання обладнання. Однак такий мінімальний рівень безпеки дає можливість зловмисникам вести ворожу розвідку або отримати ідентифікаційні значки, робочі жилети, шоломи, а в деяких випадках навіть робочі комп'ютери чи спеціальні інструменти. Невід'ємною вразливістю об'єктів з такою розгалуженою мережею є складність забезпечення постійного захисту всього персоналу, приміщень та обладнання. Розширення мережі, що збільшує площу атаки, також є життєво важливим фактором при плануванні та здійсненні КІСР.

### Пошук прогалин на рівнях управління організацією та бізнесом

##### Людський капітал**,** культура та безпека

У критичній інфраструктурі людський фактор є одним з найважливіших чинників функціонування системи та її ефективної роботи. На початкових етапах планування і розбудови критичної інфраструктури пріоритетними зазвичай є деталі, пов'язані з безпекою периметру, цифровою безпекою та операційною безпекою, і порівняно менше уваги приділяється необхідним інвестиціям у людський фактор. Більшість ключових концепцій безпеки, таких як ситуаційна обізнаність, стратегічні комунікації, підозрілість, стійкість і культура безпеки, фундаментально пов'язані з людським капіталом критичної інфраструктури: людьми, які володіють, керують і експлуатують систему. Адже навіть найсучасніші системи нічого не варті без кваліфікованої робочої сили.

Деякі дослідники визначають людський компонент як одну з взаємозалежностей критичної інфраструктури.

Розуміння людського виміру персоналу, як під час виконання службових обов'язків, так і поза ними, має важливе значення для ефективної практики КІСВ. На більшості об'єктів критичної інфраструктури персонал поділяється на три основні категорії: технічний, нетехнічний та управлінський. У кожній категорії ці підпорядковані команди використовують свої унікальні навички та можливості, а також співпрацюють для досягнення спільної мети. Таким чином, кожна команда розвиває власну робочу культуру, тоді як вся організація також будує культуру безпеки, спрямовану на зменшення загроз і підвищення стійкості. Відділ людських ресурсів (HR) - це підрозділ, який в першу чергу відповідає за розуміння та організацію робочої сили. На практиці, однак, відділи кадрів зосереджуються в основному на перевірці біографічних даних, а не на розумінні індивідуальних відмінностей працівників, які можуть сприяти або перешкоджати співробітництву, що є ключовими елементами загальної системи безпеки. Однією з вразливостей, притаманних об'єктам критичної інфраструктури, є брак ситуаційної обізнаності, тобто "знання того, де ви знаходитесь, де знаходяться інші дружні елементи, а також статус, стан і місцезнаходження ворога". У цьому визначенні є три рівні ситуаційної обізнаності:

(1) сприйняття критичних факторів у навколишньому середовищі,

(2) розуміння значення цих факторів, особливо у поєднанні з цілями особи, яка приймає рішення,

(3) передбачення того, як ці фактори впливатимуть на систему в найближчій перспективі.

Налагодження співпраці між елементами трудового колективу вимагає особливої координації та комунікативних навичок, які є основою ситуаційної обізнаності. Часто відділ кадрів найкраще підходить для того, щоб докладати зусиль для покращення організаційної культури, комунікацій та співпраці. Без цілеспрямованих зусиль, спрямованих на покращення співпраці між підрозділами та їхнім персоналом, в організації можуть утворитися прогалини або "сліпі зони", що призведе до вразливостей, якими легко скористаються вороги.18 Зусилля, спрямовані на побудову нормальних, здорових комунікацій і співпраці між відділами, можуть запобігти формуванню відомчих субкультур на шкоду організаційній культурі та покращити загальний стан КІСР в організації.

Більшість організацій мають "червоні команди", які слугують для перевірки стану безпеки організації та пошуку способів проникнення на об'єкт фізичними або кібернетичними методами. У реальному прикладі члени "червоної команди" можуть використовувати жилет компанії, каску або фальшивий ідентифікаційний бейдж і підійти до входу як субпідрядник або команда технічного обслуговування сторонніх послуг. У цій спробі "червона команда" може використовувати достовірні і точні дані, отримані різними методами, щоб переконати охоронця дозволити в'їзд. Будь-яка відсутність координації між відділами - наприклад, неповідомлення служби безпеки про загублену ідентифікаційну картку або вкрадену уніформу - може дозволити справжньому зловмиснику , а не лише члену "червоної команди", отримати доступ до об'єкту. Для побудови надійної культури та системи безпеки відділи кадрів можуть сприяти зміцненню довіри між працівниками, забезпеченню відкритого спілкування та покращенню координації. Розширення прав і можливостей окремих працівників і створення сильної організаційної культури сприяє підвищенню особистої відповідальності і заохочує персонал брати на себе відповідальність за умови на об'єкті, в тому числі за безпеку. Аналогічну концепцію викладено в розділі 6, присвяченому обговоренню спільнот безпеки в аеропортах. Якщо не врахувати ці відмінності між підрозділами, це може призвести до вразливостей і збоїв, якими можуть скористатися "червоні команди" або реальні суб'єкти загрози, використовуючи методи соціальної інженерії.

Зрештою, за організаційну культуру та безпеку на об'єкті відповідає керівництво. Власники та керівники повинні вживати заходів для підвищення довіри та співпраці між підрозділами, а також заохочувати культуру, в якій працівники можуть робити свій внесок у процес прийняття рішень і, за необхідності, брати в ньому участь. Ці зусилля можуть залучити людський капітал організації та заохотити працівників повідомляти про проблеми, коли вони виникають, особливо з точки зору безпеки. Такий підхід до участі також уможливить управління змінами і полегшить процес адаптації, необхідний для вдосконалення політики і практики КІСР.

##### Управління бізнесом та координація у сфері критичної інфраструктури

Бізнес-сектор є одним з центральних у критичній інфраструктурі. Оскільки багато секторів критичної інфраструктури перебувають у приватній власності - а отже, отримують прибуток від своїх послуг - бізнес-мислення іноді переважає над основними практиками безпеки та захисту. Окрім координації та комунікації всередині організації, керівництво також відповідає за налагодження безпечної та здорової комунікації із зовнішніми регулюючими органами для забезпечення безперервної роботи об'єкта. Ці комунікації також включають заходи з обміну інформацією та розвідувальними даними щодо можливих загроз. Про багатовекторний обмін інформацією та розвідданими див. розділ 11. На Рисунку 3-3 показано роль і ключові зв'язки бізнес- рівня в організації та за її межами .

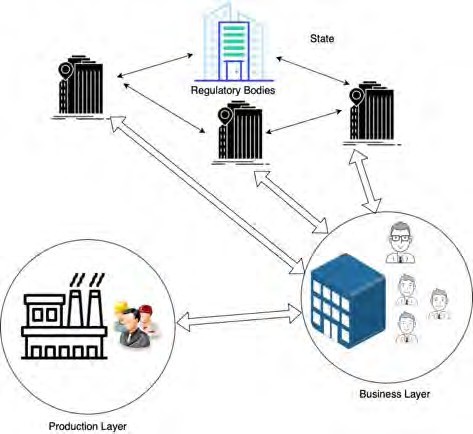


Рисунок **3-3.** Роль бізнес**-**рівня

Бізнес-рівень також відповідає за управління ефективною діяльністю установи перед обличчям таких загроз, як кібератаки. Однією з найбільш корисних інвестицій, яку можуть зробити менеджери, є проведення регулярних раптових навчань для підготовки співробітників, посилення співпраці та мінімізації наслідків кібератаки. Такі вправи дають змогу працівникам відчути певну невизначеність і стрес реальної кібератаки, прищеплюють правильні реакції, покращують процес прийняття рішень і роблять таку поведінку більш природною для них. Вправи також можуть виявити когнітивні упередження працівників, зокрема, надмірну впевненість у дружніх можливостях і недооцінку загроз для систем організації. На жаль, плинність кадрів , вимоги повсякденного бізнесу і сприйняття навчань як надто деструктивного явища в сукупності обмежують проведення цих цінних навчань і переваги, які вони можуть принести. Якщо бізнес-верства сліпо довіряє технологічним інвестиціям та ігнорує людський компонент у цих соціо- технологічних системах, то організація стає більш вразливою до руйнівних кібератак.

Нарешті, бізнес-рівень є центром управління ініціативами з управління змінами. Хоча бізнес-менталітет чинить опір змінам, які можуть порушити роботу об'єкта, оновлення цифрових компонентів є важливим для кібербезпеки критичної інфраструктури. Факти свідчать про те, що впровадження необхідних змін, як правило, приносить значні переваги об'єктам критичної інфраструктури і переважає витрати на модернізацію. Щоб допомогти вищому керівництву ініціювати і підтримувати значні зміни, життєво важливо визначити ролі і обов'язки різних рівнів організації і працівників різних департаментів. Виконавчі лідери також повинні краще розуміти технічний рівень, щоб керувати об'єктом під час кризових ситуацій і пом'якшувати ймовірні загрози.

### Умонастрої та загрози Дійові особи

##### Різниця в менталітеті**:** Нападники та захисники

Успішні зусилля із забезпечення безпеки ґрунтуються на трьох ключових компонентах: (1) запобіжні заходи для охорони і захисту проекту і структури, (2) датчики і сигналізація для оповіщення систем у разі порушення або будь-якої зловмисної діяльності, і (3) людський потенціал. Навіть якщо критично важлива інфраструктура спроектована бездоганно і здатна виявити будь-яку аномалію, лише людський фактор - менеджери, оператори і весь персонал - можуть визначити відповідні заходи реагування у разі виникнення проблем. Загрози, які зловмисні кіберактивісти створюють для критичної інфраструктури, є комплексними, як показує ця аналогія:

Сьогоднішнє середовище кібербезпеки схоже на одночасну гру в шахи в 1000 партій з різними супротивниками різного рівня майстерності. Якщо проти 98% гравців молодшого рівня (скриптових дітей) захистити дошку нескладно, то 2% найкращих вимагають справжніх зусиль і стратегії.

У сфері безпеки критичної інфраструктури правила гри в кіберпросторі визначаються наступальним і оборонним мисленням. Захисники не знають, хто атакуватимуть систему, коли вони це зроблять і як вони це зроблять. Оскільки вектор загрози не є очевидним, захисники повинні 24 години на добу підтримувати пильну увагу у всіх відповідних сферах захисту, а до будь-яких сигналів слід ставитися з особливою обережністю через невизначеність загрози. Захисники виконують роботу, яка часто повторюється, не знаючи, чи приносять їхні зусилля позитивні результати, і яка може стати настільки рутинною, що захисники відволікаються і втрачають фокус на ознаках ворожої активності. Місія кіберзахисту не приносить негайного задоволення і не є добре зрозумілою для операторів і керівників об'єктів критичної інфраструктури. На папері легко підтримувати такі зусилля, але насправді кіберзахист протягом тривалого періоду часу є складною місією. З іншого боку, зловмисники мають певну мету, мотивацію для досягнення успіху і час, щоб випробувати всі можливі способи досягнення бажаного результату. Протягом усього процесу вибору мішені та атаки зловмисники зацікавлені, зосереджені та уважні до деталей, які дають їм змогу знайти та використати вразливості системи. Зловмисники, як правило, не схильні до спокус сірості або рутини, з якими стикаються захисники; навпаки, наступальний менталітет характеризується сильною мотивацією до подолання перешкод.

Хоча тренування і навчання відіграють важливу роль у розвитку безпеки і стійкості критичної інфраструктури, реальне моделювання потенційних зловмисників є непростим завданням. Як своєрідні "адвокати диявола", "червоні команди" відіграють вирішальну роль у демонстрації можливих наслідків ворожих атак. Тести на кібер- та фізичне проникнення, які проводять червоні команди, в першу чергу спрямовані на рівень управління об'єктом і зосереджуються переважно на питаннях, які можуть призвести до порушення нормальної роботи підприємства. Часто "червоні команди" інформують відповідні сторони до початку імітації атаки, і вони зобов'язані дотримуватися певних етичних правил при проведенні атаки. Тут дотримання етики і демонстрація справжньої психології атаки є взаємовиключними, оскільки реальні зловмисники не мають жодного етичного кодексу, який вони повинні враховувати або якому вони повинні підкорятися. Цю подвійність безпекового мислення неможливо легко змінити за допомогою звичайних інструментів. В епоху гібридності та асиметрії зловмисники мають кілька переваг над захисниками. Однією з вирішальних переваг для зловмисників є вертикальна ієрархія державного сектору або державних систем критичної інфраструктури. Зіткнувшись з аномалією або атакою, захисники об'єкту, на який спрямована атака, повинні проінформувати кілька управлінських груп, а вище керівництво об'єкту - повідомити державні органи влади для ліквідації наслідків такої атаки. Однак будь-яка атака вимагає швидкого реагування та оперативних дій, щоб забезпечити продовження роботи об'єкту.

##### Загроза Дійові особи

Для тих, кого атакують, фундаментальним і природним питанням є: "Хто зловмисник?". Демонструючи звичайне і традиційне розуміння кіберзагроз, література з кібербезпеки окреслює конкретні категорії зловмисників і визначає хакерів, кракерів, ламерів, скриптових дітлахів і вовків-одинаків як основних суб'єктів загрози. Хоча суб'єкти цього спектру відрізняються за своїми можливостями, ці окремі категорії вже не є актуальними, оскільки сьогодні "питання знання повного імені зловмисника стає менш актуальним, ніж знання того, хто є ворогом і хто є спонсорами, наприклад, державний суб'єкт або терористична організація".

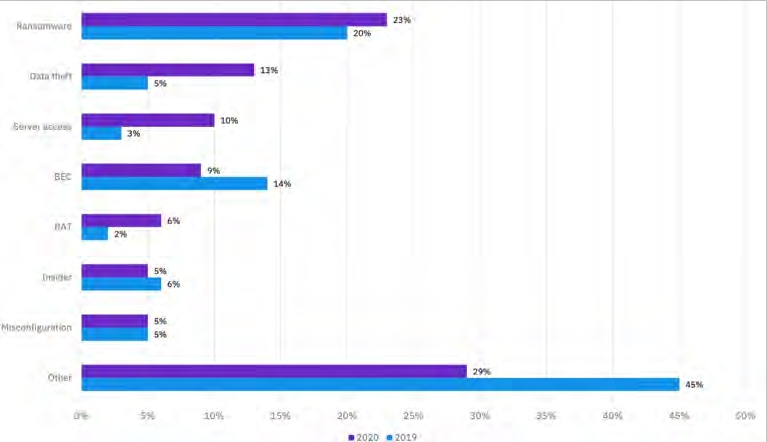
З огляду на складні мережі, унікальні організаційні структури та роль у підтримці сучасного життя, критичні об'єкти інфраструктури відрізняються від інших типів цілей. Дослідники вказують на зростаючу тенденцію низькотехнологічних атак на об'єкти критичної інфраструктури, зокрема, на об'єкти інфраструктури зв'язку та Інтернет-мережі, які здійснюються аматорами, що не мають досвіду і глибоких знань у цьому секторі. В одному з таких прикладів зловмисники стверджували, що успішно проникли в німецьку систему управління залізницями, але насправді вони лише скомпрометували веб- інтерфейс для набору моделей поїздів. Незважаючи на такі невдачі аматорів, широке коло суб'єктів загроз прагне атакувати критичну інфраструктуру, причому всі вони мають різні рівні спроможності та мотивації. Загальний профіль потенційних зловмисників включає наступні групи.

* Опортуністичні зловмисники. Ці зловмисники не мають конкретної мети, але намагаються поширити своє шкідливе програмне забезпечення якомога ширше, щоб збільшити шанси на успіх.
  + Промислові опортуністичні зловмисники. Різновид опортуністичних зловмисників, які націлені, зокрема, на промисловий сектор. Ці зловмисники намагаються використати будь-яку атаку нульового дня або оголошену вразливість, щоб застати свою ціль зненацька, доклавши відносно невеликих зусиль.
  + Конкуренти. Ці зловмисники націлені на викрадення інфраструктурних даних, таких як креслення або технічна інформація. У цих подіях часто беруть участь міжнародні конкуренти з цього сектору або національні спецслужби, які практикують кібершпигунство, і розрізнити ці дві сторони досить складно.
  + Інсайдерські загрози. Ці зловмисники - нинішні або колишні незадоволені співробітники, які здійснюють свої атаки з різних причин.
  + Просунуті постійні загрози. Ці групи зловмисників можуть організовувати широкомасштабні, складні атаки, які відстежуються спільнотою безпеки, але їх важко зупинити.2 Ці висококваліфіковані зловмисники можуть бути державними суб'єктами, які мають намір здійснити кіберсаботаж або спричинити хаос у країні-цілі, порушивши або зупинивши роботу сервісу.
  + Хактивісти. Ці зловмисники переслідують ідеологічні цілі, які легітимізують їхню атаку. Вони зацікавлені не в результатах, а в просуванні своєї ідеологічної позиції шляхом підриву організації- мішені.

Власники та керівники об'єктів критичної інфраструктури можуть також використовувати просту шкалу для оцінки можливих рівнів кіберзагроз об'єкту - наприклад, від одного (нескладний) до п'яти (складний) - щоб визначити відповідний рівень загрози, від якого вони планують захищатися. Визначення відповідного рівня захисту дозволяє командам з управління критичною інфраструктурою калібрувати свої заходи кібербезпеки відповідно до рівня загроз, з якими вони стикаються. Зрештою, цей крок дає керівникам краще розуміння їхньої спроможності захиститися від кібератак, допомагає їм здійснити необхідну підготовку та інвестиції, а також спрямовує їхнє реагування, якщо атаки перевищують прогнозований рівень загрози.

**Поточні та нові кіберзагрози**

Щороку з'являються нові вектори атак або способи дій для загроз, які позначають епоху. Існують також загальні методології, які зловмисники вважають за краще практикувати, і які стають все більш популярними. Ця реальність означає, що більше інструментів для атак стають доступними для більшої кількості потенційних зловмисників завдяки простому і швидкому пошуку в Інтернеті. На додаток до основних засобів кібербезпеки, вкрай важливо розуміти ландшафт загроз, щоб захистити мережі та посилити позиції CISR. Звіт IBM 2021 Security X-Force, який відображає найпоширеніші типи кібератак у 2019-20 роках, демонструє зростання використання програм-вимагачів, троянів для віддаленого доступу та компрометації ділової електронної пошти за останні кілька років (див. рис. 3-4).32 Крім того, зловмисники н а д а ю т ь перевагу крадіжкам даних, які також пов'язані з фішингом і соціальною інженерією, особливо під час підготовки до більш складних атак. Серед цих різноманітних типів атак у цьому розділі ми розглянемо використання п р о г р а м - в и м а г а ч і в , компрометації ділової електронної пошти, підміни облікових даних та атаки на ланцюги поставок проти об'єктів критичної інфраструктури.



**Рисунок 3-4. Розподіл кібератак за типами, 2019-20 (**(Діаграма від IBM)

##### Програми**-**вимагачі

Програми-здирники - це не просто шкідливе програмне забезпечення, яке націлене на дані користувача, це поєднання двох понять: "викуп" і "програмне забезпечення" . По- перше, *ware* - це шкідливе програмне забезпечення, яке дозволяє програмам-здирникам шифрувати всі дані в зараженій комп'ютерній системі за допомогою різних рівнів асиметричного шифрування. По-друге, вимога *викупу вказує на* цілеспрямовану кампанію та конкретний бізнес-план програми-здирника, спрямований на утримання даних жертви в полоні та їхнє звільнення лише після отримання платежу. Дослідження показують, що у 2021 році підприємства приватного сектору зазнавали атаки з використанням програм-вимагачів кожні 11 секунд, порівняно з однією атакою кожні 40 секунд у 2016 році.33

Програми-здирники з'явилися на ринку з 1989 року. Того року Джозеф Л. Попп (Joseph L. Popp) здійснив першу в історії атаку з використанням вірусу-вимагача, розповсюдивши 20 000 дискет, які нібито містили інформацію про СНІД, серед учасників Міжнародної конференції зі СНІДу, організованої Всесвітньою організацією охорони здоров'я Троянська програма зашифрувала імена файлів на комп'ютері замовника і приховала каталоги, а потім вимагала 189 доларів США за доступ до файлів. Етапи атак вірусів-здирників, такі як шифрування і вимога викупу для відновлення доступу, по суті, залишилися незмінними з часом, хоча методологія розповсюдження змінилася. Сьогодні програми-вимагачі мають високу ймовірність успіху при відносно низьких шансах бути виявленими. Як наслідок, програми-вимагачі стали інструментом, який обирають зловмисники, щоб заробляти гроші, докладаючи обмежених зусиль. Кількість кампаній з використанням програм-вимагачів проти об'єктів критичної інфраструктури зросла з 2019 року і прискорилася під час пандемії COVID-19 (див. рис. 3-5).34

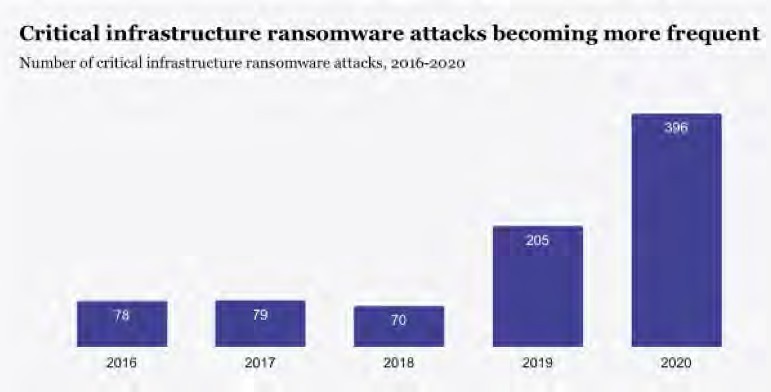


Рисунок **3-5.** Зростання кількості атак на критично важливу інфраструктуру з використанням програм**-**вимагачів

(Діаграма Університету Темпл)

Нещодавній приклад масштабної атаки з використанням програм-вимагачів стався 7 травня 2021 року на компанію Colonial Pipeline, одного з провідних американських операторів нафтопроводів і джерела палива для східної частини Сполучених Штатів. Атака зупинила роботу трубопроводу, спричинила дефіцит пального та панічний попит на заправках по всьому регіону, а також призвела до затримок запланованих авіарейсів. Атака на Colonial Pipeline - це перший випадок, коли кібератака з використанням програмного забезпечення з вимогою викупу зачепила таку велику кількість людей у їхньому звичному повсякденному житті. Успіх атаки Colonial Pipeline та нещодавня тенденція до зростання вказують на те, що атаки з використанням програм-вимагачів залишаться в майбутньому. Тому важливо розуміти природу атак з вимогою викупу, щоб посилити позиції CISR та підготуватися до таких атак. На Рисунку 3-6 наочно показано життєвий цикл атаки з використанням програм-вимагачів та основні етапи, які він охоплює.

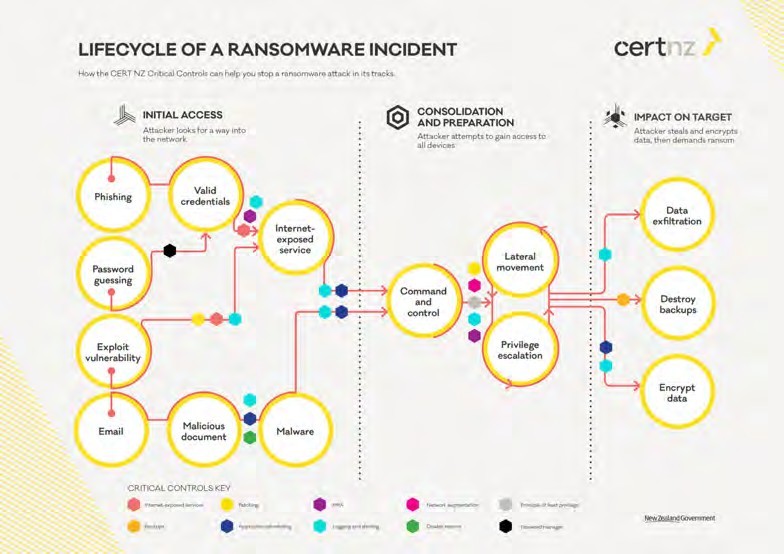


Рисунок **3-6.** Життєвий цикл атаки вірусу**-**здирника

(Діаграма від CERT NZ)

Хоча на рис. 3-6 кампанія з вимагання розділена на три етапи - початковий доступ, консолідація та підготовка, а також вплив на ціль - ця модель не враховує процес переговорів. Щоб зрозуміти інцидент з використанням програми-вимагача від початку до кінця, корисно розглянути шість основних етапів, які складають життєвий цикл атаки, що має багато спільного з кіберланцюгом вбивств, про який йшлося раніше в цій главі.

Першим кроком атаки з використанням програм-вимагачів є кампанія розповсюдження, під час якої зловмисники шукають потенційних жертв, до яких можна проникнути відносно легко і з мінімальними витратами часу та зусиль. Суб'єкти кіберзагроз використовують кілька методів для пошуку відповідних цілей, наприклад, індексацію вразливостей у пошукових системах. Наприклад, зловмисники, які використовують Shodan - пошукову систему для пристроїв, підключених до Інтернету - або подібні програми для сканування Інтернету, можуть знайти потенційні цілі. На першому етапі зловмисник намагається заразити ціль шкідливими файлами (корисним навантаженням) кількома способами, такими як фішингова атака, атака "водопою", використання набору експлойтів або автоматичне завантаження.

Другий етап, проникнення та інсценування, починається, коли зловмисник знаходить способи доступу до цільової мережі. На цьому етапі зловмисник намагається зрозуміти мережу та обмеження свого облікового запису. Пізніше зловмисник використовує стелс і маскує виконувані програми, щоб краще зрозуміти обстановку. Етап підготовки в основному пов'язаний з перевіркою локальних конфігурацій і пошуком ключів реєстру для різних прав і налаштувань проксі-серверів, привілеїв користувачів і доступності. Зловмисники обережно використовують інструменти аналізу інтернет-протоколів, щоб зрозуміти можливості цілі.

Після проникнення та інсценування настає третій етап - сканування, на якому зловмисники зосереджуються на деталях, які забезпечать успіх атаки. Усі ІТ- та ОТ-системи мають свої особливості, але бізнес-моделі та галузеве програмне забезпечення, в якому вони працюють, можуть змінювати налаштування. Зловмисники перевіряють структуру резервного копіювання та критично важливі файли, щоб зупинити бізнес- активність, а також перевіряють фінансовий стан жертви, щоб визначити суму викупу. Нарешті, зловмисники намагаються отримати адміністративні привілеї, щоб контролювати системи безпеки, такі як інструменти управління інформацією та подіями безпеки, системи виявлення та реагування на кінцеві точки та платформи віртуалізації.

На четвертому етапі, шифрування, зловмисники шифрують файли жертви в пріоритетному порядку, непомітно для антивірусного програмного забезпечення. Зазвичай зловмисники надають пріоритет файлам, які використовуються в щоденних операціях, оскільки ці файли, як правило, є важливими для безперервності бізнесу. Оскільки шифрування - це гонка з обмеженим часом, яку зловмисники намагаються завершити якомога швидше, щоб запобігти використанню резервних копій для відновлення системи, вони часто обирають вихідні дні для початку операцій шифрування. Зловмисник також завантажує критичні дані цільової системи, щоб використати їх як важіль на наступному етапі циклу атаки.

П'ятий етап - виявлення та вимога викупу - починається з моменту порушення або зупинки роботи бізнес-систем - часто в перший день робочого тижня - і отримання власником бізнесу повідомлення від групи зловмисників, які атакують його. У більшості випадків це текстовий файл на робочому столі, який містить таймер зворотного відліку, перелік поширених запитань щодо роботи програми-вимагача та вимогу зловмисників про сплату певної суми викупу за розшифрування файлівжертви.

Заключний етап - переговори та врегулювання - починається тоді, коли жертва розуміє, що її система паралізована кампанією вимагачів. З'ясування того, як зловмисники зламали систему, на яку спрямована атака, і вивчення того, який варіант програми- вимагача зашифрував дані, є життєво важливими елементами для управління. Оскільки сектори критичної інфраструктури також є частиною національної безпеки, повідомлення правоохоронних органів, відповідних державних установ та страхової компанії є важливими першими кроками. Комунікація з нападниками має важливе значення для врегулювання кризи, але перед початком прямих переговорів об'єкт нападу повинен проаналізувати всі можливі варіанти розвитку подій та альтернативні плани.

Після того, як установа, що стала об'єктом атаки, вирішить розпочати переговори, організація повинна призначити провідного переговірника та визначити, як приймати рішення впродовж процесу. Під час переговорів призначений переговірник повинен вимагати від зловмисників певні докази - наприклад, плани каталогів системи та докази можливості розшифрування - щоб зрозуміти наміри та можливості групи вимагачів. У більшості випадків зловмисники проводять ретельний пошук у цільовій мережі, тому вони знають фінансову спроможність жертви заплатити викуп. Учасник переговорів повинен попросити п р о знижку до остаточного розрахунку між установою-мішенню і групою захоплення, що є останнім етапом процесу. Після укладення угоди установа-мішень повинна провести глибокий криміналістичний аналіз інциденту і вжити необхідних заходів для запобігання майбутнім кібератакам.

Згідно з кіберпопередженням, опублікованим Агентством кібербезпеки та інфраструктури США, у 2020 році неназване підприємство з компримування природного газу, розташоване в США, стало об'єктом атаки зловмисників-здирників. Використовуючи фішингове посилання для отримання початкового доступу до ІТ- та операційних мереж організації, зловмисники розгорнули товарне програмне забезпечення – здирник для шифрування даних у цих мережах з метою їх максимального знищення, а потім вимагали сплати викупу. В мережі OT людино- машинні інтерфейси, архіватори даних та сервери опитування зазнали втрати доступності, втрати оперативних даних в режимі реального часу, що в кінцевому підсумку призвело до часткової втрати видимості для операторів. Хоча на об'єкті зберігався контроль над програмованими логічними контролерами та загальними операціями, система реагування на надзвичайні ситуації на об'єкті надавала пріоритет загрозам фізичній безпеці над кіберінцидентами. Таким чином, керівництво об'єкта вирішило зупинити його роботу на два дні.

Підсумовуючи, можна сказати, що атаки програм-вимагачів на цей компресорний завод і нафтопровід "Колоніальний", про які йшлося раніше в цьому розділі, ілюструють нещодавнє збільшення кількості кампаній з використанням програм- вимагачів і зростання ризиків, які вони становлять для критично важливих об'єктів інфраструктури.

##### Компроміс ділової електронної пошти **(BEC)**

Зростання кількості кампаній з вимаганнями за останні кілька років супроводжується збільшенням кількості атак на ділову електронну пошту, також відомих як компрометація електронних поштових скриньок. ФБР зафіксувало помітне збільшення кількості таких атак з 2015 року - з різким зростанням грошових збитків від них з 2017 року - на суму понад 26 мільярдів доларів США до 2019 року (див. рис. 3-7).

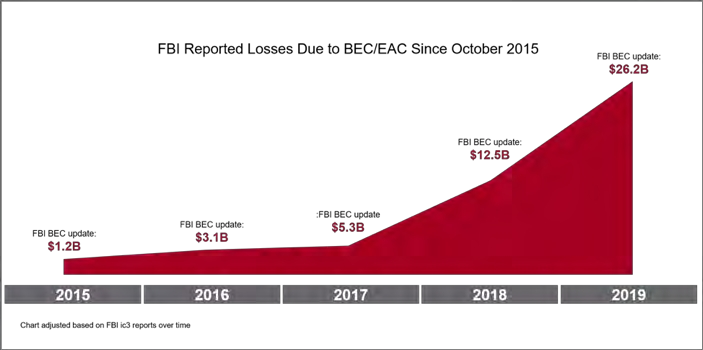


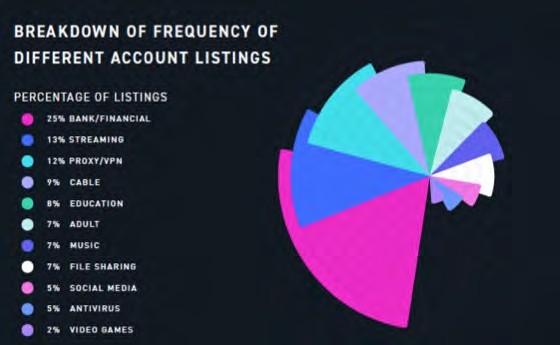
Рисунок **3-7.** Щорічні втрати через компрометацію ділової електронної пошти та облікових записів електронної пошти

(Діаграма Центру розгляду скарг на інтернет-злочини ФБР)

У 2020 році Центр розгляду скарг на інтернет-злочинність ФБР отримав 19 369 скарг щодо компрометації ділової електронної пошти. Концепція BEC - це витончене шахрайство, спрямоване на те, щоб змусити нічого не підозрюючих керівників і співробітників здійснювати платежі або надсилати конфіденційні дані на шахрайські акаунти. Шахрайство часто здійснюється за допомогою таких методів, як соціальна інженерія або комп'ютерне вторгнення, які маніпулюють користувачами, змушуючи їх надсилати гроші або дані. Оскільки ці атаки є вузькоспрямованими і не містять корисного навантаження, їм, як відомо, важко запобігти. Існуючі рішення для виявлення загроз, які аналізують заголовки, посилання та метадані електронних листів, часто пропускають ці типи атак. У типовому прикладі BEC працівники відділу кадрів або фінансові представники отримують електронні листи, які виглядають як листи від працівників вищого рівня, з проханням оновити інформацію про їхні прямі депозити за період виплати зарплати. Фінансова інформація, надана представникам відділу кадрів або бухгалтерії, як правило, веде безпосередньо до рахунку злочинця. Ці типи атак, як правило, спрямовані проти керівників вищого рівня в середовищі критичної інфраструктури і змушують їх надсилати технічну або іншу інформацію, яка може порушити роботу служб критичної інфраструктури або закласти підґрунтя для більш руйнівної кібератаки в майбутньому.

##### Обліковий запис Начинка

Зростаюча діджиталізація приносить із собою проблему автентифікації на різних платформах. Як наслідок, зростає частота підміни облікових даних - типу кібератаки, коли зловмисники отримують скомпрометовані імена користувачів і паролі для доступу до облікових записів користувачів. Громадяни країн- членів і партнерів НАТО потребують численних імен користувачів і паролів для доступу до державних послуг, банківських рахунків або банкоматів, електронної пошти і акаунтів у соціальних мережах, а також до багатьох інших функцій, необхідних для повсякденного життя. Враховуючи обмеженість людської пам'яті, люди схильні повторно використовувати схожі та передбачувані паролі для своїх облікових записів і послуг. Зростання витоків даних і зломів на різних сайтах скомпрометувало величезну кількість імен користувачів і паролів. Результати нещодавнього дослідження щодо використання паролів показують, що навіть після повідомлення про те, що їхні персональні дані були скомпрометовані, лише близько третини користувачів створили нові паролі, більшість з яких не були надійними або унікальними. Інше нещодавнє дослідження показало, що п'ять мільярдів унікальних облікових даних користувачів циркулюють на форумах у темних мережах, де кіберзлочинці продають банківські рахунки та облікові дані адміністратора домену іншим злочинцям у різних точках темної м е р е ж і (див. рисунок 3-8, де показано 11 різних категорій облікових записів у відсотковому співвідношенні).



Малюнок **3-8.** Перелік скомпрометованих акаунтів у темній мережі

(Діаграма за допомогою цифрових тіней)

При підміні облікових даних зловмисник створює бот-мережу, яка вводить скомпрометовані облікові дані в платформи, одночасно змінюючи адреси інтернет-протоколів. Зловмисники записують успішні входи і або отримують ідентифікаційну інформацію чи гроші з цього облікового запису, або зберігають їх для подальшого використання. У просунутій формі підміни облікових даних зловмисники проводять вилучення та сканування даних на таких сайтах, як LinkedIn, Facebook, Twitter та Amazon, використовуючи програмне забезпечення типу Open Bullet, щоб знайти реальних людей та визначити їхню приналежність до певної організації.

Нещодавнім прикладом підміни облікових даних є атака зловмисників на Colonial Pipeline. Зловмисники отримали доступ до Colonial Pipeline через службу віртуальної приватної мережі (VPN), яка була створена для віддаленого доступу до мережі компанії. На момент атаки VPN-обліковий запис все ще функціонував, але не був активним. Немає конкретної інформації про те, звідки зловмисники отримали ці облікові дані. Однак пароль VPN-аккаунта був знайдений серед витоків паролів у темну мережу. Іншим прикладом є кібератака на стартап відеоспостереження Verkada, під час якої 150 000 камер були скомпрометовані колективом хактивістів, відомим як APT-69420 Arson Cats. Хакери ініціювали атаку з підміною облікових даних, отримавши доступ до системи Verkada на рівні "супер-адміністратора", використовуючи ім'я користувача та пароль, які вони знайшли у відкритому доступі в Інтернеті.

Результати досліджень та приклади атак на підміну облікових даних, наведені в цьому розділі, вказують на те, що якщо особа має один скомпрометований обліковий запис, це може легко призвести до компрометації кількох облікових записів. Цей момент також розмиває різницю між особистими та робочими обліковими записами і розкриває ризики, які може становити для систем критичної інфраструктури практика управління паролями співробітників або її відсутність у вигляді підміни облікових даних.

##### Ланцюг постачання Атаки

Окрім вразливостей та ризиків, притаманних людському фактору, більшість об'єктів критичної інфраструктури покладаються на ланцюги поставок з постійно мінливими можливостями кіберзахисту та середнім і високим рівнем залежності від зовнішніх організацій. Атаки на ланцюги поставок - це спосіб націлитися на законні довірчі відносини між об'єктами критичної інфраструктури та зовнішніми організаціями, які забезпечують їхню роботу, і використати їх у своїх цілях. Кінцева мета таких атак - отримати доступ до систем постачальника та скомпрометувати їх, а потім розширити цей доступ углиб афілійованих організацій. Атаки на ланцюги поставок зазвичай складаються з двох важливих етапів. На першому суб'єкти кіберзагроз непомітно проникають в компанію-постачальника та її мережі. Другий етап - поширення шкідливого програмного забезпечення по мережі - набагато простіший, ніж перший. Оскільки між вузлами ланцюга постачання та постачальником вже існують налагоджені та довірчі відносини, користувачі, як правило, приймають будь-які оновлення та виправлення, що надходять від постачальника.

Нещодавнім прикладом атаки на ланцюжок поставок є атака SolarWinds у 2020 році, яка шокувала експертів з кібербезпеки, оскільки вона торкнулася тисяч клієнтів по всьому світу.

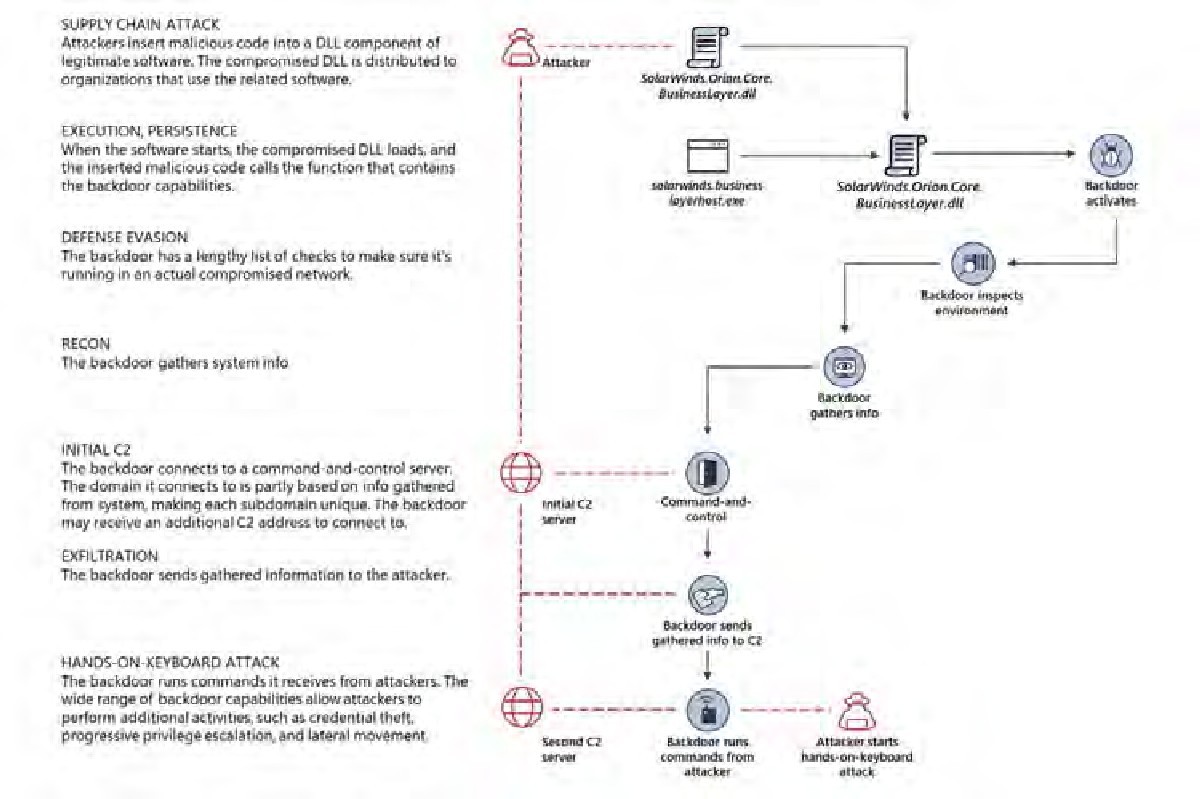
Основний продукт SolarWinds, Orion, - це платформа моніторингу продуктивності для оптимізації ІТ-інфраструктури компаній, які користуються послугою, що налічує близько 300 000 клієнтів. Під час атаки на SolarWinds кібератаки використовували відомий продукт (Orion) в рамках довірчих відносин, щоб скомпрометувати ці компанії та установи, без особливих зусиль отримавши доступ до їхніх захищених систем.

13 грудня 2020 року відома фірма з кібербезпеки FireEye опублікувала звіт про атаку SolarWinds, зазначивши, що зловмисники проводили глобальну кампанію вторгнення з використанням шкідливого програмного забезпечення під назвою SUNBURST. Згідно зі звітом:

FireEye виявив широкомасштабну кампанію, яку ми відстежуємо як UNC2452. Учасники цієї кампанії отримали доступ до численних державних і приватних організацій по всьому світу. Вони отримали доступ до жертв через троянізовані оновлення програмного забезпечення для моніторингу та управління ІТ-інфраструктурою Orion компанії SolarWind. Ця кампанія могла розпочатися ще навесні 2020 року і наразі триває.

Пізніше було підтверджено, що зловмисники отримали доступ до програмного забезпечення Orion компанії SolarWinds у березні 2020 року і вставили шкідливий код у бібліотеку динамічних посилань програми оновлення Orion. Як тільки компанії, що використовують Orion, оновили програму - перший етап цієї атаки на ланцюжок поставок - цей код активував бекдор, який контролює налаштування мережі та передає необхідну інформацію на командно-контрольний сервер суб'єктів кіберзагрози. На другому етапі зловмисники отримали вражаючий рівень доступу з такими можливостями, як ескалація привілеїв і латеральне переміщення (див. рис. 3-9 для огляду етапів атаки SolarWinds).46

За оцінками, приблизно 18 000 клієнтів встановили оновлення безпеки Orion у березні 2020 року, а це означає, що близько 6 відсотків клієнтської бази SolarWinds мали заражені системи і були вразливими протягом більшої частини 2020 року до того, як FireEye виявив кібератаку. Оскільки клієнтська база складається з користувачів з державного та приватного секторів, атака вплинула на низку відомих організацій, таких як AT&T, CISCO, McAfee, Microsoft, *New York Times*, Symantec, Visa, численні університети та урядові установи США, в тому числі міністерства торгівлі, оборони, енергетики, внутрішньої безпеки, державного департаменту та казначейства, центри з контролю та профілактики захворювань, а також Національну адміністрацію з дерної безпеки.48 Цей список не є вичерпним, і дуже ймовірно, що від атаки постраждало набагато більше організацій.



Малюнок **3-9.** Операція атаки на ланцюжок поставок

**SolarWinds**

(Діаграма від Microsoft)

Всього за п'ять днів до того, як попередити громадськість про атаку SolarWinds, компанія FireEye оголосила, що "країна з наступальними можливостями найвищого рівня" проникла в її мережу і викрала набір інструментів "червоної команди", які FireEye використовувала для імітації атак і можливостей потенційного супротивника під час розробки більш ефективних продуктів кібербезпеки.49 У відповідь на атаку SolarWinds, яка надала зловмисникам доступ до висококласних інструментів безпеки FireEye, а також до конфіденційної інформації та критично важливої інфраструктури кібербезпеки, аналітики спочатку вказали на Росію як на джерело кібератаки. Кілька місяців пішло на те, щоб зібрати криміналістичні докази атаки SolarWinds і зрозуміти, якої шкоди вона завдала. З огляду на труднощі з визначенням авторства кібератак, влада США спочатку з обережністю ставилася до оголошення того, яка група здійснила кібератаку. Однак у квітні 2021 року Агентство національної безпеки, Агентство кібербезпеки та інфраструктурної безпеки і ФБР опублікували спільну рекомендацію з кібербезпеки, в якій приписують атаку SolarWinds - а також кілька інших - суб'єктам Служби зовнішньої розвідки Росії, відомим як APT29, Cozy Bear і The Dukes.

### Висновок

Роль кібербезпеки в рамках зусиль РСБІ характеризується особливими відмінностями і труднощами в кількох ключових сферах. Такі динамічні фактори, як швидка зміна технологій, характер і проблеми державно-приватного співробітництва, інвестиції в безпеку з боку бізнесу, різний рівень кваліфікації робочої сили і проблеми в ланцюгах поставок, разом створюють гіперконкурентне середовище. Ці виклики лише висвітлюють сувору реальність того, що існують межі того, що і скільки зацікавлені сторони можуть реально захистити в критично важливій інфраструктурі. Вразливості змінюються, загрози еволюціонують, а підтримувати необхідний людський капітал у складі робочої сили з кожним роком стає все складніше. Конфлікти і тертя, що існують у фізичній сфері, існують і в кіберпросторі.

Задля підтримання життєдіяльності державні органи намагаються регулювати всі можливі аспекти критичної інфраструктури, зосереджуючи увагу на загрозах, які несуть зловмисні сили. Однак добре написані нормативні акти не враховують автоматично вимоги та очікування різних секторів критичної інфраструктури і не сприяють таким необхідним технологічним удосконаленням. Елемент невизначеності також перешкоджає психологічному настрою, необхідному для внесення змін і підготовки до підвищення стійкості. Крім того, команди з кібербезпеки часто відчувають гостру нестачу персоналу і страждають від обмеженого часу на навчання, щоб пройти регулярну сертифікацію і таким чином адаптуватися до нових технологічних розробок і практик, що застосовуються супротивниками. За таких умов дуже складно здійснювати заходи з РІКБ з традиційним мисленням у сфері безпеки. Обмежені ресурси вимагають нових поглядів і практик.

Однак питання про те, який спосіб мислення прийняти і як це зробити, є одним з найскладніших питань, з яким стикаються зацікавлені сторони, що працюють у сфері критичної інфраструктури. У своєму нещодавньому інтерв'ю експерт з кібербезпеки та бізнесмен Дмитро Альперович пропонує потенційний шлях до формування нового бачення кібербезпеки:

Я вже більше 10 років кажу, що вторгнення неминучі, ніхто не застрахований, і кожен повинен почати думати про це з точки зору "нас, швидше за все, зламають, нас, швидше за все, скомпрометують, але як ми можемо запобігти шкоді?"... Правильний спосіб думати про стратегії безпеки в майбутньому - це припустити, що стався злом, безперервно шукати будь-яку присутність супротивників у вашій мережі і виганяти їх якомога швидше.

Кіберпростір - і зростаючий зв'язок, який він привносить майже в усі аспекти сучасного життя, - пропонує мало чітких кордонів або ліній оборони, які б утримували супротивників подалі. Ця ситуація створює невизначеність, яка вимагає від учасників критичної інфраструктури прийняти нові перспективи і впроваджувати нові політики CISR, які можуть вижити і досягти успіху в цих умовах. Найкращою альтернативою на шляху до побудови більш стійких і безпечних систем є прийняття менталітету нульової довіри і "припущення про порушення" в майбутньому. Таке нове мислення у сфері безпеки має зосереджуватися на інвестиціях у людський капітал та покращенні підготовки, обізнаності щодо ситуації і загальних можливостей персоналу з кібербезпеки об'єктів критичної інфраструктури.

# - 4 -

## Гібридні загрози критичній інфраструктурі США і НАТО

Керол В. Еванс

Захист критичної інфраструктури є життєво важливим стратегічним завданням і викликом для Сполучених Штатів і Організації Північноатлантичного договору. Супротивники активно атакують об'єкти критичної інфраструктури в країнах- членах Альянсу, особливо в секторах енергетики, транспорту, інформації, зв'язку і оборонно-промислової бази (ОПБ), як потенційний засіб підриву військового потенціалу, проектування сил, мобільності і життєзабезпечення.

Для забезпечення розуміння гібридних загроз критичній інфраструктурі з боку супротивника і інноваційних способів протидії їм з боку США і НАТО цей розділ складається з трьох розділів. У першому розділі розглядається еволюція характеру загроз критичній інфраструктурі. Технологічна конвергенція між комунікаційними і інформаційними технологіями з кіберпідключенням до систем критичної інфраструктури змінила парадигму загроз з кінетичних на кібернетичні і гібридні засоби нападу. Цей відносно недавній розвиток подій створив можливості для супротивників використовувати вразливості критичної інфраструктури, від якої залежать збройні сили США і НАТО. У другому розділі представлено аналіз кількох векторів гібридних загроз, які можуть атакувати, підірвати або скомпрометувати бойові можливості США і НАТО, а також їх спроможність до проектування сил і засобів і забезпечення життєдіяльності. Перший вектор містить гібридні загрози для батьківщини США - зокрема, цілеспрямоване проникнення в енергетичну інфраструктуру, яка підтримує американські об'єкти і бази, з метою втручання здатність збройних сил розгортати і підтримувати передові бойові сили і техніку. Другий вектор гібридної загрози - це ворожі напади на логістику США і НАТО, що може погіршити можливості США з проектування сил за кордоном, а також мобільність і стійкість НАТО на театрі військових дій. Третя гібридна загроза пов'язана зі стратегічним проникненням, володінням і контролем Китаю над ключовими об'єктами інфраструктури і ланцюгами постачання в Європі через його ініціативу "Один пояс, один шлях" і прямі іноземні інвестиції. Цей вектор надає можливість підірвати оперативну сумісність і політичну єдність США і НАТО. Насамкінець розділ завершується висвітленням заходів США і НАТО з усунення і пом'якшення цих загроз шляхом інвестування в безпеку і стійкість критичної інфраструктури через розбудову організаційної спроможності, політичні рамки і виконання базових вимог до стійкості приймаючої країни.

### Кібер**-**кібер**-**гібридні загрози для критичної інфраструктури

Характер загрози критичній інфраструктурі США і країн НАТО значно змінився: від кінетичних атак терористичних організацій до використання кібернетичних і гібридних засобів національними державами, маріонетками і іншими супротивниками. Починаючи з 2001 року, спостерігалась швидка ескалація гучних атак на об'єкти критичної інфраструктури в країнах Альянсу, здійснених Аль-Каїдою та іншими терористичними організаціями. Серед них атаки на Пентагон і Всесвітній торговий центр 11 вересня, вибухи в мадридській електричці і на залізничному вокзалі в Аточі в 2004 році, вибухи на транспорті в Лондоні в 2005 році, скоординована серія терористичних атак в Парижі в 2015 році і стрілянина в аеропорту імені Ататюрка і вибухи, скоєні терористами- смертниками в 2016 році. Усі ці приклади вимагали фізичної присутності нападників і використання кінетичних засобів (див. розділ 2 з оглядом фізичних терористичних загроз і розділи 6 і 7 з більш детальною інформацією про ці та інші приклади, спрямовані проти сектору цивільної авіації і залізничного транспорту).

Проте поява кіберпростору забезпечила новий механізм доставки, який збільшив швидкість, частоту і потужність атак на критично важливу інфраструктуру США і НАТО. Ефективність кіберінструментів зросла завдяки швидкому взаємозв'язку інформаційно-комунікаційних систем з системами критичної інфраструктури, в тому числі завдяки розвитку Інтернету речей і створенню "розумних" міст (див. розділи 3 і 14, де детально розглядаються кіберзагрози і суб'єкти, а також рекомендації з управління ризиками для кібербезпеки). Як зазначив тодішній директор Національної розвідки США адмірал Денніс Блер: "Зростаючий зв'язок між інформаційними системами, Інтернетом та іншими інфраструктурами створює можливості для зловмисників порушувати роботу телекомунікацій, електроенергетики, енергопроводів, фінансових мереж та інших об'єктів критичної інфраструктури".1 Ця інформаційно-комунікаційна, цифрова і кібернетична революція, що складається з взаємозалежних мереж інфраструктур інформаційних технологій (апаратне і програмне забезпечення, дані і протоколи) і інформації (Інтернет, телекомунікаційні мережі, комп'ютерні системи, вбудовані процесори і контролери), створила вектор атаки, завдяки якому кібернетична сфера стала улюбленою зброєю супротивників Сполучених Штатів і НАТО. Для супротивників кіберпростір забезпечує анонімність і менший ризик бути виявленими і постраждати, а також вимагає невеликих ресурсів для доступу до широкого кола різноманітних цілей - і все це з можливістю діяти майже з будь-якого географічного місця. Звідси і поширення кібератак на інфраструктуру США і НАТО, адже можна атакувати стратегічні цілі з мінімальним ризиком, не будучи фізично присутнім і не вступаючи в протистояння з оборонними силами.

Ці атаки стають все більш регулярними і витонченими з боку Китаю, Росії, Ірану та Північної Кореї. За даними американської розвідки, Китай "становить постійну загрозу кібератак на наші основні військові системи і системи критичної інфраструктури", а Росія "становить загрозу кібершпигунства, інформаційного впливу і атак на Сполучені Штати і наших союзників" і "...зараз розгортає засоби для кібератак, щоб мати змогу підірвати або пошкодити цивільну і військову інфраструктуру США під час кризи".2 Операція "Клівер" - широкомасштабна глобальна кампанія зі спостереження і проникнення - приписується Ірану. Цілями цієї кампанії були нафта і газ, енергетика і комунальні послуги, громадський транспорт, авіалінії, аеропорти, лікарні, телекомунікації, DIB, хімічні компанії, а також урядові і військові мережі в країнах НАТО: Канаді, Франції, Німеччині, Туреччині, Великобританії та США. Серед найдосконаліших у світі груп, що становлять загрозу, Головне розвідувальне управління Північної Кореї - широко відоме як Група Лазаря або APT38 - здійснило фішингові атаки на співробітників американських енергетичних,

аерокосмічних і технологічних компаній, а також Державного департаменту США і Міністерства оборони США.

Група також відповідальна за атаку вірусу-здирника WannaCry у 2017 році, яка призвела до зупинки роботи Національної служби охорони здоров'я Великої Британії. У 2021 році Міністерство юстиції США висунуло звинувачення трьом північнокорейським програмістам, пов'язаним з APT38, у низці гучних кібератак. Слід зазначити, що останнім часом північнокорейські кіберкоманди націлилися на фінансові установи та біржі віртуальних валют, щоб зібрати кошти на підтримку програми балістичних ракет країни.

Вторгнення і анексія Росією Криму в 2014 році та підтримка сепаратистського повстання на сході України призвели до появи терміну "гібридна війна" та інших термінів, таких як "конфлікт у сірій зоні" і "необмежена війна", для опису того, що вважалося новою формою війни. Гібридна війна також застосовувалася до дій Росії в Грузії і в балтійських країнах - Естонії та Латвії (обидві країни є членами НАТО і Європейського Союзу). Така діяльність викликала занепокоєння, "що Росія намагатиметься використати російську меншину для отримання впливу в країнах Балтії, застосовувати таємні дії для захоплення території, використовувати підривну діяльність для виправдання звичайної атаки або іншим чином використовувати заперечувані або приховані засоби для отримання впливу в країнах Балтії і підриву ЄС і НАТО". Ці приклади гібридної війни свідчать про притаманну російським діям невизначеність, яка перешкоджатиме вчасній і скоординованій реакції з боку НАТО, тим самим підриваючи довіру до Альянсу і його зобов'язання перед східними членами і фактично надаючи Росії право вето на євроатлантичне розширення.

Концепція гібридної війни в останні роки викликала жваві дебати серед військових стратегів і науковців, причому багато експертів стверджують, що в цьому типі війни немає нічого нового. Дійсно, НАТО перейшла від використання гібридної війни до більш широкої концепції гібридних загроз. Під цим кутом зору гібридна війна є складовою цілої низки гібридних загроз. Очікується, що остання не призведе до застосування статті 5 Вашингтонського договору. За визначенням НАТО, гібридні загрози:

поєднують військові та невійськові, а також приховані та відкриті засоби, включаючи дезінформацію, кібератаки, економічний тиск, розгортання нерегулярних збройних формувань та використання регулярних збройних сил. Гібридні методи використовуються для того, щоб розмити межі між війною і миром і посіяти сумніви у свідомості цільових груп населення. Вони спрямовані на дестабілізацію і підрив суспільства.

У цьому відношенні концепція гібридної загрози підкреслює системну вразливість демократичних держав з боку ревізіоністських супротивників і авторитарних держав, що вимагає контрзаходів, які передбачають загальнодержавний підхід і цивільно-військове співробітництво.

Гібридні загрози є корисною основою для розуміння того, чому супротивники США і НАТО все частіше використовують критично важливу інфраструктуру як зброю. Інфраструктура є привабливою мішенню для примусу, залякування і тиску на цільову державу, як це продемонстрували російські кібератаки на українську електромережу в 2015 і 2016 роках, а також на низку об'єктів критичної інфраструктури за кілька днів і годин до вторгнення Росії в Україну в лютому 2022 року. Противники також можуть використовувати кінетичні засоби для досягнення цих ефектів, не обов'язково беручи участь у відкритих військових діях. Хороший приклад такого типу гібридної загрози стався у 2017 році, коли російські військові кораблі перешкоджали прокладанню підводного електричного кабелю між Швецією і Литвою, заважаючи суднам Nordbalt, що прокладали кабель, прокладати його. Кабель був прокладений для збільшення енергопостачання в обох країнах і для полегшення обміну електроенергією між балтійським і північним ринками електроенергії, тим самим зменшуючи їхні сукупні витрати на електроенергію.

У наступному розділі буде показано, як супротивники використовують безліч векторів гібридних загроз для створення і подальшого використання залежностей між цивільною і військовою інфраструктурою у спосіб, що має згубний вплив на військову міць США і НАТО.

### Підготовка поля бою**:**

Озброєння критичної інфраструктури**,** щоб кинути виклик військовій перевазі США і НАТО

Стримуюче значення сил США і НАТО має вирішальне значення. Стримування ґрунтується не лише на надійних військових силах і засобах, структурі збройних сил і проектуванні сил, але і на здатності критично важливої інфраструктури США і країн-членів НАТО підтримувати швидке реагування, графіки підкріплень і засоби життєзабезпечення. Проникнення, порушення роботи, контроль і знищення ключових об'єктів глобальної критичної інфраструктури є передовим інструментом супротивника для послаблення місій і операцій НАТО. У цьому розділі розглядаються три сфери, в яких супротивники розгортають гібридні загрози проти критичної інфраструктури в США і Європі з метою підірвати таке панування.

##### Гібридні загрози для США та ведення війни Можливості

Супротивники, зокрема Росія і Китай, свідомо і ефективно атакують енергетичну інфраструктуру, особливо американські електромережі, необхідні для підтримки військових об'єктів і баз США, щоб поставити під загрозу їхні майбутні військові спроможності. Електрична мережа є ключовим сектором життєзабезпечення, який живить усі інші сектори цивільно- військової інфраструктури: водопостачання, санітарію, зв'язок і транспорт. Кінетичні атаки на електромережу США розглядаються Росією і Китаєм в контексті превентивних можливостей нанесення першого удару. Кібератаки, однак, є основним засобом для нанесення удару по енергосистемах США і країн-членів НАТО, оскільки сучасні енергосистеми покладаються на складні системи диспетчерського контролю і збору даних (SCADA), а також на використання нових комунікаційних і мережевих технологій, які надають потенційним супротивникам доступ до "чорних ходів". Корисно коротко розглянути кібератаки Росії на українську електромережу, оскільки ці атаки дозволили Москві протестувати, довести і вдосконалити свої можливості у сфері кібер-війни для подальшого працевлаштування в США (див. розділ 5 для більш детального вивчення цих кібератак).

Зв'язок між критичною інфраструктурою як інструментом гібридної війни був відкрито продемонстрований в Україні, де російська кібер-армія, тісно пов'язана з Кремлем, систематично атакувала майже всі сектори української інфраструктури з 2015 року. Ці атаки відбувалися н а тлі незаконної анексії Криму Росією у 2014 році та продовження військових зіткнень у східній частині Донецької та Луганської областей України. Найбільш помітними були атаки на українську електромережу в грудні 2015 року, в результаті яких значна частина столиці, Києва та західної частини Івано-Франківської області залишилася без світла, після чого в 2016 році відбулася ще одна, більш технологічно складна атака на одну з київських підстанцій електропередач. Ці кібератаки приписували російському угрупованню, відомому як Sandstorm, яке розгорнуло своє шкідливе програмне забезпечення BlackEnergy для проникнення в спеціалізовані комп'ютерні архітектури, що використовуються для дистанційного керування фізичним промисловим обладнанням і системами управління. Найбільше занепокоєння кібер-експертів викликало те, що Sandstorm вже атакувала мережі НАТО і скомпрометувала комп'ютери американських і європейських електричних і водопостачальних компаній за допомогою тієї ж самої троянської програми. Це шкідливе програмне забезпечення забезпечило групі достатній контроль, щоб викликати відключення електроенергії на території США. Як попередив один з експертів з кібер-криміналістики, "супротивник, який вже націлився на американські енергетичні компанії, перейшов межу і вивів з ладу електромережу [в Україні]. Це була неминуча загроза для Сполучених Штатів".

У березні 2018 року Федеральне бюро розслідувань США і Міністерство внутрішньої безпеки підтвердили, що російські урядові команди хакерів активно "націлювалися на урядові установи і численні сектори критичної інфраструктури США, включаючи енергетику, ядерну промисловість, комерційні об'єкти, водопостачання, авіацію і критично важливі виробничі галузі". Російські команди кібератак включали Sandstorm, Dragonfly і Palmetto Fusion, деякі з них отримали віддалений доступ до реальних промислових систем управління і мереж енергетичного сектору США, в тому числі до атомної електростанції в Канзасі. Кібератаки на енергосистему США тривають. Наприклад, група зловмисників, відома як Xenotime і Triton, скомпрометувала системи безпеки електричних об'єктів, щоб спричинити потенційні збої в роботі та пошкодження електростанцій. За словами дослідника з американської фірми з кібербезпеки Dragos, спостереження за американською електромережею "свідчить про попередні дії, необхідні для підготовки до майбутнього вторгнення і, можливо, майбутньої атаки".

Кібератаки не обмежуються лише російськими зловмисниками. За оцінками, Китай також може вивести з ладу енергосистему США за допомогою кібератаки. У 2014 році тодішній командувач Кіберкомандування США і директор Агентства національної безпеки адмірал Майкл Роджерс свідчив, що Сполучені Штати виявили в американських системах шкідливе програмне забезпечення з Китаю, яке дозволило Пекіну "відключити дуже сегментовані, дуже індивідуальні частини нашої інфраструктури".Фірма Mandiant, що займається кібербезпекою, також підтвердила, що хакери, які працюють від імені китайського уряду, активно проникають в американські комунальні системи, які обслуговують все - від виробництва електроенергії до транспортування води і палива по всій країні.

Гібридні загрози енергетичній інфраструктурі США з'явилися в той час, коли низка факторів робить цю інфраструктуру більш вразливою. У Сполучених Штатах більшість електроенергії, яку споживають військові об'єкти, надходить з комерційної електромережі. Останніми роками ці військові бази використовуються для проведення спеціалізованих бойових дій, обробки, використання і поширення розвідданих, а також для мережевого зв'язку в режимі реального часу для командування і управління. Ця діяльність значно збільшила військову залежність США від енергоресурсів, зокрема електроенергії.

Десятиліттями недостатнє інвестування в об'єкти американської військової бази в поєднанні з посиленою залежністю від приватної інфраструктури, яка значною мірою не контролюється військовими, є головним ускладнюючим фактором, що створює ще одне джерело для ворожої експлуатації. Збільшення географічної Концентрація інфраструктури є одним з таких факторів. Наприклад, понад 31 відсоток суднобудівних і судноремонтних потужностей ВМС США знаходиться в Норфолку, штат Вірджинія, та його околицях.21 Об'єкти Міністерства оборони (МО) і пов'язана з ними інфраструктура залежать від безперервного, гарантованого електропостачання для підтримки місій і операцій як на континентальній частині США, так і за її межами. Будь-яка тривала втрата електропостачання є, як було визнано, кричущою ахіллесовою п'ятою національної безпеки. Америка повинна очікувати, що супротивники будуть націлені на її енергосистему і намагатимуться вивести її з ладу, що може призвести до каскадних і наростаючих збоїв у транспортній, телекомунікаційній та інших критично важливих інфраструктурних послугах, від яких залежить армія США (див. розділ 12 для подальшого пояснення цих взаємозалежностей і потенційних збоїв, а також необхідності розбудови стратегій стійкості, які б достатньою мірою враховували їх).

Як визнав один колишній високопоставлений чиновник Міністерства оборони, "найрозумніше - це маневрувати навколо цих сил, атакувати критично важливу інфраструктуру, об'єкти тут, у Сполучених Штатах, від яких залежить розгортання, функціонування і підтримка наших збройних сил за кордоном". Готовність і здатність супротивників розгортати руйнівну кіберзброю в майбутній війні зі Сполученими Штатами мають величезні наслідки для національної безпеки. Безпосереднє занепокоєння викликає загроза стримуванню і власним можливостям проектування сили США, оскільки: "Не має значення, наскільки боєздатними, наскільки добре підготовленими або наскільки передовими є збройні сили країни, якщо вони не можуть вчасно потрапити на фронт".

##### Гібридні загрози операціям мобільності і життєзабезпечення США і НАТО

Наші сили стримування і оборони підкріплені надійними силами, як на місцях, так і готовими до підкріплення в Європі і з-за Атлантики.

Декларація Брюссельського саміту НАТО

-2018

НАТО ... має інвестувати в свою здатність відстежувати і захищати від будь-якої китайської діяльності, яка може вплинути на колективну оборону, військову готовність або стійкість в зоні відповідальності Верховного головнокомандувача об'єднаних збройних сил НАТО в Європі ( SACEUR).

НАТО - 2030: Об'єднані заради нової ери Здатність США і НАТО проектувати сили залежить від

на мобільність та сталість, остання з яких ґрунтується на безпечних

і надійну логістику. Оскільки Сполучені Штати і НАТО готуються до конкуренції великих держав з Росією і Китаєм, стратегічна мобільність для розгортання і підтримки збройних сил на цих відповідних театрах буде мати вирішальне значення. Крім того, стратегічна мобільність лежить в основі надійних сил і засобів стримування, а в цьому новому середовищі гібридних загроз спроможність перекидати війська є вразливою. Мобільність починається з військових об'єктів на континентальній частині США і не закінчується доти, доки війська і техніка не будуть передислоковані і підготовлені до операцій на театрі бойових дій. Справді, здатність Сполучених Штатів мобілізувати свій військовий потенціал для швидкого реагування на кризи, конфлікти і війни - це те, що робить НАТО надійною організацією.

У цьому розділі аналізується, як супротивники визначають ключові об'єкти логістичної інфраструктури і мобілізаційні вузли, що підтримують війну США і НАТО, щоб зірвати своєчасну підготовку, розгортання і підтримку військових сил і засобів на батьківщині США, а також в країнах-членах НАТО. У ньому вперше розглядається, як супротивники можуть використовувати гібридні загрози, щоб зірвати розгортання збройних сил США за межами Північної Америки і послабити здатність Сполучених Штатів вести тривалі бойові дії проти НАТО, націлившись на об'єкти критичної інфраструктури.

Ворожі напади на об'єкти інфраструктури, що підтримують війну, не є чимось новим. Радянський Союз розумів, що військовий персонал і підкріплення з батьківщини США затягнуть будь-який майбутній конфлікт на європейському театрі воєнних дій, що створить сприятливу диспозицію для НАТО. Відповідно, радянські військові та розвідувальні структури зосередилися на завданні шкоди американській мобілізаційній базі та підтримуючій інфраструктурі, включаючи американські військові об'єкти і військово-морські бази, торгові порти, залізниці, інші транспортні вузли та сектори життєзабезпечення. Радянський Союз проводив оцінку того, як американські війська готувалися до стратегічного розгортання зі Сполучених Штатів, що вони мобілізували, які ресурси були потрібні для транспортування і забезпечення розгортання військ, і які військові і цивільні структури були задіяні в цьому процесі. Оцінка моделювання з відкритим вихідним кодом, проведена Аргонською національною лабораторією, показала, що успішні атаки на критично важливу інфраструктуру США матимуть серйозні наслідки для військової дезорганізації, в тому числі збільшення часу пересування, фактичну втрату активів і дефіцит критично важливих навичок і матеріальних засобів.

В той час як Радянський Союз створив логістичну інфраструктуру DIB США для цілей кінетичного наведення, сучасні супротивники мають можливість здійснювати атаки за допомогою гібридних загроз. Ця здатність означає, що батьківщина США більше не може вважатися притулком, а супротивники мають стратегічну досяжність і засоби для нападу на ключові вузли і зміщення центрів розгортання збройних сил. Сьогоднішнє конкурентне середовище розгортання - це середовище, в якому політики національної безпеки і військові планувальники більше не можуть вважати, що матеріально-технічні засоби можуть безперешкодно прибути на європейський театр воєнних дій.

Складна обстановка стає ще більш проблематичною з огляду на те, що передових сил США в Європі - з їхніми вимогами щодо ротації і збалансування сил - недостатньо, що ще більше посилює потребу в швидкому підкріпленні військами, боєприпасами і матеріальною базою. Проте розгортання військового потенціалу під час нападу - це сценарій, до якого оборонні і національні структури США залишаються в значній мірі непідготовленими. Дійсно, нещодавнє дослідження припускає, що оскільки Сполучені Штати не мають "комплексної стратегії захисту свого цивільного населення і оборонної промислової бази, а також мобілізації і підтримки нації під час війни" з 1993 року, "Америка ризикує програти свою наступну війну з однією або кількома великими національними державами".

Ці виклики ускладнюються значними критичними недоліками в транспортній і логістичній інфраструктурі США, які підривають їхні можливості з розгортання і підтримання військ і створюють додаткові вектори загроз, якими можуть скористатися супротивники. Однією з таких слабких сторін є нестача стратегічної мобільності в короткостроковій перспективі, яка визнана неприйнятним ризиком для розгортання збройних сил. Нині транспортні сили США Командування ВМС США (USTRANSCOM) - функціональне бойове командування, відповідальне за забезпечення повітряних, наземних і морських перевезень для задоволення потреб мобільності США - має достатньо транспортних літаків, щоб доставити до театру бойових дій лише одну бойову групу бронетанкової бригади з приблизно

5 000 військовослужбовців і кількома сотнями військових машин. Не менш гнітюча картина і зі стратегічними морськими суднами США, оскільки 70 відсотків органічного флоту буде старше 60 років у 2034 році.

На додаток до старіння органічного флоту морських перевезень, ТРАНСКОМ визнав, що зменшення кількості суден, які відстають від американських, недостатнє військово-морське супроводження і скорочення флоту торговельного флоту і моряків є іншими конкуруючими і шкідливими факторами для стратегічних морських перевезень. У 2018 році армія США попередила Комітет з питань збройних сил Палати представників Конгресу США, що до 2024 року національні можливості морських перевезень, на які сухопутні війська і морська піхота покладаються для транспортування до 90 відсотків свого обладнання в разі великої війни або кризи, впадуть нижче необхідного рівня. У своєму інформаційному документі для Комітету армія зазначила, що цей дефіцит морських перевезень "підриває ефективність звичайних засобів стримування США, оскільки навіть повністю забезпечені ресурсами і підготовлені сили мають обмежену стримуючу силу, якщо супротивник вважає, що він може досягти своєї стратегічної мети у вікно можливостей до прибуття американських сухопутних військ".

Мобільність місії ТРАНСКОМ значною мірою залежить від приватних комерційних постачальників повітряних, наземних і морських перевезень, які є дуже вразливими до кібератак і перебоїв в енергопостачанні. У своїх свідченнях в Сенаті у 2018 році генерал Даррен МакДью, тодішній командувач ТРАНСКОМ, зазначив, що його "логістичне підприємство є більш вразливим до цих зловмисних [кібер] дій, ніж інші військові організації, зважаючи на наші унікальні відносини з комерційними партнерами". Ця вразливість особливо очевидна, оскільки 90 відсотків військової логістики і глобальних операцій TRANSCOM здійснюються в несекретних комерційних мережах. Запущений Росією Кібератака NotPetya у 2017 році є повчальним прикладом потенційних майбутніх ризиків для TRANSCOM. Ця кібератака, яка спочатку була націлена на Україну, призвела до того, що один з найбільших транспортних провайдерів TRANSCOM, компанія Maersk, та всі її глобальні портові, судноплавні, логістичні та контейнерні операції зупинилися більш ніж на 10 днів. Постраждали понад 76 портів і 800 суден, а відновлення систем мережі коштувало Maersk приблизно 300 мільйонів доларів США. Порушення глобальних ланцюгів постачання, спричинені атакою NotPetya, були величезними. Детальніше про характер і наслідки кібератаки NotPetya див. у розділі 5.

##### Гібридні загрози з боку Китайської Народної Республіки Китай

Повертаючись до загроз мобільності і операціям НАТО з підтримання життєдіяльності на європейському театрі, слід посилити аналіз гібридної діяльності Китаю і, зокрема, підписаної Генеральним секретарем Комуністичної партії Китаю Сі Цзіньпіном Ініціативи "Один пояс, один шлях" (BRI). Значні інвестиції в морську інфраструктуру Європи спрямовуються через "Морський Шовковий шлях" BRI XXI століття, який складається з трьох блакитних водних шляхів і масивних інвестицій в портову інфраструктуру, включаючи глибоководні морські порти і споруди, промислові зони вільної торгівлі, сховища енергії, трубопроводи і нафтопереробні потужності. Китайська Народна Республіка (КНР) стверджує, що Морський Шовковий шлях необхідний для забезпечення безпеки морських шляхів сполучення і торговельних маршрутів для її потреб в енергії, природних ресурсах і ланцюгах поставок.

Два морських шляхи Шовкового шляху - Китай-Індійський океан-Африка-Середземне море і Китай-Європа-Льодовитий океан - розвиваються для того, щоб з'єднати і прискорити торгівлю та інвестиції з Китаю в Європу, найбільшого торгового партнера КНР. У самій Європі Китай швидко розширює свої портові потужності і портфелі термінальних операцій. Основні китайські проекти портової інфраструктури включають талійські порти Трієст, Венеція і Равенна, словенський порт Каподістрія і хорватський порт Фіуме. Крім того, китайські державні компанії на чолі з China Ocean Shipping Company (COSCO), четвертим за величиною контейнерним флотом у світі, придбали контрольні та міноритарні пакети акцій у 13 європейських портах. У Зебрюгге, другому за величиною порту Бельгії, COSCO володіє 90 відсотками єдиного в країні оператора терміналу. В Іспанії COSCO має 51% акцій і управлінський контроль над найбільшим терміналом у Валенсії, а також 40% акцій компанії Noatum.

Контейнерний термінал у Більбао. Вона також володіє міноритарними частками в інших терміналах в Антверпені, Лас- Пальмасі та Роттердамі. Разом ці порти забезпечують приблизно

10 відсотків європейських контейнерних потужностей для морських перевезень.

Масштабні інвестиції КНР як в портову інфраструктуру, так і в портові операції в Піреї, Греція, привернули увагу і викликали занепокоєння деяких спостерігачів з ЄС і НАТО. Пірей - єдиний глибоководний порт у східному Середземномор'ї, який має потужності та інфраструктуру для перевалки вантажів, а глибина гавані дозволяє швартуватися дуже великим контейнеровозам. Він має велику стратегічну перевагу для контейнерних перевезень над північноєвропейськими портами Гамбург і Роттердам, оскільки розташування Пірея скорочує тиждень транзитного часу з Азії, що дозволяє заощадити приблизно

2 мільйони доларів за поїздку. Для США і НАТО Пірей також є найбільшою військово-морською базою Греції, а також центром операцій НАТО і Шостого флоту ВМС США в Середземному морі.

Китай визнав геостратегічну цінність порту Пірей, який Сі Цзіньпін називає "головою дракона". У 2016 році, всього через шість років після початкових інвестицій, COSCO стала мажоритарним акціонером контейнерних терміналів у Піреї, експлуатуючи два з трьох терміналів порту через свою дочірню компанію Piraeus Container Terminal. COSCO також має операційний контроль над третім терміналом через свою мажоритарну частку в Адміністрації порту Пірей, яка збільшилася з 51 до 67% після нещодавньої поправки до угоди 2016 року. Планується, що Пірей стане найбільшим контейнерним портом Середземномор'я і головним світовим перевалочним вузлом, заснованим на моделі антрепоту Сінгапуру.

Інвестиції китайської компанії "Морський шовковий шлях" в порт Пірей викликали тривогу в Брюсселі щодо вразливості фінансового становища слабкіші держави ЄС до іноземного впливу та примусу. Ці інвестиції, а також інші інвестиції БРІ, про які йтиметься далі в цьому розділі, також спричинили необхідність розробки узгодженої системи перевірки іноземних інвестицій на рівні ЄС та запровадження більш суворих заходів перевірки іноземних інвестицій для моніторингу придбання стратегічної критичної інфраструктури в державах-членах ЄС.

Проте для НАТО інвестиції КНР в європейські порти мають набагато більше наслідків для безпеки. Безпосереднє значення має гарантований доступ до європейської портової інфраструктури і об'єктів, необхідних для швидкого і тривалого розгортання, переміщення і забезпечення військ і матеріальних засобів НАТО під час кризи, конфлікту або війни. За словами одного зі спостерігачів НАТО, контроль КНР над європейською морською інфраструктурою "може зменшити готовність членів Альянсу переміщувати військові сили, в тому числі чутливі технології, через порт і навколишні мережі. Це може призвести до порушення планування і зменшення кількості військових навчань, що знизить здатність НАТО захищати країни Балтії під час кризи з Росією". Варто також відзначити залежність від спеціальних глибоководних споруд, необхідних для кораблів американських морських котиків. Відмова або перешкоджання доступу до таких портів матиме згубний вплив і на здатність США перекидати сили з батьківщини. Найбільше занепокоєння викликає те, що НАТО бракує детальної ситуаційної обізнаності щодо володіння і контролю КНР над морською інфраструктурою і транспортними вузлами в Європі, а також розуміння того, як така діяльність може перешкоджати мобільності Альянсу.

Більш важливим геостратегічним питанням для НАТО щодо взаємозв'язку між цільовими комерційними інвестиціями КНР в портову інфраструктуру і контролем над глобальними портовими операціями є прагнення Пекіна створити так звані "опорні пункти" для уможливлення військово-морської експансії Народно-визвольної армії Китаю (НВАК) і підтримки майбутніх китайських військово-морських експедиційних сил і засобів для ведення війни. За останнє десятиліття військово-морські сили НВАК розширили свої операції в Середземному і Балтійському морях, а також в Арктичному регіоні. Китайські інвестиції в порти Середземного і Балтійського морів, Індійського океану і уздовж узбережжя Африки забезпечують можливість базування ВМС НВАК, а також створюють потенціал для диверсій, спостереження і збору розвідданих військових кораблів союзників і операцій, які регулярно використовують ці порти і покладаються на них.

Контроль КНР над портовою інфраструктурою Європи і Балтії може сприяти посиленню китайсько-російської військово- морської співпраці. З 2012 року Китай і Росія проводять щорічні двосторонні військово-морські навчання під назвою "Спільне море". Метою цієї серії навчань є вдосконалення тактичних і оперативних можливостей, проведення спільних операцій і підвищення оперативної сумісності між китайськими і російськими військово-морськими силами. Нещодавні навчання "Спільне море" проходили в суперечливих місцях - в тому числі в Середземному морі (2015 рік), Південно-Китайському морі (2016 рік) і Балтійському морі (2017 рік) - що відображає відповідну підтримку Пекіном і Москвою ключових пріоритетів безпеки один одного.

Ці події спонукали НАТО винести мобільність і логістику на передній план операцій з розгортання і забезпечення сил і засобів. На Брюссельському саміті НАТО 2018 року було зроблено остаточну заяву п р о важливість розгортання, мобільності і забезпечення сил: "Ми прагнемо посилити нашу здатність розгортати і підтримувати наші війська і їхню техніку в Альянсі і за його межами і прагнемо поліпшити військову мобільність на суші, в повітрі і на морі якнайшвидше, але не пізніше 2024 року". В результаті було створено два нових командування НАТО.

По-перше, у 2020 році почало діяти Командування об'єднаних збройних сил (JFC-NF) в Норфолку, штат Вірджинія. Його місія полягає в забезпеченні і захисті морських ліній зв'язку і безпеки в Атлантичному океані з огляду на зростаючу присутність російських підводних човнів і майбутню діяльність ВМС НВАК в Північній Атлантиці. По-друге, НАТО створила Об'єднане командування з підтримки і забезпечення (JSEC) в Ульмі, Німеччина, під оперативним командуванням SACEUR для підтримки, координації і гарантування швидкого пересування військ і техніки через європейські кордони. За словами речниці НАТО Оани Лунгеску, "нове командування в Ульмі допоможе нашим силам стати більш мобільними і забезпечують швидке підкріплення в рамках Альянсу, гарантуючи наявність потрібних сил в потрібному місці і в потрібний час".

На додаток до створення JFC-NF і JSEC, НАТО значно розширила свої навчання, зосередившись на логістиці як сфері ведення війни. Наприклад, навчання "Трайдент джанкче" у 2018 році були найбільшими навчаннями НАТО з часів холодної війни і мали на меті продемонструвати здатність Альянсу до спільних дій в рамках операції за статтею 5.46 Нещодавні навчання "Стедфаст дефендер - 21" перевірили готовність і військову мобільність НАТО від Північної Америки до Чорноморського регіону, в яких брали участь як об'єднані об'єднані збройні сили ОЗС НАТО в Північній Америці, так і об'єднані об'єднані сили ОЗСЄС. Метою цих навчань, під час яких сили розміром з дивізію були перекинуті зі Сполучених Штатів до Європи і вимагали від цих сил вивезти техніку з армійських складів в Європі, а потім перемістити особовий склад і техніку через театр бойових дій до кількох полігонів, було перевірити швидке підкріплення північноамериканськими силами за сценарієм, який передбачав відмову в доступі до критично важливих європейських портів.

Європейська ініціатива стримування США - до 2018 року відома як Ініціатива європейського запевнення - стала ще одним важливим механізмом, за допомогою якого Сполучені Штати посилили передову присутність і підтримку своїх сил в Європі. Основна увага в рамках Ініціативи європейського стримування була зосереджена "на стійкому спільному прийомі, розміщенні, подальшому переміщенні і інтеграції (JRSOI), що призвело до поліпшення інфраструктури аеродромів та інших транспортних вузлів, а також до попереднього розміщення запасів". Спільно з НАТО ЄС у координації з НАТО вирішує питання військової логістики приймаючої країни за допомогою проекту Постійної структурованої співпраці, спрямованого на посилення військової мобільності і забезпечення ефективного переміщення військ і техніки через європейські кордони.

##### Гібридні загрози для оборонно**-**промислового комплексу США та Європи Бази

Китай, зокрема, поставив собі за національну мету придбання іноземних технологій для розвитку своєї економіки і модернізації збройних сил. Він всебічно націлений на передові технології США.

технології та люди, інформація, бізнес і дослідницькі

установи, які їх підтримують.

Карі А. Бінген, 2018 р. - тодішня заступниця заступника міністра оборони США з питань розвідки

Для досягнення цієї національної мети Китай використовує ефективне поєднання промислової, торговельної та інвестиційної політики. Китайські аналітики здебільшого зосереджуються на незаконних засобах придбання КНР цих технологій через шпигунство, кібероперації, обхід обмежень експортного контролю США, а також через примусові вимоги щодо обміну інтелектуальною власністю з іноземними компаніями, які інвестують в китайський ринок. Лише нещодавно в центрі уваги опинилися китайські стратегічні інвестиції за кордоном - за допомогою підтримуваних Пекіном інвестиційних структур, таких як Китайська інвестиційна корпорація і великі суверенні інвестиційні фонди - в оборонно- промислові сектори США і країн-членів НАТО. Пекін використовує три інвестиційні інструменти: прямі іноземні інвестиції і придбання американських і європейських компаній подвійного призначення; інвестиції в інфраструктуру BRI, особливо в країнах Балтії і Південної Європи; і просування китайських державних і приватних компаній-лідерів до домінування на ключових ринках - особливо в телекомунікаціях - в рамках стратегії Пекіна "Вийти назовні" ("Go Out"). У сукупності ці заходи є потенційними гібридними загрозами для США і НАТО, оскільки вони призводять до того, що КНР отримує доступ і контроль над ключовими об'єктами інфраструктури ПДБ під час кризи. Існує також довгострокове створення стратегічних залежностей, які уможливлюють примус, використання розвідданих і засоби для розколу Європи і послаблення солідарності Альянсу.

Що стосується прямих іноземних інвестицій та придбань Китаю в європейському ЦПІ, то прикладом може слугувати поглинання у 2008 році британської компанії Dynex Semiconductor дочірньою компанією великої державної залізниці China South Rail. Це поглинання дозволило НВАК виробляти біполярні транзисторні напівпровідники з ізольованим затвором - критичний компонент електромагнітних систем запуску літаків, що використовуються для авіаносців і залізничних гармат ВМС НВАК наступного покоління. Іншим гучним прикладом 2016 року стало придбання китайською Midea Group робототехнічної компанії Kuka, ключового гравця німецької Індустрії 4.0.

Пекін також зробив значні інвестиції в південноєвропейські електромережі. Наприклад, Державна електромережева корпорація Китаю (SGCC) інвестувала значні кошти в операторів електромереж у Португалії та Італії. У 2012 році SGCC стала основним акціонером Redes Energéticas Nacionais, національної енергетичної компанії Португалії, що зробило її домінуючим акціонером в португальській енергосистемі. Аналогічно, інше китайське державне підприємство, China Three Gorges, прагнуло отримати контроль, збільшивши свою 23-відсоткову частку в Energias de Portugal, найбільшій португальській енергетичній компанії, активи якої включають дамбу Алкева. У 2014 році SGCC придбала частку в італійській CDP Reti, яка володіє мережами передачі газу та електроенергії, а в 2017 році - 24% акцій ADMIE, незалежного оператора електромереж у Греції. Завдяки цим стратегічним покупкам Пекін контролює великі взаємозв'язки південноєвропейської енергосистеми.

Слід зазначити, що стратегії придбання китайськими державними компаніями електромереж не були настільки успішними в Північній Європі. Наприклад, спроби придбати 14% акцій бельгійського дистриб'ютора газу та електроенергії Eandis і 20% акцій німецької високовольтної енергетичної мережі 50 герц зазнали н е в д а ч і .53 Будучи провідним світовим постачальником трансформаторів, Китай створює проблему залежності від ланцюга поставок і занепокоєння щодо цілісності для безпеки енергосистем США і Європи. У 2020 році тодішній президент Дональд Трамп видав указ 13920 "Про безпеку об'єднаної енергетичної системи США", зосередивши увагу на корупції в ланцюгах постачання трансформаторів та іншого об'ємного енергетичного обладнання, а також на небезпеці використання супротивником скомпрометованого обладнання для відключення електроенергії оборонним об'єктам та іншим важливим державним установам.

І Росія, і Китай також використовували іноземні інвестиції в стратегічні географічні місця для збору розвідувальної інформації про США і НАТО і їх військові пересування. Добрим прикладом є російська компанія з нерухомості у Фінляндії Airiston Helmi, яка була створена для розміщення російського персоналу і великих транспортних платформ у стратегічно важливому районі фінського архіпелагу. Airiston Helmi також зручно розташована вздовж головної транзитної протоки для вантажних суден, поблизу місця базування бойових кораблів ВМС Фінляндії, а також поблизу ключових кабелів зв'язку, що проходять по морському дну. Так само в 2016 році Anbang Group - китайська компанія з тісними зв'язками з Пекіном - намагалася придбати культовий готель Hotel del Coronado на острові Коронадо в Сан- Дієго, де розташовано кілька ключових об'єктів ВМС США на тихоокеанському узбережжі, таких як військово-морська база десантних військ Коронадо, військово-морське командування спеціальних операцій і військово-повітряна станція Норт-Айленд, де дислокується авіаносна ударна група 1.55 По той бік Атлантики, в Шотландії, інша китайська компанія придбала готель Rosslea Hall, всього за кілька миль від Фаслейну, який є портом базування всього британського флоту - чотирьох атомних підводних човнів класу "Авангард" з балістичними ракетами - єдиного засобу ядерного стримування Великої Британії, а також восьми атомних ударних підводних човнів.56

Нещодавні аналітичні дослідження зосереджувалися на шкідливих інвестиціях КНР у європейські ЦІ в рамках китайської ініціативи BRI.57 Під загальною парасолькою BRI Китай започаткував ініціативу "17+1", яка включає 12 країн-членів ЄС та п'ять балканських країн, з основними інфраструктурними кредитами, спрямованими на будівництво високошвидкісних залізничних мереж, портової інфраструктури, телекомунікацій, мостів та автомагістралей. Незважаючи на членство в НАТО, кілька південноєвропейських країн - зокрема, Італія, Греція та Португалія - приєдналися до БРІ, надаючи Китаю критичні ворота і транс'євразійський плацдарм для виходу на ринок ЄС. Можна стверджувати, що китайські інвестиції в рамках БРІ в Європі є частиною цілеспрямованої стратегії Пекіна, спрямованої на економічно слабших членів ЄС і НАТО і втягнення їх в орбіту Китаю. Крім того, підводні телекомунікаційні кабелі "Цифрового шовкового шляху" КНР, що з'єднують Китай з Європою, підняли привид комунікаційної залежності приймаючої країни НАТО від майже рівного собі конкурента. Підводні кабелі мають важливе стратегічне значення. Приблизно 400 підводних кабелів передають 98 відсотків міжнародних інтернет-даних і телефонного трафіку по всьому світу. Американські компанії здебільшого володіють і експлуатують ці телекомунікаційні лінії, забезпечуючи відчуття безпеки Сполученим Штатам і членам Альянсу які занепокоєні диверсіями або стеженням. Китайські компанії Huawei Marine і Hengtong Optic-Electric Company, третім за величиною акціонером якої є Huawei Technologies, будують високочутливий кабель "Мир", який буде прокладений суходолом з Китаю до Пакистану, потім під водою через Африканський Ріг до кінцевого пункту в портовому місті Марсель, Франція. Huawei Technologies також виробляє обладнання для наземних станцій кабелю "Мир" і його підводного передавального пристрою. Таке стратегічне позиціонування надає національному телекомунікаційному гіганту КНР можливість перенаправляти або відстежувати трафік даних, або, в разі конфлікту, розірвати зв'язок з країнами. Одним із прикладів такої вразливості підводних комунікацій є кабель передачі даних Arctic Connect, який з'єднає Азію і Європу північним морським шляхом уздовж арктичного узбережжя. Говорячи про цю глобальну проблему безпеки, тодішній державний секретар США Майк Помпео закликав міжнародне співтовариство "забезпечити, щоб підводні кабелі не були підірвані для збору розвідданих Китайською Народною Республікою в гіпермасштабних масштабах".

Стратегічне проникнення Китаю в ключові сектори інфраструктури оборонно-промислового потенціалу через просування своїх державних підприємств і національних лідерів - особливо в галузі телекомунікацій 5G - має величезний потенціал для підриву оборонно-промислового потенціалу США і Європи і створення вразливої залежності від ланцюгів постачання. Нещодавня пропозиція компанії Huawei забезпечити інформаційно-комунікаційні мережі 5G в США і Європі є дуже актуальною і викликає певні занепокоєння НАТО з приводу безпеки частково тому, що мережі 5G також набагато вразливіші до кібератак, ніж їхні попередники. Наприклад, чи повинні Сполучені Штати і Європа залежати від Китаю в забезпеченні ключової інфраструктури подвійного призначення DIB? Чи не використає КНР 5G як "троянського коня" для комерційного і військового шпигунства та гібридних загроз, контролюючи світову бездротову і телекомунікаційну магістраль, і чи не буде вона використовувати його в якості "троянського коня"?

Залежність від ланцюгів постачання 5G КНР створює додаткову проблему вразливості систем і компонентів. Нещодавні вторгнення SolarWinds в урядові та приватні мережі США, які були здійснені через скомпрометовані ланцюжки постачання програмного забезпечення, підкреслюють саме цю проблему вразливості. Сполучені Штати і НАТО добре усвідомлюють вразливість оборонних ланцюгів постачання, що містять матеріали китайського виробництва, а також наслідки впровадження технологій КНР в системи зв'язку, особливо зважаючи на те, що більшість військових комунікацій здійснюється через комерційну телекомунікаційну інфраструктуру. Дійсно, в останній Національній стратегії контррозвідки США підкреслюється, що супротивники націлені на вразливі місця в ланцюгах постачання і проводять інші операції перед атакою, щоб "експлуатувати, підривати і завдавати шкоди критично важливим об'єктам інфраструктури і військовому потенціалу США і країн Альянсу під час кризи".

У Сполучених Штатах реакція адміністрації Трампа на спроби Huawei домінувати на американському ринку 5G була швидкою і рішучою. Вона заборонила Huawei брати участь у всіх федеральних контрактах на постачання телекомунікаційного обладнання та послуг, а державним підрядникам США також було заборонено вести бізнес з Huawei. У січні 2019 року Міністерство юстиції США висунуло офіційні звинувачення у шахрайстві, перешкоджанні правосуддю та крадіжці комерційної таємниці проти Huawei. Адміністрація Трампа також чинила значний політичний тиск на своїх союзників у розвідувальному співтоваристві "П'ять очей" - Австралію, Канаду, Нову Зеландію, Велику Британію та Сполучені Штати - з метою заборонити Huawei на їхніх ринках.

Занепокоєний більшими наслідками китайських інвестицій та іншої ворожої діяльності, пов'язаної з інфраструктурою ОПК, Конгрес США ухвалив Закон про модернізацію оцінки ризиків іноземних інвестицій від 2018 року, який розширив повноваження Комітету з іноземних інвестицій у США, щоб запобігти отриманню іноземними супротивниками контролю над активами оборонно-промислової інфраструктури. У 2018 році тодішній президент Трамп видав указ №13806, який зобов'язав провести оцінку ширшого сектору ОПК США. За результатами цієї оцінки було зроблено висновок: "Усі аспекти виробничої та оборонно-промислової бази наразі перебувають під загрозою в той час, коли стратегічні конкуренти і ревізіоністські сили, як видається, зростають у силі і можливостях".

На противагу цьому, Європа розділилася у визнанні та усвідомленні потенційних вразливостей і залежностей у сфері безпеки, які створюють китайські інвестиції в інфраструктуру. Навіть тоді, коли Європа починає усвідомлювати стратегічну важливість китайських інвестицій в інфраструктуру.

Незважаючи на наслідки інвестицій КНР, підхід до Китаю з боку урядів країн-членів Альянсу залишається дуже нерівномірним. У жовтні 2019 року тодішня канцлерка Ангела Меркель дозволила китайським компаніям Huawei і ZTE розширити доступ до німецьких мереж 5G. Оскільки Німеччина є одночасно ключовим членом НАТО і найбільшим двостороннім торговельним партнером Китаю, рішення Меркель має численні наслідки для міжнародної безпеки. Один з аналітиків НАТО стверджує, що воно загрожує безпеці НАТО і операціям збройних сил США, що базуються в Німеччині, і суперечить попередженням американської розвідки.

Використовуючи свою присутність в європейській інфраструктурі ДІБ, Пекін неодноразово користувався потужним політичним впливом і ефективним правом вето в ЄС. Угорщина та Греція, наприклад, намагалися заблокувати будь-які прямі згадки про Китай у заяві ЄС щодо рішення Постійної палати третейського суду в Гаазі, яка відхилила законні претензії КНР у Південно-Китайському морі. В іншому гучному інциденті Греція заблокувала заяву ЄС в Організації Об'єднаних Націй з критикою ситуації з правами людини в Китаї.67 Б'ючи на сполох щодо довгострокових наслідків європейських інвестицій в BRI для єдності ЄС, Зігмар Габріель, тодішній міністр закордонних справ Німеччини, попередив: "Якщо нам не вдасться, наприклад, розробити єдину стратегію щодо Китаю, то Китаю вдасться розділити Європу".

Безпека і залежність критично важливої інфраструктури приймаючої країни - таких як кабелі передачі даних, мережі 5G, електромережі, транспортна і логістична інфраструктура - від Китаю викликає занепокоєння в НАТО. Участь Китаю в ключових інфраструктурних проектах в Європі викликає занепокоєння і привертає дедалі більшу увагу НАТО до намірів Пекіна і необхідності вироблення спільної політики Альянсу щодо Китаю. З нагоди 70-го ювілейного засідання НАТО в Лондоні в грудні 2019 року Генеральний секретар Єнс Столтенберг попередив: "Ми бачимо, що зростання могутності Китаю змінює глобальний баланс сил ... ми повинні звернути увагу на той факт, що Китай наближається до нас, інвестуючи значні кошти в інфраструктуру Тому, звичайно, це має певні наслідки для НАТО".

Нещодавній звіт НАТО більш прямо вказує на потенційні наслідки, які здатність супротивника проникнути в інфраструктуру DIB м о ж е мати для безпеки НАТО: "Масштаби і вплив прямих іноземних інвестицій в стратегічні сектори - такі як аеропорти, морські порти, виробництво і розподіл енергії або телекомунікації - в деяких країнах Альянсу ставлять під сумнів можливість збереження доступу і контролю над такою інфраструктурою, особливо під час кризи, коли вона необхідна для підтримки військових". Поступовий прогрес був досягнутий останнім часом завдяки новому регламенту ЄС, який встановлює рамки для перевірки прямих іноземних інвестицій в європейську критично важливу інфраструктуру і технології. У 2019 році ЄС створив систему перевірки іноземних інвестицій з міркувань безпеки і громадського порядку, але залишив окремим країнам-членам повноваження з перевірки і прийняття рішень.71 Як і в питаннях енергетичної безпеки, НАТО намагається подолати залежність від інфраструктури європейських приймаючих країн і вразливість, яку ця залежність створює для логістики, захищеного зв'язку, оперативної сумісності та інших вимог, необхідних для мобілізації, розгортання і забезпечення сил і засобів.

### **Заходи НАТО з усунення**

**вразливостей від гібридних загроз**

НАТО розробила багатогранний і слабо скоординований підхід до подолання вразливості критично важливої інфраструктури, спричиненої гібридними загрозами з боку супротивників. Початкові зусилля Альянсу були зосереджені на розбудові організаційної спроможності шляхом створення Центрів передового досвіду (ЦПО) НАТО на підтримку захисту критично важливої інфраструктури. Основними прикладами таких центрів є Центри досконалості за такимитнапрямами, як: Захист від тероризму (Анкара, Туреччина) в 2004 році; Спільний кіберзахист (Таллінн, Естонія) в 2008 році; Енергетична безпека (Вільнюс, Литва) в 2012 році; і Морська безпека (Стамбул, Туреччина) в 2020 році. Діяльність цих центрів була з протидії гібридним загрозам, що базується в Гельсінкі, Фінляндія. Разом ці ЦПО підвищують обізнаність і підтримують безпеку та стійкість критично важливої інфраструктури шляхом навчання, освіти та обміну передовим досвідом між урядовцями, науковцями, представниками приватного сектору та іншими профільними експертами.

Паралельно НАТО розробила вкрай необхідну політичну основу для реагування на гібридні загрози колективній обороні Альянсу. Ця політика була оприлюднена на Брюссельському саміті 2018 року. У декларації саміту НАТО підтвердила, що хоча "головна відповідальність за реагування на гібридні загрози покладається на країну, проти якої спрямована атака, НАТО готова, за рішенням Ради, надати допомогу члену Альянсу на будь-якому етапі гібридної кампанії. У випадках гібридної війни Рада може прийняти рішення про застосування статті 5 Вашингтонського договору, як у випадку збройного нападу".

НАТО також розробила і розгорнула інструменти для посилення стійкості критично важливої інфраструктури країн- членів. Інструментарій НАТО з протидії гібридним загрозам включає в себе кращу обізнаність про ситуацію завдяки більш цілеспрямованому обміну розвідданими і інформацією шляхом створення в 2017 році в штаб-квартирі НАТО об'єднаного відділу розвідки і безпеки, а також інших механізмів обміну інформацією з ЄС і приватним сектором. Додаткові приклади передового досвіду в галузі обміну інформацією і розвідданими див. в розділі 11. Ініціатива "Спільна кіберзахист" посилила допомогу в галузі кіберзахисту завдяки розгортанню мобільних груп реагування на комп'ютерні надзвичайні ситуації і кращій координації сил і засобів реагування на комп'ютерні надзвичайні ситуації і інциденти між ЄС і НАТО. Огляд рекомендацій з удосконалення сил і засобів кібербезпеки див. у главі 14.

Інші ініціативи зосереджені на аналізі енергетичної взаємозалежності країн-членів НАТО і вразливості до гібридних загроз і втручань, а також на заходах з пом'якшення наслідків для підвищення стійкості енергетичної інфраструктури в Європі. Про ці загрози та інтеграцію енергетичної інфраструктури України в європейську мережу йдеться в розділі 5. НАТО дедалі частіше використовує навчання і військові ігри, такі як "Дефендер - 21" і "Локдаун шилдз", для виявлення гібридних загроз критично важливим об'єктам інфраструктури, які можуть підірвати розгортання сил і засобів НАТО і їхню логістику. Наприклад, "Локд шилдс" - це щорічні навчання, які дають змогу експертам з кібербезпеки удосконалювати свої навички захисту національних інформаційно-технологічних систем та іншої критично важливої інфраструктури від атак в режимі реального часу. Крім того, НАТО створила групи антигібридної підтримки, які можуть бути задіяні в кризових ситуаціях або для допомоги в розбудові національних антигібридних сил і засобів. НАТО вперше розгорнула одну з них

Ці команди з протидії гібридним загрозам були створені в листопаді 2019 року на допомогу Чорногорії, тоді ще новому члену НАТО, в її зусиллях з пом'якшення вразливості критичної інфраструктури до гібридних загроз.

Визнаючи, що НАТО залежить від критично важливої інфраструктури приймаючої країни, яка належить і експлуатується переважно приватним сектором, останнім часом зусилля НАТО були зосереджені на посиленні стійкості цивільної інфраструктури Альянсу до гібридних загроз і атак і на її відновленні після них. Власники і оператори об'єктів критичної інфраструктури приватного сектору, керуючись бізнес-моделями витрат, часто не інвестують в створення резервів або впровадження заходів кібербезпеки, що робить їх вразливими до гібридних загроз - про що дуже добре свідчать численні нещодавні кібератаки на ключові об'єкти глобальної критичної інфраструктури.

Принцип стійкості закріплений у статті 3 Вашингтонського договору, яка визначає першу лінію оборони НАТО як обов'язок кожного члена Альянсу "підтримувати і розвивати індивідуальну і колективну здатність протистояти збройному нападу" шляхом "постійної і ефективної самодопомоги і взаємодопомоги".74 НАТО визнає, що в динамічному середовищі гібридних загроз, про які йшлося вище, дедалі частіше виникає потреба у вищому рівні національної стійкості. На Варшавському саміті 2016 року НАТО оголосила про впровадження семи базових вимог до країн для вимірювання і поліпшення національної стійкості і цивільної готовності. Ці вимоги передбачають посилення стійкості в семи стратегічних секторах: безперервність державного управління, енергетика, переміщення населення, продовольчі і водні ресурси, масові жертви, цивільні комунікації і транспортні системи.75 На підтримку цих зусиль НАТО створила групи консультативної підтримки стійкості, які надають експертні знання і допомагають країнам-членам оцінювати і розбудовувати стійкість.

Ці різноманітні заходи відіграли надзвичайно важливу роль у винесенні на передній план подвійної проблеми безпеки і стійкості критично важливої інфраструктури і забезпеченні вкрай необхідної координації між ЄС, НАТО і окремими державами. Проте НАТО все ще потрібно розшифрувати ключові інфраструктурні залежності приймаючої країни і визначити, де вразливі місця в приватній або іноземній власності на критично важливу національну інфраструктуру можуть перешкоджати виконанню місій, пов'язаних із застосуванням сили, мобільністю і підтримкою операцій в умовах гібридних загроз, що викликають суперечки. Визначення ключових функцій місії з підтримки критичної інфраструктури і пов'язаних з ними вразливостей - це підхід, який міністерство застосовує в США і який може бути поширений на НАТО.

Із запровадженням у 2012 році Стратегії забезпечення виконання місій відбулася значна зміна парадигми: від захисту об'єктів оборонної КІ до посилення стійкості місій Міністерства оборони. Стратегія визначає забезпечення місії як "процес захисту або забезпечення безперервного функціонування і стійкості сил і засобів, в тому числі персоналу, обладнання, об'єктів, мереж, інформації та інформаційних систем, інфраструктури і ланцюгів постачання, які є критично важливими для виконання основних функцій місії ( MEFS) Міністерства оборони в будь-якому операційному середовищі або за будь- яких умов". Визнаючи, що понад 90 відсотків інфраструктури США знаходиться в приватному секторі, стратегія також закликає до зміцнення партнерства Міністерства оборони з цими власниками і операторами комерційної інфраструктури. Стратегія була доповнена іншими політичними директивами, які вимагають від усіх служб, департаментів і агентств Міністерства оборони керівних принципів і процедур для виявлення, оцінки, управління і моніторингу ризиків для стратегічних місій.77 Наразі програми забезпечення місій на рівні Об'єднаного штабу, Офісу міністра оборони і служб поширюються на об'єкти, розташовані на континентальній частині США, а також на допоміжну внутрішню критично важливу інфраструктуру. Таким чином, для Міністерства оборони існує ключова можливість співпрацювати з НАТО над впровадженням програми забезпечення місій, яка б передбачала ретельну оцінку і управління ризиками, моделювання і визначення залежностей критично важливої інфраструктури з використанням спеціальних знань і досвіду, таких як Аргонська національна лабораторія, і передбачала б добре перевірені заходи з пом'якшення наслідків для забезпечення стійкості критично важливої інфраструктури і резервування життєво важливих вузлів для наборів місій НАТО.

### Висновок

Супротивники активно атакують об'єкти критичної інфраструктури США і НАТО з метою підриву військового потенціалу, проекції сили, мобільності і життєзабезпечення. У деяких випадках супротивники проникають в цю інфраструктуру з метою виявлення вразливих місць для подальшої експлуатації, а в інших випадках об'єкти критичної інфраструктури стають зброєю як форма гібридної загрози. Поки Сполучені Штати і НАТО долають виклики цієї поточної і майбутньої форми загрозливої діяльності, країнам-партнерам доцільно вивчати їхній досвід. Інтернаціоналізація інвестицій і ланцюгів постачання в поєднанні зі стрімким розвитком комунікацій, обчислювальної техніки, штучного інтелекту та інших технологій створює нову глобальну і регіональну взаємозалежність критично важливих об'єктів інфраструктури. Ця нова інфраструктурна взаємозалежність вимагатиме посилення координації між цивільним і військовим та державним і приватним секторами.

# - 5 -

## Європейська енергетика та випадок України

Тереза Сабоніс-Хелф

Розвинені держави потребують безперервного надходження енергоресурсів як з внутрішніх, так і з зовнішніх джерел. У воєнний час здатність постачати паливо на поле бою може мати вирішальне значення. Навіть у мирний час відмова від енергоресурсів може мати катастрофічні наслідки. Припинення постачання нафти може призвести д о зупинки транспорту; припинення постачання газу занурює суспільство в опалювальну, електричну та промислову кризу; а відключення електроенергії занурює населення в темряву і тишу. Хоча будь-які перебої в постачанні створюють критичні проблеми, вразливість електроенергетичних систем набуває все більшої актуальності. Інтенсивність використання даних у повсякденному житті та суспільні зусилля зі скорочення викидів парникових газів спонукають сучасне суспільство все більше рухатися до електрифікації.

Хоча електрифікація є більш важливою у двадцять першому столітті, електроенергетична інфраструктура Заходу залишається продуктом двадцятого століття, створюючи нові стратегічні виклики для колективного мислення про безпеку та стійкість. Потенційні перебої в електропостачанні стають все більш катастрофічними для урбанізованих територій і водночас більш привабливими для суб'єктів, які прагнуть підриву. Одночасно розширюються можливості для підриву: оскільки системи стають більшими, "розумнішими" і більш міжнародно пов'язаними, з'являються нові технології, що впроваджуються в електромережу, відкривають нові шляхи для атак. Тісний взаємозв'язок між безпекою електроенергії та кібербезпекою вимагає розуміння безпеки та стійкості критичної інфраструктури (CISR), що враховує обидва типи вразливостей. Тут приклад України є повчальним. Досвід України в галузі енергетичної безпеки і кібербезпеки за останні роки розкриває значні ризики і дає уявлення про зусилля Організації Північноатлантичного договору з посилення цивільної готовності і колективної безпеки і стійкості критичної інфраструктури серед членів і партнерів Альянсу, в тому числі і України. Він також ілюструє складнощі, які чекають на нас попереду.

Зсув попиту на всю енергію в бік електричної енергії очевидний у ринкових і політичних тенденціях. У 2018 році на електроенергію припадало 19 відсотків загального світового споживання енергії, але ця цифра стрімко зростає. У своєму звіті 2021 *Net Zero до 2050 року* Міжнародне енергетичне агентство (МЕА) зазначило, що якщо світ хоче досягти своїх цілей щодо боротьби зі зміною клімату, то до 2040 року електроенергія повинна становити майже половину всієї енергії. Це був значний перегляд у бік збільшення порівняно з прогнозом 2019 року, згідно з яким частка електроенергії зросте до 20-31 відсотка до цієї дати. Очікується, що Європейський Союз очолить цей перехід на основі своєї політики. Політика ЄС сприяє інвестуванню в транскордонні електроенергетичні проекти, а політика, спрямована на створення щонайменше 30 мільйонів електромобілів до 2030 року, призвела до того, що продажі електромобілів потроїлися з 2019 року.

Значне підвищення ефективності, можливості для збільшення використання відновлюваних джерел енергії та скорочення викидів - все це може бути результатом зростання залежності від електромереж, але ця зміна також означає зміну ризиків для критичної інфраструктури. Системи питного водопостачання та водовідведення, продукти харчування, охорона здоров'я, зв'язок та фінансові послуги залежать від надійного електропостачання. Про взаємозв'язок між секторами життєзабезпечення та іншими секторами критичної інфраструктури див. розділ 1. Крім того, у світі зростає попит на електроенергію з боку центрів обробки даних, які вже зараз є одними з найбільших споживачів електроенергії.

За оцінками експертів, до 2030 року глобальний попит на електроенергію для центрів обробки даних збільшиться у 15 разів. Подальша електрифікація автопарку також зробить транспорт більш залежним, а інтеграція мереж збільшує можливість поширення вразливостей.

Хоча цей перехід до електрифікації несе нові ризики, країни-імпортери енергоресурсів у минулому продемонстрували здатність успішно протистояти новим ризикам в енергетичному секторі. У цьому розділі ми пропонуємо короткий огляд еволюції європейських підходів до безпеки енергопостачання з акцентом на сучасні проблеми, пов'язані з безпекою електромереж. Останніми роками Україна зазнала значних перебоїв в роботі електромереж, і Європа реалізує стратегію посилення енергетичної безпеки України шляхом тіснішої прив'язки її систем до європейських - стратегію, яка вимагає значних змін у політиці та стратегії як для України, так і для ЄС.

### Коротка історія європейської енергетичної безпеки Занепокоєння

Безпека енергопостачання вже давно є стратегічним питанням для держав-імпортерів. Коли Вінстон Черчилль, тодішній перший лорд адміралтейства, оголосив у 1911 році про своє рішення перевести Королівський військово- морський флот з вугільних на нафтові лінкори, він прийняв свідоме рішення обміняти безпеку постачання вугілля на швидкість і гнучкість нафти, навіть якщо вона буде імпортованою. Він, як відомо, стверджував, що "безпека і впевненість у нафті лежать лише в різноманітності та різноманітності". Відтоді безпека постачання - через численні маршрути, численних постачальників і надійний транспорт - залишається військовим і зовнішньополітичним пріоритетом для європейських держав. У кожну епоху кризи з постачанням енергоресурсів спонукали до інновацій і стратегій колективної безпеки. Під час Другої світової війни операція "Плутон", таємний проект зі створення та експлуатації підводного трубопроводу для постачання нафти через Ла-Манш, мала вирішальне значення для успіху вторгнення в Нормандію і створила прецедент для підводних трубопроводів, які сьогодні є основним засобом передачі енергії.7 Енергопостачання було вразливим місцем для обох сторін

Історики наводять численні докази того, що держави Осі страждали від ключової вразливості нафтового сектору і намагалися порушити постачання союзників.

Першим великим шоком для постачання в мирний час стала нафтова криза 1973 року. Паніка і цінова спіраль, що виникли в результаті цілеспрямованого скорочення пропозиції, змусили країни-імпортери створити МЕА. Згідно з договором МЕА, країни-члени зобов'язані створювати стратегічні запаси нафти, що дорівнюють 90 дням чистого імпорту нафти, і ділитися цими запасами у випадку кризи. Хоча обов'язкове спільне використання резервів застосовувалося лише тричі в історії МЕА, підтримка стратегічних резервів стала вважатися найкращою практикою.

Після Іранської революції світ пережив другий нафтовий шок у 1970-х роках, який змусив Європу почати розглядати альтернативні види палива і перейти на імпорт природного газу. На чолі з Західною Німеччиною Європа вирішила побудувати газопровід з Сибіру до Європи, щоб вирішити проблему надмірної залежності від нестабільної Перської затоки. Незважаючи на заперечення США та ембарго на постачання обладнання, трубопровід протяжністю 3300 миль і потужністю 32 мільярди кубометрів на рік був завершений у 1984 році. Європа пообіцяла, що її залежність від поставок радянського газу не перевищуватиме 30 відсотків. Цей "прийнятний рівень залежності" став стандартною практикою в радянський період і стимулював імпорт газу з Північної Африки на додаток до радянського природного газу. На думку дослідника енергетики Тана Густафсона, економічна необхідність взяла гору над політичними міркуваннями як для Радянського Союзу, так і для європейців. Радянський Союз, економіка якого у 1980-х роках розвалювалася від десятиліть централізованого контролю, став настільки ж залежним від валютних надходжень від продажу природного газу, наскільки Європа була залежна від радянських вуглеводнів. Прагнучи утримати цей важливий ринок, Москва зберегла репутацію надійного постачальника і довела, що вона є послідовним, неполітизованим постачальником для держав, які платять світові ціни.

Європа скористалася перевагами природного газу, який створює менше місцевого забруднення та парникових газів порівняно з іншими викопними видами палива. Він став популярним для виробництва електроенергії, тепла та промисловості, забезпечуючи більшу гнучкість для виробників електроенергії. На відміну від вугільних та атомних електростанцій, виробництво електроенергії на газових станціях можна легко відкалібрувати відповідно до мінливого попиту. Тому електростанції, що працюють на природному газі, можуть працювати з прибутком і меншим фінансовим ризиком у широкому діапазоні сценаріїв попиту, тоді як такі джерела, як вугілля або атомна енергетика, втрачають гроші, якщо не працюють на повну потужність. Газові електростанції також потребують менших початкових капітальних інвестицій та екологічних дозволів, ніж вугільні, атомні та гідроелектростанції, а отже, мають значно коротші терміни введення в експлуатацію.

З огляду на ці переваги, не дивно, що природний газ почав домінувати у виробництві електроенергії в Європі, а також дедалі ширше використовуватися в промисловості. Однак газ створив новий виклик з точки зору безпеки. Якщо постачання нафти можна було забезпечити кількома маршрутами, то постачання природного газу вимагає постійного навантаження і тиску, його складніше зберігати, ніж нафту чи вугілля, і - оскільки ним потрібно управляти по всьому ланцюгу постачання - дає владу операторам газотранспортної системи. Вчений-енергетик Маргарита Балмаседа називає цю проблему *мережевістю*, або "ступенем, до якого загальне функціонування системи може залежати від того, чи працює мережа належним чином *як мережа*".

Ступінь залежності Європи від джерела, яке було дуже залежним від мережі, став очевидним після розширення ЄС у 2004 році, коли до нього увійшли країни, які вже мали радянську інфраструктуру, що пов'язувала їх з Росією, а також давні двосторонні енергетичні відносини з Москвою. На відміну від європейського досвіду неполітизованого постачання, колишні країни Східного блоку мали тривалий досвід політизації як ціни, так і постачання. Чеська Республіка, всі три країни Балтії, Угорщина, Польща, Словаччина та Словенія мали давні енергетичні відносини з Москвою, а Росія намагалася продовжувати двосторонній підхід, підкріплений щорічними контрактами та старою радянською трубопровідною інфраструктурою. З часом, коли напруженість у відносинах з окремими країнами зростала, Росія виявила, що вся Європа втягнута в те, що вона раніше вважала двосторонніми угодами. Крім того, почали виникати проблеми з транзитом. Територія, яка була частиною однієї колишньої радянської держави, тепер стала кількома суверенними державами, а логістика і логіка транзиту стали набагато складнішими, оскільки кожна держава переслідувала свої власні інтереси і стикалася з власними проблемами перехідного періоду.

Суперечки Росії з Україною взимку 2005, 2006 і 2007 років, що виникли через несхвалення Росією антиросійських політичних діячів, а також через несплату Україною законтрактованих обсягів імпорту газу та його зникнення. У грудні 2008 року, коли двосторонні переговори зірвалися і Росія вийшла з них, пообіцявши зменшити обсяги постачання газу в Україну, криза, що виникла, тривала 21 день. Занепокоєння щодо енергетичної вразливості ставало дедалі гучнішим. Наприкінці цієї кризи Європа вирішила знайти підхід, який би обмежив владу Росії у постачанні природного газу. НАТО також відреагувала, визначивши роль Альянсу в енергетичній безпеці на Бухарестському саміті в 2008 році і створивши Центр передового досвіду НАТО з енергетичної безпеки у Вільнюсі в 2012 році.

У 2009 році Європа внесла значні зміни до законів, що регулюють торгівлю енергоресурсами між Росією та Європою. Визнаючи виклик *мережевості*, ЄС прийняв законодавство, відоме як Третій енергетичний пакет, щоб з'єднати європейські енергетичні ринки новими способами і зменшити можливості Москви чинити тиск на окремого члена ЄС. Крім того, ЄС визначив газ та електроенергію як пріоритетні сфери для активного втручання в розвиток інфраструктури. На той час багатьом європейським державам не вистачало інтерконекторів, які б дозволили їм постачати один одному газ у кризових ситуаціях. Створення такої системи інтерконекторів стало критично важливим компонентом обмеження здатності Москви відключати природний газ окремим країнам. Завдяки першій європейській директиві про безпеку газопостачання, потужність міжєвропейських з'єднань значно покращилася - збільшилася

18% у період з 2009 по 2017 рік - за цей період Європа інвестувала в чотири нові транскордонні газопроводи і перетворила дев'ять існуючих ліній на двосторонні з'єднання.17 Подальші вдосконалення були досягнуті шляхом введення вимоги, щоб транзитні держави стали газовими хабами, обладнаними для імпорту газу щонайменше з трьох джерел, а також мали можливість зберігати природний газ.18 Ці дві вимоги призвели до значного збільшення можливостей імпорту зрідженого природного газу (ЗПГ) і, таким чином, зменшили загрозу поставок з наземних монопольних джерел.

Фактичне фізичне руйнування трубопроводів не торкнулося Європи в цю епоху, але в колишньому Радянському Союзі кілька інфраструктурних криз призвели до того, що створення альтернативних маршрутів. Чеченці в Грозному неодноразово руйнували трубопроводи, якими нафта постачалася з Азербайджану до Росії, що змусило Азербайджан у 1994 році розпочати реконструкцію занедбаного нафтопроводу Баку-Супса. Введений в експлуатацію в 1999 році, цей нафтопровід зі скромною пропускною спроможністю (145 000 барелів на день), який пролягав через Грузію до Чорного моря, став доказом того, що Грузія може слугувати ефективним транзитером, незважаючи на громадянські конфлікти в країні. За цим послідувало будівництво нафтопроводу Баку-Тбілісі-Джейхан і паралельного газопроводу Баку-Тбілісі-Ерзурум, які були введені в експлуатацію в 2006 році, незважаючи на тиск з боку Росії.

Європа також відповіла на загрози безпеці поставок шляхом диверсифікації трубопровідних маршрутів. Нові лінії, включаючи "Північний потік І", нещодавно завершений "Північний потік ІІ", "Турецький потік" і Південний газовий коридор - хоча лише останній транспортує неросійський газ - допомагають зменшити загрозу переривання поставок в одному місці. Європа додатково забезпечила безпеку поставок, збільшивши використання ЗПГ. Однак значна різниця у вартості між трубопровідним газом і ЗПГ робить останній більш привабливим як аварійне джерело, ніж постійне. До пандемії COVID-19 середній коефіцієнт використання існуючих LNG- терміналів у Європі становив лише 25%. Крім того, ринок змінюється. Європейський інвестиційний банк заявив про намір поступово припинити інвестиції в газову інфраструктуру до кінця 2022 року. Можна з оптимізмом припустити, що цілі з нульовими викидами будуть досягнуті, оскільки банк вже змінив свій початковий 2021 рік для поступової відмови від викопного палива, але економічна ефективність надлишкової газової інфраструктури знаходиться під великим питанням.

Як показали попередні приклади, зміна джерела - з вугілля на нафту або з нафти на газ - також зміщує ризик. Нова епоха не є винятком. Перехід до відновлюваних джерел енергії надає зростаючу роль електроенергії, і якщо Європа стоїть на порозі електричної ери, то електромережа ХХ століття повинна бути краще зрозумілою і захищеною від загроз ХХІ століття. Відновлювана енергія, як правило, виробляється всередині країни, що зменшує залежність від довгих ланцюгів імпорту, характерних для викопних видів палива. Але для того, щ о б енергосистеми працювали найбільш ефективно, інженерний імператив полягає в тому, щоб

(1) з'єднати їх між часовими поясами, щоб коливання попиту були менш значними,

1. включати країни з різними джерелами, щоб оптимізувати сезонну гідроенергію або сонячну енергію в певний час доби, і
2. створити високофлексибільні ринки, щоб закупівлі електроенергії могли легко змінюватися. З точки зору критичної інфраструктури, ця електромережа є навіть більш *мережевою,* ніж газопроводи, що постачають природний газ. Спільна мережа - це мережа, в якій внутрішня електроенергія повинна бути захищена від зовнішніх атак, а енергетичні партнери, навіть якщо вони є союзниками, повинні дотримуватися високих стандартів, щоб вразливість їхньої системи не поширювалася на більшу мережу.

Європа сповнена рішучості увійти в нову еру електроенергії. Відповідно до Європейського кліматичного закону, прийнятого в 2020 році, ЄС зобов'язаний скоротити викиди парникових газів на 55% від базового рівня 1990 року до 2030 року. За оцінками експертів, це означає, що споживання викопного палива має скоротитися приблизно на 36% з 2020 по 2030 рік, а електроенергія заповнить цю прогалину. Перехід до передачі та зберігання електроенергії чітко простежується в політиці та пріоритетах фінансування ЄС. Список проектів спільного інтересу ЄС на 2019 рік, традиційно зосереджений на стратегічних енергетичних проектах, включає 149 проектів, з яких 100 спрямовані на передачу та зберігання електроенергії, а шість - на розгортання "розумних" електромереж. Генеральний директорат ЄС з питань енергетики розробляє та впроваджує європейську енергетичну політику, спрямовану на створення конкурентного та доступного ринку технологічно передових енергоносіїв; сприяння сталому виробництву, транспортуванню та споживанню енергії відповідно до цілей ЄС щодо декарбонізації до 2050 року; покращення умов для безпечного та надійного енергопостачання "в дусі солідарності між країнами ЄС, що забезпечує високий ступінь захисту європейських громадян".24 Ці прагнення змусили ЄС підкреслити важливість розширення європейської енергосистеми на сусідні держави навіть тоді, коли Європа прагне підвищити стійкість існуючої енергосистеми.

Зміна ринків і поширення маршрутів не зменшили занепокоєння НАТО зростанням загроз енергетичній безпеці, а нова загроза в епоху транскордонної електроенергії є новим стратегічним викликом. НАТО визначила для себе три ролі в енергетичній безпеці:

(1) підвищення обізнаності, включаючи обмін розвідданими про розвиток енергетики;

(2) підтримка захисту критичної енергетичної інфраструктури шляхом включення сценаріїв, пов'язаних з енергетикою, до навчань, обміну передовим досвідом і проведення навчальних курсів;

(3) підвищення енергоефективності у військовій сфері.25 Хоча енергетика залишається переважно внутрішнім і невійськовим питанням, НАТО посилила свою увагу до цих проблем, а також визнала важливий зв'язок між гібридним конфліктом і енергетикою. Детальніше про природу гібридних загроз див. у розділі 4.

Починаючи з чеченської війни, Росія застосовує гібридну стратегію конфліктів у колишніх радянських регіонах. Оскільки гібридні атаки шукають недорогі і високопродуктивні способи впливу на політику держав, НАТО визнала, що енергетика є привабливою мішенню. У 2020 році Науково-технічна рада НАТО офіційно створила дослідницьку робочу групу з питань енергетичної безпеки в епоху гібридної війни. Перед цією групою стоїть завдання проаналізувати "гібридну енергетичну загрозу та її вплив на військову готовність і здатність НАТО виконувати місії, стійкість інфраструктури країн-членів Альянсу та їхню здатність брати участь у місіях НАТО, і, зрештою, на злагодженість Альянсу". Випадок України, ймовірно, посяде чільне місце в їхній оцінці, оскільки він надає багатий набір прикладів зв'язку між гібридною війною і енергетичною безпекою XXI століття.

### Випадок Україна

Україна має багато прикладів тривожного перетину енергетичної безпеки, гібридної війни та кібератак. У грудні 2015 року російські суб'єкти успішно атакували українську енергосистему, що визнано першим хакерським відключенням електроенергії в регіоні та однією з перших кібератак, які призвели до фізичного виведення систем з ладу. Кібер-технології знову вивели з ладу українську енергосистему в грудні 2016 року. Друга атака була більш витонченою і мала на меті (хоча й невдало) завдати довготривалої шкоди енергосистемі. Через рік ще одна кібератака, спрямована на бізнес-сектор України, а не на її інфраструктуру, знову пошкодила електромережу, але більш відома тим, що завдала збитків на суму близько 10 мільярдів доларів США, більша частина з яких була за межами України. Хоча вони відрізнялися за цілями та складністю, кожна кібератака мала певні спільні елементи і, що найважливіше, спільне походження. Міністерство юстиції США встановило, що у 2020 році, що за всіма трьома атаками стояло угруповання "Піщаний черв'як", яке фінансується Головним розвідувальним управлінням Росії.

Країни НАТО зробили значний внесок у якнайшвидше відновлення електропостачання і зменшення майбутньої вразливості. Проте вони виявили, що визначення джерела кібератаки зайняло певний час, що ускладнило організацію дипломатичної відповіді на неї. Кібератаки були особливо проблематичними для ЄС, який вже взяв на себе зобов'язання інтегрувати Україну до власної енергосистеми.

##### Задаючи український контекст**:** Рання енергетика Конфлікт

Незважаючи на свою шокуючу цінність, перша атака на українську енергосистему в грудні 2015 року не була "громом серед ясного неба". Енергетика вже відігравала важливу роль у військових цілях Росії в Україні. Інтенсивна розробка родовищ у Чорному морі біля узбережжя Криму могла б зменшити енергетичну залежність України від Росії, а отже, і важелі впливу Росії. Перемога Росії в Криму коштувала Україні близько 80% її нафтових і газових родовищ у Чорному морі через невизначеність щодо прав на шельф. Крім того, оскільки основні радянські магістральні газопроводи пролягають під Донбасом, Росія припустила, що фізичний контроль над ними, ймовірно, посилить її контроль над поведінкою України. Тому справедливо вважається, що енергетика відіграє важливу роль у досягненні російських цілей у конфлікті.

Поведінка України як транзитної держави - особливо крадіжки російського газу з великих стратегічних запасів - призвела до зниження надійності постачання газу до Європи та зростання занепокоєння з боку Європи щодо її залежності від Росії. З 2014 року Україна передала своє газосховище - одне з найбільших у світі - під контроль європейських регуляторних структур, що підвищило прозорість, зруйнувало амбіції Росії перебрати на себе регулювання цього сховища і забезпечило додаткову безпеку Європи від російських маніпуляцій з цінами та поставками. Як реакція на енергетичну напруженість між країнами, Україна припинила купувати природний газ безпосередньо у Росії у 2015 році і тепер реімпортує газ з Європи, хоча й залишається транзитною державою для Росії. Співпраця між ЄС та США гарантувала, що Росія скоротить використовувати Україну як транзитну державу до 2024 року, незважаючи на бажання Кремля припинити транзит через Україну наприкінці 10-річного контракту, який закінчився в грудні 2019 року. Кожен з цих прикладів ілюструє, що енергетика залишається важливим питанням у російських претензіях.

##### Розпочалася російсько**-**українська війна

Окрім того, що енергетика відігравала певну роль у цілях конфлікту та суперечках між сторонами, вона також була ключовим інструментом конфлікту. Енергетична та водопровідна інфраструктура, спільна для Росії та України, стала фізичною мішенню для лояльних до України суб'єктів на початку війни. Короткий огляд конфлікту допоможе проілюструвати цю тезу.

У лютому 2014 року, після кількох місяців протестів у Києві, тодішній президент Віктор Янукович очолив країну і сформував прозахідний уряд. У березні 2014 року Кримський півострів, більшість населення якого складають етнічні росіяни, проголосував за відокремлення від України і приєднання до Російської Федерації. Голосування, яке зазнало критики через ймовірне втручання Росії, не було визнане ні міжнародним співтовариством, ні Україною. Росія, однак, визнала референдум і анексувала півострів. Невдовзі після анексії місцеві сепаратисти та російські "зелені чоловічки" розпочали сепаратистську війну на Донбасі, який межує з Росією і має етнічну російську більшість. У міру того, як конфлікт затягувався - з 2014 по жовтень 2021 року загинуло понад 10 300 і було поранено майже 24 000 осіб - українські сили обмежили територію, яку утримували сепаратисти, але не змогли їх повністю витіснити. На Рисунку 5-1 показані зони конфлікту в Криму та на Донбасі у 2014 році.31

20 листопада 2015 року, коли на Донбасі ще тривала гаряча війна, лояльні до Києва диверсанти підірвали ключові опори, що з'єднували Крим з українською електромережею, зруйнувавши доступ Криму до української електроенергії. До цього часу Крим продовжував імпортувати 80 відсотків електроенергії в зимовий період з України, незважаючи на своє рішення про відокремлення. Український уряд не взяв на себе відповідальність за саботаж, але й не поспішав усувати завдані збитки.

1,9 мільйона жителів Криму занурилися в темряву. Не маючи наземного сполучення з Кримом, Росія намагалася поставити генератори і налагодити резервне електропостачання для своєї нової республіки-клієнта. Крим все ще перебував у кризовому стані і в значній мірі в темряві, коли 23 грудня 2015 року в Україні сталося перше відключення електроенергії, спричинене кібер- атакою.



Рисунок **5-1.** Зони російсько**-**українського конфлікту **(2014)**

(Карта від Global Security)

Кібервійна починається **(BlackEnergy** та **KillDisk)**

У другій половині дня 23 грудня 2015 року почалося відключення електроенергії в трьох областях України, включаючи Київ. Незважаючи на відчайдушні зусилля операторів, зловмисники змогли дистанційно взяти під контроль понад 50 підстанцій. Багато операторів диспетчерських центрів безпорадно спостерігали, як шкідливе програмне забезпечення анулювало їхні паролі і як віддалено керували. На їхніх екранах з'явилися курсори. До кінця атаки 130 мегават генеруючих потужностей вийшли з мережі, залишивши близько 225 000 споживачів по всій Україні без електроенергії. Ситуацію погіршила атака на телефонний зв'язок, яка використовувала автоматизовані системи для перевантаження телефонів, що унеможливило повідомлення клієнтів про перебої в роботі та ускладнило зв'язок електростанцій одна з одною. Вимкнувши всі системи диспетчерського контролю та збору даних (SCADA) і працюючи в ручному режимі, оператори відновили електропостачання за один-шість годин, але підстанції не працювали в повному обсязі ще кілька місяців.

Зловмисникам вдалося заволодіти системами за допомогою віддалених логінів, отриманих за допомогою фішингових атак та зламу систем передачі даних. Експертний аналіз показав, що атака почалася за шість місяців до цього з відносно складних фішингових атак на електронну пошту, які виглядали як офіційна кореспонденція Міністерства енергетики України. Щонайменше один користувач у кожному з шести цільових центрів розповсюдження став жертвою фішингу, який при відкритті файлу запускав макрос BlackEnergy у ключові системи. Потрапивши в систему, ці макроси завершували розвідку мережі, викрадали облікові дані та паролі і отримували доступ до центру управління, надаючи зловмисникам повну інформацію про систему. У призначений час зловмисники взяли систему під свій контроль, відкривши автоматичні вимикачі, щоб вимкнути системи. Вся операція зайняла приблизно 60 хвилин. Після виведення мережі з ладу зловмисники використали шкідливе програмне забезпечення KillDisk для знищення деяких систем на кожній з трьох головних станцій. Атака була зосереджена на розподільчому секторі, який є найбільш децентралізованим сектором мережі. Понад два місяці потому критичні пристрої на 16 підстанціях залишалися пошкодженими, а вимикачами доводилося керувати вручну.

У попередні місяці шкідливі програми BlackEnergy та KillDisk були виявлені в українських державних установах і завдали їм шкоди. Вони також були знайдені у польських енергетичних компаніях і навіть у деяких енергетичних і водопостачальних компаніях у США. Використання цього шкідливого програмного забезпечення в електромережі все ще шокує, оскільки воно являє собою складне довгострокове планування і, за загальним визнанням, є першим випадком успішного виведення з ладу електромережі через хакерську атаку. Хоча дехто стверджував, що кібератака була відплатою за роль України у відключенні електроенергії в Криму, вторгнення в системи почалися ще в березні, до відключення електроенергії в Криму. Однак є дані, що свідчать про те, що попередній план атаки, можливо, був поспішно реалізований після фізичної атаки на кримську електромережу.

Кібер**-**війна загострюється **(CrashOverride)**

Друга атака на українську електромережу сталася 17 грудня 2016 року. Ця кібератака на електропередавальну станцію під Києвом вивела з ладу 20 відсотків її потужностей. Ця атака була спрямована на об'єкт передачі, а не на об'єкти розподілу, як це було під час попередньої атаки. Автоматизована атака відкрила всі автоматичні вимикачі на ключовій станції передачі. Українська електроенергетична компанія "*Укренерго"* та українські експерти з кібербезпеки стверджували, що ця атака була схожа на першу, але подальший аналіз виявив дещо більш тривожне.

Атака була спланована таким чином, щоб завдати фізичної шкоди електрообладнанню. Команда з кібербезпеки Dragos, яка досліджувала інцидент, дійшла висновку, що відключення електроенергії мало стати першим етапом більш масштабної та амбітної атаки. Під час відключення електроенергії зловмисники здійснили атаку на захисні реле, очевидно, щоб вивести з ладу аварійні пристрої і зробити небезпечним перезапуск мережі. У звіті Драгоса робиться висновок, що хакери мали намір завдати значної шкоди *після* відновлення електропостачання.44 Виходячи з попередньої реакції у 2015 році, зловмисники очікували, що інженери компанії поспішать перезапустити системи вручну. Відключивши пристрої захисту від збоїв, зловмисники розраховували, що працівники, які відновлювали систему, спровокують перевантаження по струму, що потенційно могло призвести до катастрофічні збитки, що призводять до тривалих перебоїв у передачі енергії, пошкодження енергетичних активів і травмування працівників.45 Цей тип кіберпідриву є відносно рідкісним, і, як показує цей випадок, його важко успішно здійснити, але він загрожує серйозними наслідками. Примітно, що це перше застосування кіберзброї було як спонсороване державою, так і спрямоване на енергетичну інфраструктуру, зокрема, на сектори передачі і виробництва електроенергії, від яких залежить вся енергосистема. Див. розділ 14, в якому ця атака розглядається серед 10 найбільших кіберінцидентів.

Хоча атака провалилася, здебільшого через помилки зловмисників, рівень амбіцій і новаторський підхід вражає. Для маніпулювання промисловими системами управління було використано програмне забезпечення, а не ручна взаємодія хакерів у реальному часі з системами, як це було у 2015 році. Зловмисники використовували шкідливе програмне забезпечення, відоме як CrashOverride. Це шкідливе програмне забезпечення націлене на захисні реле, які автоматично розмикають автоматичні вимикачі, якщо небезпечні умови загрожують пошкодженням трансформаторів. Зловмисники знали, що в реле є функція безпеки, яка дозволяє перевести їх у режим оновлення мікропрограми, що зробить реле непридатними до використання до моменту ручного перезавантаження Шкідливе програмне забезпечення не спрацювало лише тому, що зловмисники не змогли правильно ввести адреси інтернет-протоколу захисних реле.

Навіть якби ці адреси були введені правильно, не факт, що атака була б успішною. Спроби фізичного саботажу за допомогою шкідливого програмного забезпечення були здійснені лише двічі: атака Stuxnet на іранські ядерні об'єкти у 2009 році та атака Triton/Trisis н а саудівський нафтопереробний завод Petro Rabigh у 2017 році. Атака Triton/Trisis, пов'язана з московським Центральним науково-дослідним інститутом хімії і механіки, зупинила роботу саудівського заводу, але не завдала йому шкоди. Іншими словами, зловмисники CrashOverride використовували передові, неперевірені методи, хоча вони мали певні докази того, що їхній підхід може спрацювати. У 2007 році випробування в Національній лабораторії Айдахо показали, що пошкодження захисного реле в системі передачі електроенергії може знищити 27-тонний генератор.

Майк Ассанте, керівник цього секретного проекту, працював у команді, яка розслідувала атаку на Україну, і помітив схожість у підходах.

Не дивно, що серйозність атаки спочатку не була визнана в Україні, оскільки вона відбулася на тлі сотень інших кібератак. У липні 2016 року відбулася масова фішингова кампанія, спрямована на урядові організації. Потім, у грудні 2016 року, атаки розгорнулися на Міністерство фінансів України, Державне казначейство, Пенсійний фонд, Державну адміністрацію залізничного транспорту та Міністерство оборони. Згодом тодішній президент Петро Порошенко повідомив, що за останні два місяці 2016 року хакери атакували державні установи близько 6500 разів, а нещодавні атаки на Державне казначейство завадили своєчасній виплаті зарплат і пенсій. Через тиждень після атаки на Державне казначейство хакери атакували Міністерство оборони і вивели з ладу його веб- сайт, вочевидь, намагаючись перешкодити оновленню інформації про конфлікт на Донбасі.

##### Супутній збиток**:**

Кібератака на українську економіку **(NotPetya)**

На відміну від перших двох кібератак, третя атака не була спеціально спрямована на енергетичну інфраструктуру, хоча енергетична інфраструктура стала об'єктом атаки в міру розгортання кризи. У лютому 2017 року Агентство національної безпеки США (АНБ) попередило компанію Microsoft про викрадення коду EternalBlue, який використовував вразливості в протоколі Windows, що дозволяло віддалено заволодіти вразливим комп'ютером. У березні Microsoft випустила патч, але в усьому світі все ще залишалися комп'ютери, які не отримали оновлення. WannaCry у квітні та NotPetya у квітні ефективно використали EternalBlue у своєму шкідливому програмному забезпеченні.

Атака NotPetya розпочалася в Україні в червні 2017 року, якраз напередодні свята Дня Конституції. Зловмисники навмисно заразили M.E. Doc - програмне забезпечення для бізнесу, яке широко використовується в Україні. Коли клієнти заходили на сайт для оновлення, шкідливе програмне забезпечення отримувало доступ до персональних комп'ютерів усіх в Україні та за її межами. NotPetya став найшвидше розповсюджуваним шкідливим програмним забезпеченням, яке коли-небудь бачили. Хоча енергетичні системи не були основною ціллю цієї атаки, оператор української системи передачі "Укренерго*", який все ще* відновлювався після кібератак 2015 та 2016 років, зазнав удару якраз перед тим, як завершив модернізацію системи безпеки. *Київенерго*, українська теплоенергетична компанія, також постраждала разом з п'ятьма іншими енергетичними компаніями.

Хоча NotPetya вимагав від власників заражених комп'ютерів сплатити 300 доларів у біткоїнах, він не був програмою-вимагачем. Натомість шкідливе програмне забезпечення безповоротно знищувало дані навіть тоді, коли його жертви читали вимогу про викуп, стираючи головні завантажувальні системи та призводячи до того, що комп'ютери не могли знайти свої операційні системи. Україна постраждала особливо сильно. Окрім енергетичної інфраструктури, від атаки постраждали кілька національних ЗМІ, чотири лікарні, два аеропорти, а також понад 22 банки, банкомати та карткові платіжні системи. За оцінками, 10 відсотків усіх комп'ютерів в країні було знищено в результаті атаки NotPetya.

Збитки, однак, не обмежилися Україною, а торкнулися організацій у приблизно 65 країнах світу. За оцінками Білого дому, збитки становлять понад 10 мільярдів доларів. Мабуть, найвідомішою жертвою NotPetya стала Maersk, велика світова морська судноплавна компанія. Maersk заразилася через один ноутбук, що належав фінансовому директору в Одесі. Maersk повідомила, що NotPetya заразив більшу частину її мережі протягом семи хвилин і знищив 49 000 ноутбуків в організації, паралізувавши глобальне судноплавство. Серед компаній, які повідомили про це збитки приголомшливі: Компанія Merck втратила 870 мільйонів доларів, а також 30 000 комп'ютерів і 7500 серверів, виведених з ладу внаслідок атаки; FedEx/TNT втратила 400 мільйонів доларів ; Saint-Gobain втратила 380 мільйонів доларів; а Maersk втратила 300 мільйонів доларів. Аналіз потенційних майбутніх ризиків для Транспортного командування США, а отже, для проекту сил США і НАТО та військової мобільності, пов'язаних з впливом NotPetya на світове судноплавство, див. у розділі 4.

Хоча експерти з кібербезпеки розділилися в думках щодо того, чи перевищив вплив NotPetya наміри його творців, вони загалом описують його як найближчий приклад кібервійни на сьогоднішній день. Як зазначає експерт з кібербезпеки Кеннет Джірс, "це була найбільш руйнівна атака в історії, за масштабом і вартістю вона набагато перевищила б ракету, випущену з Донбасу по Києву". Риторика щодо кібервійни - це більше, ніж риторика: Страхове відшкодування компанії Merck на суму 1,3 мільярда доларів було відхилено на тій підставі, що атака була актом війни, за який компанія не несе відповідальності. Деякі експерти, в тому числі з української служби кібербезпеки, стверджують, що атака також слугувала для зачистки, дозволяючи хакерам знищити докази шпигунства або розвідки. Інші експерти, такі як Крейг Вільямс з Cisco, роблять висновок, що повідомлення про те, що вести бізнес в Україні небезпечно, було зроблено потужно і цілеспрямовано. Незалежно від того, чи передбачали зловмисники вплив NotPetya, він змістив баланс, оскільки країни почали приписувати кібератаки Росії.

##### Зазначення авторства Еволюціонує

Атрибуція - встановлення особи, відповідальної за кібератаку,- як відомо, є складним завданням, що робить її привабливим варіантом в умовах гібридного конфлікту. Більшість кіберзловмисників замітають сліди, спрямовуючи свої атаки через інші країни або використовуючи методи, які, як відомо, пов'язані з іншими злочинними угрупованнями, щоб ввести в оману слідство. Протягом двох тижнів після першої атаки Сполучені Штати направили в Україну групу експертів, щоб краще зрозуміти цей тип атак і розробити стратегії захисту від них. До складу команди увійшли дійшли висновку, що ця атака свідчить про певне державне спонсорство та підтримку. Однак Сполучені Штати набагато менше прагнули приписати цю атаку Росії, ніж вони приписували попередні атаки Північній Кореї, незважаючи на постійне зростання кількості таких атак. Див. розділ 4, де детально описані докази інших кібервторгнень і атак під керівництвом Росії.

Україна вже давно стверджує, що кожна з трьох описаних вище кібератак мала схожий "почерк" і методи. Українські експерти з самого початку визначили Sandworm як команду, відповідальну за ці та багато інших кібератак на українську землю. Коли міжнародні експерти зібрали більше інформації, вони теж почали вірити в імовірність державного спонсорства.

Протягом шести місяців після атаки Центральне розвідувальне управління США з високою ймовірністю приписувало атаки NotPetya Росії, але ця доповідь була засекречена.71 Лише в лютому 2018 року американські спецслужби підтвердили роль російських військових у запуску NotPetya. Заява США з'явилася через кілька годин після заяв урядів Великої Британії та Данії, які вже засудили роль російських військових у цій атаці. Заява тодішнього прес- секретаря Білого дому містила наступне звинувачення:

Вона була частиною постійних зусиль Кремля з дестабілізації України і ще чіткіше демонструє участь Росії в конфлікті, що триває. Це також була безрозсудна і невибіркова кібератака, яка матиме міжнародні наслідки.

Хоча чітких міжнародних наслідків, ймовірно, не було, докази продовжували накопичуватися в міру того, як американські слідчі виконували свою роботу. У жовтні 2020 року Міністерство юстиції США оприлюднило обвинувальний акт проти хакерської групи Sandworm, звинувативши кожного з шести членів поіменно і чітко ідентифікувавши їх як офіцерів російської розвідки. Згідно із заявою, "жодна країна не використовувала свої кіберможливості так зловмисно або безвідповідально, як Росія, бездумно завдаючи безпрецедентної шкоди заради невеликої тактичної переваги і задоволення своєї злості". Атаки проти українського уряду та його критичної інфраструктури були першим правопорушенням, описаним у заяві, за яким слідували прямі посилання на BlackEnergy, Industroyer, KillDisk і NotPetya.

Існує багато причин, чому Сполучені Штати не поспішали звинувачувати Росію в кібератаках. Дехто зазначає, що за публічним звинуваченням логічно має слідувати відплата - а консенсусу щодо відповідної відплати немає, - тоді як інші зосереджуються на тому, що Сполучені Штати також беруть активну участь у таємних кіберопераціях. Походження EternalBlue підкреслює цю проблему, оскільки АНБ попередило Microsoft про вразливість в її системі після витоку EternalBlue, яка була розроблена для використання цієї вразливості.

### Вчитися в України**:**

### Покращення захисту інфраструктури

Коли Україна приєдналася до Енергетичного співтовариства ЄС у 2011 році, вона взяла на себе зобов'язання реформувати свій енергетичний сектор відповідно до європейських стандартів і прийняти законодавство ЄС про внутрішній енергетичний ринок. В обмін на це Україна отримала значну підтримку в реформуванні енергетичного сектору та все більше інтегрується в європейські енергетичні системи. В електроенергетиці приєднання до європейських енергетичних ринків створює особливу проблему: українська електромережа залишається синхронізованою з російською мережею. Це не є унікальною проблемою для України; країни Балтії також залишаються синхронізованими з російською та білоруською мережами. Зусилля, спрямовані на повне приєднання країн Балтії до європейської енергосистеми, розпочалися у 2009 році і мають завершитися до 2025 року. Цей процес залишається складним і делікатним, оскільки вимагає трансформації інфраструктури, фундаментальних змін у торгівлі електроенергією та прийняття вищих цін.

Замість того, щоб знеохотити ЄС, кібератаки проти України стали каталізатором узгоджених зусиль, спрямованих на подальше просування України в енергетичний простір ЄС. У червні 2017 року ЄС уклав угоду з Україною та Молдовою про роботу над повною синхронізацією енергосистем після того, як кожна країна від'єднається від російської енергосистеми. Дата завершення - 2023 рік. Метою інтеграції України до європейської енергосистеми є підвищення надійності та безпеки постачання, підвищення конкурентоспроможності та покращення стійкості енергосистеми, а також диверсифікація енергетичного балансу як для України, так і для Європи. Вартість синхронізації оцінюється в 400 мільйонів доларів США, тоді як вигоди від неї перевищують 1 мільярд доларів США щорічно.

Першим важливим кроком на шляху до інтеграції енергосистем України та ЄС стало від'єднання вугільної електростанції потужністю 2300 мегават на острові Бурштин від української енергосистеми та приєднання її до європейської енергосистеми. Успіх цього проекту призвів до пропозицій щодо енергетичного мосту, який дозволив би також приєднати до європейської мережі одну атомну електростанцію, Хмельницьку-2. Після початкових затримок у серпні 2019 року тендер на реалізацію цього проєкту було присуджено компанії "Український енергоміст" - консорціуму, до якого входять Westinghouse, EDF, Polenergia International та угорська національна енергетична компанія MVM.

Підключивши Україну до європейської енергосистеми, ЄС отримає більше розуміння українських систем, можливість навчати українських операторів та доступ до додаткових потужностей атомної енергетики в той час, коли деякі країни ЄС - особливо Німеччина - відмовляються від ядерної енергетики. Україна, яка посідає сьоме місце серед світових виробників ядерної енергії, залишається сильно ядерна країна, з 15 комерційно експлуатованими ядерними енергоблоками. Європейський банк реконструкції та розвитку (ЄБРР) надав значну допомогу для модернізації безпеки реакторів. Прихильники допомоги ЄБРР стверджують, що це найкращий шанс для ЄС підвищити рівень безпеки в українській енергетиці, одночасно роблячи ядерну енергетику доступною для Європи, що декарбонізується.

Інтеграція енергосистеми є дуже амбітною як з економічної, так і з фізичної точки зору, і критики зазначають, що Україні доведеться від'єднатися від Росії, перш ніж вона зможе приєднатися до європейської енергосистеми. З економічної точки зору, такий перехід відрізав би Україну від можливості імпортувати електроенергію з Білорусі, яка часто є дешевшою. З точки зору інфраструктури, українська мережа електропередач є масивною та неефективною. Починаючи з 2015 року, ЄБРР інвестував приблизно 124 мільйони доларів у покращення мережі, але, за оцінками, знадобиться ще 5,1 мільярда доларів додаткових інвестицій. З точки зору енергетичної безпеки, цей крок значно посилює енергетичну безпеку України, але через високу мережеву природу електроенергії він створить нові загрози для європейської енергосистеми.

Проблема кібернетичної вразливості України викликає занепокоєння. Інститут інженерів з електротехніки та електроніки опублікував низку рекомендацій, що базуються на досвіді України, в тому числі щодо кращого захисту підстанцій від атак на кшталт CrashOverride. Прихильники інтеграції електроенергетики з ЄС підкреслюють, що Україна може поділитися з ними найкращими практиками як у сфері безпеки ядерної енергетики, такі в галузі кібербезпеки. Вони також зазначають, що після підписання Угоди про асоціацію з ЄС у 2014 році Україна настільки економічно пов'язана з Європою, що ризик "українського зараження" вже є очевидним. Витік даних і взаємодія з українськими інтернет-мережами вже загрожують Європі, про що свідчить атака NotPetya. Втім, тут мало що викликає сумнівів, що інтеграція української електроенергії в систему ЄС означає для Європи нові можливості для кібератак.

### Покращуємо Україну**:** Вразливі місця

##### Кібер Вразливості

Дослідження Інституту, проведене в Україні, описане вище, визначає дотримання правил і протоколів як важливий захід, який важко підірвати, але який має зворотний бік - нав'язливість і високі витрати на розгортання, експлуатацію та обслуговування. Впровадження залишається ключовим викликом в українському контексті, де навіть наймінімальніші політики і протоколи намагаються набрати обертів. Більшість комп'ютерів в Україні працюють на піратському програмному забезпеченні, яке не отримує стандартних патчів безпеки і може бути пошкодженим. Станом на 2016 рік, за оцінками, 82 відсотки всього програмного забезпечення, що використовується в Україні, було неліцензійним.

Проблема поширюється як на офіційне використання програмного забезпечення, так і на приватне та комерційне використання. У 2020 році Україна потрапила до "Пріоритетного списку спостереження " Офісу торговельного представника США (Special 301 Report), який визначає країни з проблемною поведінкою у сфері прав інтелектуальної власності (ІВ), серед 10 країн. У цьому звіті "широке використання неліцензійного програмного забезпечення українськими державними установами" увійшло до трійки найбільших проблем, що викликають занепокоєння. Аналогічно, у піврічному звіті ЄС про права ІВ в Україні за 2020 рік зазначається, що у сфері захисту та дотримання прав ІВ було досягнуто незначного прогресу, що викликає постійне занепокоєння з боку ЄС. Хоча уряд України вдосконалює закони, що регулюють ІВ, відмова від нелегального програмного забезпечення потребуватиме часу для суспільства, включаючи уряд, щоб досягти цього. Неувага до безпечного програмного забезпечення є однією з багатьох проблем в українських технологіях. У 2018 році Британська дослідницька компанія Comparitech поставила Україну на 10-те місце за рівнем кібербезпеки серед 60 досліджуваних країн, оцінивши, що 28 % українських комп'ютерів і 11% телефонів заражені шкідливим програмним забезпеченням. Враховуючи цей контекст, Україні буде складно впроваджувати важливі заходи з кібербезпеки без суттєвих змін у культурі безпеки. Огляд рекомендованих заходів з кібербезпеки див. у розділі 14.

Усвідомлюючи кіберзагрози для енергетичної інфраструктури, *Укренерго* у 2019 році створило оперативний центр кібербезпеки після того, як у 2018 році Рада національної безпеки і оборони України доклала зусиль для координації всіх ініціатив у сфері кібербезпеки в країні. Крім того, на початку 2018 року *Укренерго* оголосило, що планує встановити систему кіберзахисту для своїх операцій вартістю 20 мільйонів доларів США, а завершення робіт заплановано на 2020 рік. Тим часом атаки на енергетичну інфраструктуру з боку Росії тривають, хоча жодна з них не була настільки вражаюче успішною, як у 2015-18 роках. Найбільше занепокоєння викликає кібербезпека української атомної енергетики. У 2018 році група, відома під загальною назвою "Кіберальянс", що складається з чотирьох "хактивістських" груп під назвою "КіберХунта", "Соколине полум'я", "Трійця" і "RUH8", неоднозначно тестувала системи власної країни, намагаючись знайти вразливості. У своїх повідомленнях для преси "Кіберальянс" стверджував, що успішно дослідив "Енергоатом" і знайшов вразливості, які дозволили б хакерам легко проникнути в систему одного з ядерних об'єктів компанії. У розділі 3 наведено кілька яскравих прикладів кіберзагроз атомним електростанціям і каскадних ефектів, які можуть спричинити такі атаки.

##### Ядерна Вразливості

Згідно з офіційними документами, Україна має намір залишатися залежною від ядерної енергії приблизно на 50 відсотків, навіть якщо попит на електроенергію зростатиме. Україна підписала угоди про співробітництво в галузі ядерної енергетики з ЄС і сподівається експортувати електроенергію, вироблену на АЕС, до ЄС у зростаючих обсягах. Оновлена Енергетична стратегія України до 2030 року планує побудувати 5 000-7 000 мегават нових атомних електростанцій вартістю 25 мільярдів доларів США. Сектор ядерної енергетики викликає особливе занепокоєння з точки зору КІ та кібербезпеки.

Індекс фізичної ядерної безпеки Ініціативи зменшення ядерної загрози (Nuclear Threat Initiative), який базується на даних Міжнародного агентства з атомної енергії (МАГАТЕ), дає оцінку кібербезпеки об'єктів ядерної енергетики в 47 країнах світу. У рейтингу 2016 року Україна отримала лише один бал (з чотирьох можливих), опинившись у нижній половині рейтингу. Індекс також вимірює інші аспекти безпеки атомних електростанцій, за якими Україна має значно кращі показники, але її ризикове середовище визначено як несприятливе через поширену корупцію, низьку політичну стабільність та неефективне врядування.

Існує також певне занепокоєння щодо палива для реакторів. Постачання ядерного палива менш інтенсивно пов'язане з мережею, ніж постачання природного газу. АЕС можуть зберігати річний запас палива на майданчику, і більшість з них мають сховища для зберігання ядерних відходів у сухих бочках. Хоча Україна все ще отримує більшість ядерних послуг і ядерного палива з Росії, вона зменшує цю залежність, купуючи американське ядерне паливо. У 2016 році Україна закупила 40 відсотків свого палива у компанії Westinghouse і, за підтримки США, планує з часом розширити ці закупівлі. Майбутні пріоритети ЄС щодо ядерної енергетики є неясними, оскільки європейські держави розділилися в думках щодо її доцільності, але Україна сповнена рішучості відігравати певну роль у європейській енергосистемі, постачаючи електроенергію, вироблену на атомних електростанціях. ЄС, зі свого боку, вже бере активну участь у майбутньому ядерної енергетики України, як буде показано в наступному розділі.

**Improving Ukraine:** Допомога

Хоча Сполучені Штати не поспішали пов'язувати ці атаки з Росією, Україна швидко стала місцем для вивчення кібератак. Українська влада послідовно демонструє готовність надавати кіберрозвіддані в обмін на допомогу у захисті від подальших кібератак. Обмін інформацією та розвідданими між Україною та ЄС, НАТО і Сполученими Штатами був добре розвинений. Ще до кібератак на енергетичну інфраструктуру Сполучені Штати і НАТО долучилися до забезпечення кібербезпеки України. У 2014 році НАТО заснувала Цільовий фонд з кіберзахисту для України на чолі з Румунією. Проект, розрахований на два роки, передбачав створення лабораторій, які могли б розслідувати інциденти з кібербезпеки.

Після кібератак на інфраструктуру та розслідувань, проведених під керівництвом США, Сполучені Штати почали безпосередньо інвестувати в кібербезпеку України, скликаючи регулярні американсько-українські діалоги з питань кібербезпеки, починаючи з вересня 2017 року. Конгрес США ухвалив "Акт про співпрацю з Україною у сфері кібербезпеки 2017 року" і взяв курс на постійну підтримку та консультації. Закон про співпрацю зобов'язує США допомогти Україні з удосконаленням захисту урядових комп'ютерів, захистом критично важливої інфраструктури та розбудовою потенціалу. Сенат ухвалив аналогічний закон - "Акт про співпрацю з Україною у сфері кібербезпеки 2018 року".

У 2017-20 роках Сполучені Штати провели три Діалоги з кібербезпеки з Україною. Під час діалогів Сполучені Штати оголосили про фінансову підтримку: Державний департамент виділив 10 мільйонів доларів у 2017 році та ще 8 мільйонів доларів у 2020 році на підтримку спроможностей України у сфері кібербезпеки. Кошти 2020 року є частиною проекту Агентства США з міжнародного розвитку з кібербезпеки, який має намір інвестувати до 38 мільйонів доларів протягом чотирьох років на підтримку правової та регуляторної реформи, розвиток кіберпрацівників та залучення приватного сектору. Допомога спрямована на підтримку зусиль України щодо дотримання нещодавно підписаних договорів, спрямованих на підвищення безпеки її кіберпростору.

Зусилля НАТО з протидії гібридним загрозам зросли значною мірою у відповідь на російську агресію на східному фланзі НАТО. Детальніше про це див. у розділі 4. Від початку російсько-українського конфлікту 2014 року НАТО активізувала свою співпрацю з Україною. У 2020 році НАТО надала Україні статус Партнера з розширеними можливостями, а Україна, у свою чергу, посилається на цілі членства в ЄС і НАТО у своїй Стратегії національної безпеки до 2020 року.

Тож не дивно, що найбільша допомога Україні надійшла від ЄС. У 2019 році інституції ЄС були основним джерелом усієї зовнішньої допомоги Україні на цілі розвитку, надавши 413 мільйонів доларів США. Крім того, Німеччина та Польща зробили двосторонні внески у розмірі $205 млн та $81 млн відповідно, порівняно з $198 млн, наданими Сполученими Штатами. Лідерство Європи у наданні допомоги Україні проявляється також у підтримці критично важливої інфраструктури. Україна приєдналася до Енергетичного співтовариства ЄС у 2011 році, взявши на себе зобов'язання реформувати свій енергетичний сектор відповідно до європейських стандартів та прийняти законодавство ЄС щодо внутрішнього енергетичного ринку. В обмін на це ЄС надає широку підтримку Україні, насамперед через семінари та проекти в рамках Європейської програми захисту критичної інфраструктури (EPCIP) . EPCIP спрямована на гармонізацію підходів до CISR у транспортному та енергетичному секторах, з акцентом на інфраструктуру з транскордонним впливом. Поглиблений аналіз EPCIP та ширшої політичної бази ЄС щодо КІСР див. у розділі 10.

ЄС вже продемонстрував довгострокову прихильність до української ядерної енергетики та здійснив кілька надзвичайно амбітних інвестицій в Україну та енергетичну безпеку. Зокрема, в рамках Плану здійснення заходів на об'єкті "Укриття" (2010-19 рр.) було витрачено 2,1 млрд. євро на повне утримання радіоактивних залишків зруйнованого 4-го енергоблоку ЧАЕС. ЄС також профінансував завершення будівництва трьох ядерних реакторів в Україні - Хмельницького-2, Рівненського-4 та Запорізького-6, яке було розпочато ще за радянських часів.

Рішення ЄС про включення України до європейської енергосистеми, чому сприяє Європейська мережа операторів системи передачі електроенергії (ENTSO-E), є амбітною, але вже принесла певні плоди. У лютому 2021 року вищий законодавчий орган України підтримав законопроєкт, який дозволить *Укренерго* пройти сертифікацію за правилами ЄС, що є важливою складовою постійних зусиль з синхронізації всієї української енергосистеми з мережею ENTSO-E. *Укренерго* також *досягло* успіху в передачі наборів даних до ENTSO-E та завершило перший етап проектування нової системи SCADA у співпраці з німецьким конгломератом Siemens. Покращення людського потенціалу, зокрема покращення комунікацій та розбудова довіри, є надзвичайно важливим для України, і такі спільні проекти починають змінювати культуру на краще. Про важливість розбудови людського потенціалу для протидії кіберзагрозам читайте в розділі 3.

### Ключова вразливість зберігається

Україна була важливою "пісочницею", в якій інші країни дізналися про кібератаки. Її також називають "зоною вільного вогню", в якій Росія мала змогу випробовувати нову кіберзброю без особливих обмежень. Західні коментатори часто ігнорують той факт, щ о Україна сама була лідером у здійсненні кібератак. Україна має надзвичайно високий відсоток розробників програмного забезпечення, посідаючи перше місце у світі за кількістю розробників програмного забезпечення на 1000 жителів. З огляду на цей відсоток і глибоку асиметрію конфлікту з Росією, що триває, не дивно, що прокиївські сили здійснюють масштабні кібератаки проти Росії.

Кібер-експерти Надія Костюк та Юрій Жуков провели детальний кількісний аналіз - з використанням набору даних, що містить 1841 кібератаку, які відбулися в період 2014-17 років - і виявили, що близько 75 відсотків атак між Росією та Україною походить від прокиївських сил. Їхнє дослідження мало на меті перевірити ефективність кібератак як інструменту примусу під час війни, і вони дійшли висновку, що кібервійна не мала помітного впливу на кінетичні військові операції. Навіть якщо кібератаки виявилися неефективним інструментом у конфлікті, Костюк і Жуков надають чіткі докази того, що прокиївські кібервійська дуже активні.

Фактично, український хактивізм з'явився на початку конфлікту, особливо в групах, що входять до Кіберальянсу, який націлений на Кремль та сепаратистські сили. Кіберальянс стверджує, що витоки конфіденційної електронної пошти, пошкодження веб-сайтів, атаки типу "відмова в обслуговуванні" та "фішинг зі списом" сприяють послабленню російських зусиль, спрямованих проти України. Уряд України зберігає дистанцію, а представники розвідки офіційно заперечують свої зв'язки з Росією, хоча самі організації стверджують, що отримують обмежену підтримку від української розвідувальної спільноти.

Зі свого боку, прокиївські хактивістські сили критично ставляться до зусиль українського уряду, спрямованих на покращення внутрішньої кібербезпеки. У 2018 році "Кіберальянс" неоднозначно протестував українські системи, намагаючись виявити вразливості. Вони повідомили про 200 випадків вразливостей, включаючи успішне проникнення до секретної інформації в Міністерстві оборони і, як уже згадувалося, потенційний доступ до систем атомних електростанцій. Незважаючи на те, що багато хто захоплюється Кіберальянсом, він становить загрозу не лише для репутації українського уряду; його зухвала позиція щодо Росії та власної держави робить його потенційним подразником у відносинах з Європою, що зростають.

Не всі кібератаки, що походять з України, спрямовані на підрив діяльності російського уряду або сил, лояльних до Росії. До війни Україна була сумнозвісним притулком для кіберзлочинців, відомим, зокрема, атаками з вимогами викупу. На початку війни Сполучені Штати намагалися допомогти українському уряду знизити рівень кіберзлочинності та покращити його погану репутацію в боротьбі з кіберзлочинністю. З того часу Україна досягла значного прогресу. Під час третього американсько-українського кібердіалогу в березні 2020 року Федеральне бюро розслідувань США вручило нагороду Національній кіберполіції України та Генеральній прокуратурі за зусилля, докладені спільно з Бюро для затримання та екстрадиції кіберзлочинців.Під час спільної операції в червні 2021 року українська поліція заарештувала кількох підозрюваних, пов'язаних з бандою вірусів-вимагачів Clop, звинувативши їх у відповідальності за збитки на суму близько 500 мільйонів доларів.

Однак деякі зусилля України, спрямовані на боротьбу з кіберзлочинністю, були суперечливими. У жовтні 2020 року, у відповідь на зростання кількості кіберінцидентів під час пандемії, законопроєкти розширили повноваження поліції щодо проведення обшуків і зобов'язали інтернет-компанії надавати доступ до великих обсягів даних користувачів. Ці повноваження полегшили б розслідування кібератак, але, на думку недоброзичливців, поставили б під загрозу персональні дані в країні, де корупція залишається критичною проблемою. Однак запропонований закон відповідає стандартам ЄС, що є головним пріоритетом для України. Оскільки Україна намагається наблизитися до ЄС та енергосистеми ENTSO-E, гармонізація її законодавства та надійне забезпечення його дотримання будуть важливими показниками ймовірного успіху України.

### Висновок

Приклад України дає НАТО, країнам-членам і партнерам кілька ключових уроків у сфері енергетичної безпеки і РСБ для НАТО, її країн-членів і партнерів.

* Атаки на об'єкти критичної інфраструктури здійснюються за підтримки держави. Навіть з огляду на ці знання, необхідність відповідального встановлення винуватців може затримати рішучу реакцію.
* Кібератаки стали більш зухвалими, іноді з непередбачуваними наслідками.
  + Надзвичайна мережевість електромереж вимагає, щоб учасники спільних мереж погоджували та запроваджували стандарти CISR.
  + Перетин правдоподібного заперечення і неповного контролю над кібер-агентами може становити небезпеку як для держави-мішені кібер-активності, так і для держави, яка їх приймає.

НАТО визначає кібертероризм як "кібератаку, що використовує або експлуатує комп'ютерні або комунікаційні мережі для того, щоб викликати достатнє руйнування або перебої в роботі, щоб посіяти страх або залякати суспільство для досягнення ідеологічної мети". Це визначення дещо незручно співвідноситься з атаками в Україні, які відбувалися в контексті наземної війни між Росією та Україною. Як було показано в цьому розділі, в цьому гібридному конфлікті обидві держави мають тенденцію використовувати кіберактивістів, чия приналежність до держави невідома або неповна. Такий зв'язок вигідний державі, що атакує, коли він забезпечує правдоподібне заперечення. Відносини стають проблематичними, коли зловмисники перегинають палицю або прораховують наслідки, потенційно створюючи небезпечний ескалаційний цикл. Російсько-українські кібератаки, розглянуті в цьому розділі, ілюструють ці складні баланси. Неясно, чи можуть НАТО і ЄС толерувати подальшу мовчазну підтримку кіберактивістів з боку України, незалежно від того, скільки симпатій вони можуть мати до цієї справи. Якщо Україна хоче стати частиною високорозгалуженої енергетичної системи Європи, верховенство права має поширюватися як на групи кіберактивістів, так і на злочинні угруповання.

З огляду на триваючий конфлікт з Росією, РЄБС в Україні загрожує близькість до Росії, спільна енергетична інфраструктура (трубопроводи та мережі), часта залежність від радянських технологій, а також нормалізація кібератак в обох напрямках. ЄС, НАТО і США намагаються зменшити вразливість України через допомогу в розвитку та спільні практики і стандарти. Певний прогрес очевидний, але постійні проблеми залишаються. Покращення інфраструктури є дорогим і повільним. На думку українських критиків, кіберзахист України продовжує гальмуватися через "погану комунікацію між державними установами, опір змінам, заплутаний політичний підхід до кіберзахисту і брак коштів для набору кваліфікованого персоналу і придбання вкрай необхідного обладнання".Ця критика може бути висунута багатьом державам, включно зі Сполученими Штатами, особливо після атак на Колоніальний трубопровід у травні 2021 року. Однак, незважаючи на те, що США, НАТО та ЄС продовжують надавати допомогу в сфері кібербезпеки в Україні, вона залишається у фокусі їхньої уваги.

Хоча Костюк і Жуков не знайшли доказів того, що кібервійна має вимірний вплив на кінетичні військові операції, зворотне видається вірним. Ретельне вивчення ескалації кібератак видається корисним сигналом про наближення ескалації на полі бою або на кордоні. Росія продовжує поєднувати кібератаки з провокаційними військовими діями, про що свідчить квітень 2021 року. У квітні, коли російські війська зосереджувалися на кордоні, спостерігався помітний сплеск хакерських атак та кібератак. *US News C World Report* повідомив, що лише у березні-квітні 2021 року Україна разом з американськими партнерами запобігла 350 кібератакам. Ця цифра особливо вражає, якщо врахувати, що за попередній рік українська розвідка повідомила лише про 600 атак.

Оскільки енергетика відіграє важливу роль у суперечках між Україною та Росією і використовується обома сторонами як засіб у конфлікті, вона залишається ймовірною мішенню для кібератак у майбутньому, доки Росія дотримуватиметься гібридного підходу. Зміцнення критично важливої енергетичної інфраструктури залишається важливим компонентом безпеки України, а також, дедалі більше, безпеки ЄС. В епоху домінування електроенергії, що настає, вразливі місця змістилися. Ланцюги постачання все ще мають значення, як і в епоху нафти і газу, але інформаційні ланцюги всередині і між членами Альянсу тепер становлять критичну вразливість. Безпека енергопостачання залежить від покращення інфраструктури та нагляду не лише з боку країн-членів ЄС, але й з боку його близьких партнерів. Приклад України дає уявлення про масштаби завдання і можливі шляхи його вирішення. Дозволивши собі вільнодумство, використовуючи спостереження Черчилля про нафту, можна сказати, що безпека зараз полягає у співпраці союзників, і тільки у співпраці.

### Епілог

Це тематичне дослідження було завершене за кілька місяців до російського вторгнення в Україну в лютому 2022 року. Книга вийшла друком на початку конфлікту, але вже протягом перших двох тижнів стало зрозуміло, що розгортаються важливі події, пов'язані з кіберсферою, безпекою та стійкістю критично важливої інфраструктури. Кібер-елемент російської війни в перші тижні був таким менш агресивною, ніж очікувалося, що, на думку кібер-експертів *New York Times,* було пов'язано або з тим, що Україна має кращий кіберзахист, ніж очікувала Росія, або з тим, що російське командування вирішило поберегти інфраструктуру, щоб полегшити потенційне правління маріонеткового уряду в Україні. Існують докази на підтримку обох аргументів.

Щодо першої гіпотези, то ЄС надав Україні команду з кіберзахисту, яка була офіційно сформована 22 лютого. Очолювана Литвою, до складу якої увійшли представники Хорватії, Естонії, Нідерландів, Польщі, Румунії та Хорватії, і яка фінансується в рамках Ініціативи ЄС з питань оборони та безпеки в рамках Постійної структурованої співпраці, команда мала колективну місію "виявляти, розпізнавати та пом'якшувати кіберзагрози". Рішення ЄС найняти цю команду було частково відповіддю на відхилення наприкінці 2021 року заявки України на приєднання до Центру передового досвіду НАТО з кіберзахисту в якості учасника, який робить внесок, що вимагало б одностайного голосування для досягнення успіху. Попри цю формальну відмову, члени Альянсу в кіберцентрі пообіцяли надавати Україні постійну підтримку.

Росія здійснила кілька кібератак у дні, що передували її вторгненню в Україну: аналітики повідомляють про значні кібератаки проти України 14 січня, 15 лютого та 23 лютого. Перші дві атаки були розподіленими атаками типу "відмова в обслуговуванні" (DDoS), які були спрямовані на урядові міністерства, банки та оборонні відомства. Третя атака, яка мала форму випуску шкідливого програмного забезпечення, була потенційно найбільш руйнівною. Однак Центр загроз Microsoft у США швидко виявив нове шкідливе програмне забезпечення - відоме як FoxBlade - і заблокував його код, надав цю інформацію українському уряду і, на прохання Ради національної безпеки США, поділився нею з кількома країнами- членами Альянсу, в тому числі з країнами Балтії і Польщею.

У відповідь український уряд також мобілізував власну "ІТ-армію", яка, як стверджувалося, налічувала понад 175000 добровольців протягом кількох днів після 26 лютого. До створення "ІТ армії" незалежні Українські хакери заявили, що здійснили успішні DDoS-атаки на російські об'єкти та викрали дані білоруського виробника зброї "Тетраедр". Експерти припустили, що ця група займатиметься DDoS-атаками та захисними завданнями, щоб звільнити українську ІТ-армію хакерів для наступу на російські об'єкти.

Хоча Росія провела обмежені кібератаки в перші дні війни, її прямі атаки на українську критичну інфраструктуру були безпрецедентними. Російські війська захопили контроль над українськими атомними електростанціями в Чорнобилі 25 лютого і в Запоріжжі 4 березня. Кінетичні атаки російської армії на ці ядерні об'єкти викликали негайне міжнародне засудження. Крім того, МАГАТЕ звинуватило Росію в підриві двох із семи найважливіших стовпів безпеки атомних електростанцій: експлуатаційний персонал повинен мати можливість виконувати свої обов'язки і приймати рішення, а також повинен існувати надійний зв'язок між атомними електростанціями, регулятором та іншими суб'єктами. Хоча умови для операторів АЕС були досить несприятливими, російські війська дозволили їм продовжувати управління Запорізькою та Чорнобильською станціями. Російське військове командування не доклало жодних початкових зусиль для закриття реакторів на Запорізькій АЕС, два з яких працювали на повну або майже на повну потужність.

Рішення Росії дозволити реакторам продовжувати роботу викликає особливе здивування, враховуючи той факт, що Україна успішно від'єдналася від російської енергосистеми, прагнучи приєднатися до енергосистеми ENTSO-E. Раніше Україна запланувала випробування на ізоляцію - необхідне від'єднання від російської енергосистеми, щоб продемонструвати, що українська енергосистема може надійно працювати в автономному режимі - на 24 лютого, в той самий день, коли Росія розпочала своє вторгнення. Хоча випробування було успішним, воно мало тривати лише кілька днів, після чого Європа інтегрує Україну в мережу ENTSO-E. Однак на момент написання цієї статті члени ENTSO-E все ще вирішували, чи підключати Україну безпосередньо до європейської мережі, фактично ізолюючи її.

Хоча Росія може без особливих труднощів вивести з ладу ізольовану українську енергосистему, вона ще не зробила цього. Тому незрозуміло, чи є захоплення Росією атомних електростанцій частиною більш масштабного плану з руйнування української енергосистеми. З іншого боку, це може бути спробою забезпечити збереження контролю над електростанціями і уникнути супутньої шкоди енергетичним об'єктам з боку російських військ, що було добре задокументовано під час чеченських війн. З огляду на рішучість Росії завоювати і контролювати Україну, може виявитися, що електростанції, особливо атомні, не є настільки привабливими цілями у відкритій війні, як це було в епоху гібридного конфлікту. Захоплення Росією цих критично важливих об'єктів інфраструктури може відображати її бажання зберегти контроль і безпеку цих об'єктів, щоб керувати територією в майбутньому.

# - 6 -

## Цивільна авіація

Девід Харелл

Майже кожного разу, коли після 11 вересня цивільна авіація піддавалася серйозному терористичному нападу, заходи авіаційної безпеки, або їх відсутність, не були успішними у виявленні та запобіганні нападу. У більшості з цих випадків провал антитерористичних заходів посилювався провалами розвідки та/або контртерористичних заходів ( КТ). Фактично, останній раз, коли спроба підірвати літак у повітрі була виявлена і зірвана завдяки процедурам перевірки в аеропорту або авіакомпанії, був інцидент з Енн-Марі Мерфі в аеропорту Хітроу в квітні 1986 року.

Терористи використовують різні методи нападів на об'єкти цивільної авіації, включаючи викрадення літаків, контрабанду саморобного вибухового пристрою (СВП) на борт літака пасажиром, працівником аеропорту (інсайдерська загроза), приховування СВП у вантажі або візку з їжею, різні види саботажу, збройний напад в аеропорту, використання терористами- смертниками в аеропортах і на літаках, застосування переносних зенітно-ракетних комплексів (ПЗРК), а також підрив СВП в аеропорту. Крім того, існують додаткові методи нападу, які або застосовуються проти інших неавіаційних цілей, або були оперативно розглянуті терористами, і тому потребують розгляду. Такі приклади включають в себе таран транспортного засобу в натовп, атаки безпілотників з використанням СВУ або атаки рою безпілотників на літак під час посадки або зльоту. Атаки також можуть включати більше одного способу дій. Обговорити всі ці засоби і методи атак, а також потенційні заходи щодо їх пом'якшення в рамках одного розділу було б неможливо.

Тому в цьому розділі ми проаналізуємо авіаційну інфраструктуру та загрози, з якими вона стикається, приділяючи основну увагу вибухам повітряних суден і наземним атакам на аеропорти. Для розуміння сектору цивільної авіації в першому розділі описується, чому авіаційна галузь є настільки важливою, що робить її такою нестабільною і чому вона є такою привабливою мішенню для терористів. У другому розділі висвітлено кілька ключових причин вразливості галузі. У третьому розділі на прикладах численних тематичних досліджень, які охоплюють 20 років після терактів 11 вересня, ілюструються деякі з цих вразливостей, розглядаються заходи авіаційної безпеки у відповідь на терористичні атаки і визначаються важливі уроки, які можна винести. Насамкінець розділ завершується рекомендаціями та прикладами найкращих практик, які можуть допомогти зменшити вразливість міжнародної цивільної авіації.

### Розуміння цивільної авіації Галузь

##### Національна та глобальна критична інфраструктура

Більшість країн визначають цивільну авіацію як критично важливу інфраструктуру через масштаб впливу авіації як на світову економіку, так і на економіку окремих країн по всьому світу. Авіація відіграє ключову роль у ланцюгах постачання багатьох галузей, сприяє розвитку туризму та бізнесу, забезпечує реагування на катастрофи та пандемії, а також покращує зв'язність зростаючої глобальної мережі. У главі 1 йдеться про транспорт, а отже, і про цивільну авіацію, як про сектор життєзабезпечення. Останнім прикладом її критичної важливості є роль, яку авіація відіграла в поширенні вакцин проти COVID-19 по всьому світу. Хоча авіаційні вантажі становлять менше одного відсотка від кількості товарів, що перевозяться глобальним ланцюгом поставок, у грошовому еквіваленті ця частка становить 24 відсотки від загальної вартості всіх товарів, що перевозяться в усьому світі всіма видами транспорту. Цифри за 2019 рік демонструють масштаб авіаційної глобальної інфраструктури та ілюструють її важливість:

1. 4,3 мільярда пасажирів, які подорожували;
2. 38 мільйонів регулярних рейсів;

(3) економічний вплив у розмірі близько 2,7 трильйона доларів США;

(4) 61,3 мільйона тонн перевезених повітряним транспортом вантажів; і

(5) 65,5 мільйона робочих місць, необхідних для підтримання глобальних авіаперевезень.

Хоча цивільна авіація за своєю суттю не є військовою сферою, очевидно, що посилення безпеки і стійкості цього життєво важливого сектора є життєво важливим інтересом для НАТО як міжнародної організації, а також для її країн - членів і партнерів.

##### Нестабільна галузь

Ще однією важливою характеристикою авіаційної галузі є її нестабільність. Нестабільність пов'язана як з економічними факторами, так і з зовнішніми геополітичними факторами. На авіаційну галузь впливають коливання попиту, жорстка структура витрат, конкурентне ціноутворення, а також мінливі та нестабільні ціни на паливо. Крім того, на галузь можуть серйозно впливати глобальні події, такі як терористичні атаки 11 вересня, пандемії атипової пневмонії та COVID-19, а також світова економічна рецесія 2008 року. Ці фактори призводять до того, що галузь має низьку норму прибутку, що може призвести до того, що авіакомпанії можуть перейти від прибутковості до збитковості за дуже короткий проміжок часу. Наприклад, у 2019 році, до спалаху COVID-19, рентабельність більшості американських авіаперевізників становила від 5 до 6 відсотків, що загалом вважається низьким і вразливим показником.

##### Приваблива ціль

На додаток до нестабільності галузі, вона стала і залишається привабливою мішенню для терористичних атак з кінця 1960-х років. Починаючи з 1963 року, відбулося понад 1200 терористичних атак на цивільні повітряні судна та аеропорти, що показано на рисунку 6-1 за типами атак за певні періоди часу, приблизно за 10 років. Така значна кількість атак демонструє, наскільки привабливою є авіаційна галузь для терористів.

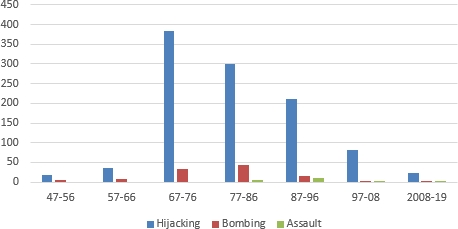


Рисунок **6-1.** Розподіл типів терористичних атак проти авіації

(Дані Авіаційної мережі безпеки)

Існує багато причин, чому терористи вважають авіацію такою привабливою мішенню, в тому числі:

* Здатність досягти події з великою кількістю жертв. Більшість терористів прагнуть здійснити атаку, яка призведе до масових жертв. Чим більша кількість жертв, тим більший вплив матиме атака. Якщо підірвати літак у світловому полі, то, швидше за все, ніхто не виживе, а великі сучасні літаки можуть перевозити більше 400 пасажирів.
* Здатність завдати значної шкоди економіці країни, що зазнала нападу. На додаток до прямих наслідків, пов'язаних із загибеллю людей, існують значні непрямі витрати, зокрема, економічні. Терористична атака на авіацію з масовими жертвами може спричинити падіння попиту на авіаперевезення , що негативно вплине на нестабільну авіаційну галузь.
* Навмисне збиття літака може бути використано як *casus belli*, який терористи можуть спровокувати. Терористична атака на авіаційні інтереси країни з жахливими наслідками в багатьох випадках розглядалася як *casus belli*. Ізраїль ледь не розпочав війну проти Сирії після спроби підірвати літак авіакомпанії Ель-Аль, що вилітав з Лондона в 1986 році. Сполучені Штати розпочали війну в Афганістані проти Аль-Каїди після терактів 11 вересня. У деяких випадках терористичні угруповання можуть домагатися ескалації бойових дій для досягнення своїх цілей.
* Психологічний фактор у тероризмі. Тероризм - це досягнення політичних цілей шляхом залякування громадськості і, таким чином, здійснення тиску на уряди. Страх не сісти на літак і безпечно дістатися до місця призначення, а бути підірваним у повітрі без жодних шансів на виживання, має величезний психологічний вплив на громадськість та індустрію.
* Національні авіаперевізники - це національні символи. Національні авіаперевізники та інші знакові авіакомпанії розглядаються терористами як символи своїх країн. Атака на національний символ іноді є бажаною метою для терористичних угрупувань.
* Негайне висвітлення у ЗМІ. Через центральне місце авіаційної галузі в повсякденному житті західного світу, будь-яка подія, що має негативний вплив на галузь, негайно висвітлюється в ЗМІ. Це висвітлення може бути непропорційним порівняно з іншими секторами. Наприклад, подія в сфері безпеки, що спричинила евакуацію аеропорту, отримує набагато більше висвітлення, ніж аналогічна подія в іншому секторі. Терористичні організації знають про цю динаміку, і висвітлення в ЗМІ, безумовно, є однією з їхніх цілей.
* Противник має певні оперативні переваги. Хоча це не вичерпний перелік, атака на літак у невагомості дає супротивнику декілька переваг, а саме

1. надзвичайно чутливе середовище на борту літака під тиском, що залишає мало місця для помилок щодо реакції і можливого результату;
2. відносно невелика кількість вибухівки або обмеженого озброєння, необхідних для того, щоб атака мала катастрофічні наслідки;
3. відсутність можливості для літака отримати підкріплення в ситуації викрадення.

### Авіаційна галузь залишається вразливою

Майже кожного разу, коли після 11 вересня сфера авіаційної безпеки (АБ) стикалася з терористичними атаками, вона не спрацьовувала належним чином. У більшості випадків погана реакція посилювалася помилками розвідки та/або КТ. Ці невдачі наочно демонструють, що авіаційна галузь залишається вразливою. Крім того, в аеропортах мали місце серйозні порушення безпеки, не пов'язані з тероризмом, що ще більше посилює занепокоєння щодо вразливості галузі.

У таблиці 6-1 перераховані найбільш значні напади на цивільну авіацію, починаючи з 11 вересня і до сьогодні, з коротким описом характеру реагування AVSEC і зазначенням того, чи змогли розвідка і/або операція з КТ попередити або зірвати напад. Пізніше в цій главі буде розглянуто кілька атак, перелічених у таблиці (позначених зірочкою\*), але не всі; тому читачам рекомендується вивчити ці приклади більш детально.

Таблиця **6-1.** Схеми атак**,** заходи **AVSEC** та дані розвідки**/**КТ

|  |  |  |
| --- | --- | --- |
| Реакція безпеки | | |
| План атаки | Антитерористичні заходи/заходи АВСЄС | Розвідка/КТ |
| 9/11 | * Збій політики * Катастрофічний збій системи | * Провали політики * Нездатність "з'єднати точки" * Відсутність "уяви" |
| \*Річард Рід "Взуттєвий бомбардуваль ник"  22 грудня 2001 року | Невдачі: приховані СВП не були виявлені у двох випадках, а СВП контрабандою пронесли на борт літака | FAA випустила попередження для аеропортів та авіакомпаній 11 грудня щодо можливості того, що терористи можуть підкинути зброю в їхнє взуття |
| Момбаса, Кенія Аль-Каїда об'єднана Атаки з ПЗРК та вибухи терористів- смертників  28 листопада 2002  року | Силовики не змогли ідентифікувати осередок, який запустив два ПЗРК, що ледь не розминулися з літаком через помилку терористів, пов'язану з близькістю ракети до цілі. | Брак розвідданих, незважаючи на велику операцію Аль- Каїди, включаючи контрабанду зброї ПЗРК |
| \*Припинення змови з рідиною 9 серпня  2006 р. | Хоча безпека аеропорту не була перевірена, той факт, що заборона на пронесення рідин була введена після того, як  сюжет демонструє, що служба безпеки аеропорту не змогла б виявити СВП | Ділянка, порушена роботою колтюбінга |
| \*Атака з  використанням саморобного вибухового пристрою (СВП)  в аеропорту Глазго  30 червня 2007  року | Відсутність заходів з протидії наїзду на бордюри, що дозволяє VBIED, керованому терористом-смертником, врізатися в фасад терміналу і дефлаградувати | Водій VBIED був у списку терористів MI5 |
| \*Рейс 253 Північно- Західних авіаліній над Детройтом "Бомбардувальник нижньої білизни"  25 грудня 2009 року | * Звичайний огляд в аеропорту не виявив СВУ, захованого на тілі Абдулмуталлаба * Процедури безпеки авіакомпанії Northwest Airlines в аеропорту Схіпол не виявили загрозу СВП | Комітет з питань розвідки Сенату США виявив 14 помилок розвідки, що призвели до спроби нападу на борт літака |
| Вантажна ділянка 29  жовтня 2010 року | Заходи з перевірки вантажу на безпеку не дозволяють виявити СВП | Попередження розвідки надходить після того, як СВП пролетіли на двох ногах |

|  |  |  |
| --- | --- | --- |
| \*Викрадення діамантів в аеропорту Брюсселя  18 лютого 2013 року | Заходи безпеки аеропорту не в змозі запобігти, виявити або відреагувати на серйозний прорив периметра  і збройне пограбування діамантів з цивільного літака на  повітряний простір | Н/Д |
| Збиття російського літака Metrojet  31 жовтня 2015 року | Неспроможність запобігти проникненню СВУ на борт літака | Брак інформації |

|  |  |  |
| --- | --- | --- |
| Реакція безпеки **(**продовження**)** | | |
| План атаки | Антитерористичні заходи/заходи АВСЄС | Розвідка/КТ |
| Вибух на борту сомалійської авіакомпанії Daallo Airlines  2 лютого 2016 року | * Скринінгові заходи обходять інсайдерські загрози * Агент служби безпеки надав зловмисникам саморобний вибуховий пристрій у ноутбуці після того, як   показ | Н/Д |
| Вибухи в аеропорту Брюсселя, скоєні терористами- смертниками  22 березня 2016 року | Неспроможність виявити терористів або запобігти їхньому проникненню в аеропорт під час розгортання атаки | Неспроможність адекватно реагувати на отриману інформацію |
| Збройний напад на стамбульський аеропорт Ататюрк з використанням терористів- смертників  28 червня 2016 року | Неспроможність зовнішнього контрольно-пропускного пункту запобігти проникненню терористів в аеропорт | Н/Д |
| Ісламська держава (ДАІШ) Змова в сіднейському літаку Змова в сіднейському літаку  15 липня 2017 року | * Невідомо, чи був би прихований СВП виявлений сіднейською перевіркою AVSEC * Розслідування показало, що вибухівка, яка була використана для СВУ, прибула до Сіднея з вантажем   виліт зі Стамбула | Попередження розвідки отримано через 11 днів після першої спроби  прокласти саморобну вибухівку на борту літака, який зірвав терорист |

При подальшому розгляді, таблиця 6-1 висвітлює три основні характеристики авіаційної безпеки, які сприяють вразливості цивільної авіації: її негнучкість, передбачуваність і труднощі з реагуванням на терористичні загрози, що постійно змінюються.

##### Авіаційна безпека є жорсткою

Системи безпеки складаються з персоналу, технологій, а також правил і постійних операційних процедур, які визначають, як ці елементи повинні працювати разом. Ці системи, як правило, великі і складні, складаються з багатьох сотень співробітників і безлічі технологій. Вхідні дані цих систем (пасажири, багаж і вантаж) мають дуже велику кількість і частоту. Система AVSEC повинна працювати в середовищі, де задіяні численні зацікавлені сторони, адаптуватися до політичних і правових обмежень, підтримуючи при цьому високий рівень обслуговування і задоволеності клієнтів. Як і багато інших систем, авіаційна безпека працює за фіксованими процедурами з невеликим простором для того, щоб по-іншому відреагувати на нерегулярного пасажира або інцидент.

Два приклади демонструють цю жорсткість системи. Перший випадок - це справа Річарда Ріда, який пізніше отримав сумнозвісну назву "Взуттєвий терорист". Рейд прибув до паризького аеропорту імені Шарля де Голля 22 грудня 2001 року, щоб сісти на рейс 63 авіакомпанії "American Airlines" до Маямі, штат Флорида, але агенти служби безпеки затримали його для допиту і обшуку його речей. Згідно зі свідченнями очевидців, співробітники служби безпеки і авіакомпанії були "стурбовані, навіть спантеличені" розпатланим зовнішнім виглядом Ріда і його беземоційною, спокійною поведінкою, незважаючи на те, що його піддали ретельному огляду. Його визначили як пасажира з підвищеним рівнем небезпеки і передали поліції. Однак, зафіксовані в системі процедури обшуку, що включали як французьку поліцію, так і працівників служби безпеки аеропорту, не дозволили їм у двох випадках виявити СВП, захований в його взутті. Як наслідок, Рейд зміг сісти на літак наступного дня з прихованим СВП і спробував його підірвати.

Другим прикладом, який також демонструє жорсткість системи, є випадок, відомий як "Терорист у спідній білизні" або "Різдвяний терорист". Незадовго до полудня 25 грудня 2009 року 23-річний громадянин Нігерії на ім'я Умар Фарук Абдулмуталлаб спробував здійснити теракт на борту рейсу 253 авіакомпанії Northwest Airlines, який прямував з амстердамського аеропорту Схіпол до Детройта і перевозив 278 пасажирів та 11 членів екіпажу. Абдулмуталлаб підірвав невеликий вибуховий пристрій, захований у спідній білизні, на борту Airbus 330, коли той заходив на посадку. На щастя, завдяки типу матеріалів, використаних в якості вибухівки в СВП , пристрій не вибухнув, а скоріше здетонував і обпік Абдулмуталлаба в процесі вибуху. Незважаючи на численні попереджувальні ознаки, які мали б внести його до списку спостереження Адміністрації транспортної безпеки (TSA), що дозволило б запобігти нападу, є кілька індикаторів AVSEC, які можна було б ідентифікувати. Наприклад, Абдулмуталлаб заплатив готівкою за квиток в один кінець з Лагоса до Детройта (через Амстердам), подорожував до США взимку без зареєстрованого багажу, попросив місце біля вікна над крилом літака і, за словами свідків, поводився нервово на виході з літака в аеропорту Схіпхол. Незважаючи на всі ці ознаки, Абдулмуталлаб не був виділений для будь-яких підвищених процедур перевірки.

Ці два приклади демонструють, наскільки гнучкими і адаптивними можуть бути супротивники, які постійно переглядають свої способи дій, в той час як заходи AVSEC залишаються відносно жорсткими. Аналогічно, авіаційна безпека також повинна бути гнучкою і здатною адаптуватися в реальному часі до загроз, що розвиваються.

##### Авіаційна безпека є дуже передбачуваною

Система AVSEC спирається на технології та процеси, які використовуються вже понад 30 років, особливо у випадку прохідних металодетекторних воріт та рентгенівських апаратів з двома джерелами. Навіть найсучасніші комп'ютерні томографи використовуються з 1995 року. Досвідчені пасажири зазвичай розуміють, чому ці сканери подають сигнал тривоги, який предмет на них викликав тривогу, або який саме предмет у їхній ручній поклажі привернув увагу сканера. Якщо звичайні пасажири розуміють ці тригери, то наскільки більше добре підготовлені і рішучі терористи, які мають доступ до цих технологій виявлення, розуміють можливості і вразливості системи і користуються ними. Наприклад, існують глобальні терористичні інтернет-форуми, які спеціально обговорюють вразливості технологій виявлення авіаційних об'єктів, таких як рентгенівські апарати, і способи їх використання, як показано на рисунку 6-2.



Малюнок **6-2.** Онлайн**-**дискусія терористів про те**,** як перехитрити рентгенівські апарати

(Зображення *Мьобіуса*)

Важливо розуміти, що чим більш передбачуваною є система безпеки, тим менша ймовірність того, що супротивник буде нею стримуватися. Позитивним моментом є те, що в деяких аеропортах Північної Америки і Європи для перевірки ручної

поклажі поступово впроваджуються більш досконалі комп'ютерні томографи, але вони коштують дорожче, ніж звичайні рентгенівські апарати, і тому для багатьох країн є економічно невигідними. Сканери тіла також є значним вдосконаленням для пунктів пропуску, але вони часто піддаються критиці з боку психологічну чутливість, що призводить до політичного протистояння, яке часто перешкоджає їхній реалізації.

##### Авіаційна безпека часто намагається встигати за загрозою

Аналіз розвитку загрози цивільній авіації з 1960-х років до сьогодення характеризується тим, що супротивники постійно шукають шляхи обходу заходів AVSEC. Наприклад, у 1960-х і на початку 1970-х років найбільш поширеною формою терористичних атак були викрадення літаків. Ця реальність призвела до впровадження базових заходів безпеки (таких як наскрізні металодетектори і перевірка ручної поклажі пасажирів). Щоб обійти ці заходи проти викрадення, терористи зосередилися на вибухах літаків. В результаті збільшення кількості вибухів літаків за допомогою саморобних вибухових пристроїв у зареєстрованому багажі пасажирів, перевірка була вдосконалена, що, в свою чергу, змусило терористів шукати інші способи обійти ці нові заходи. Деякі приклади цих нових заходів включають використання ПЗРК або контрабандне пронесення СВУ на борт літака шляхом приховання його у вантажному відсіку, а не в багажі пасажира, як це було у випадку з вантажним рейсом 2006 року. Змова з перевезенням рідини в 2006 році, яку ми розглянемо більш детально в наступному розділі, є чудовим прикладом того, що система безпеки не встигає за еволюцією загрози. З удосконаленням технологій виявлення, що застосовуються в авіаційній безпеці, терористи також знайшли способи подолання цих нових технологій шляхом створення більш досконалих, складних СВП.

Оскільки короткий огляд цих прикладів демонструє вразливі місця в авіаційній галузі, в наступному розділі буде розглянуто кілька тематичних досліджень більш детально, щоб описати різні відповіді авіаційної безпеки на терористичні атаки і визначити важливі уроки, які спільнота AVSEC повинна засвоїти.

### Тематичні дослідження**:** Відповіді та уроки

### **AVSEC** для **Learn**

##### Змова з викраденням рідин**,** Велика Британія **(2006)**

У ніч на 9 серпня 2006 року, після великої міжнародної операції з протидії тероризму, британська влада заарештувала 24 чоловіки і звинуватила їх у підготовці серії терактів у повітрі на трансатлантичні літаки з використанням вибухових рідин на борту, заховавши їх у пляшках з-під енергетичних напоїв. Змову було зірвано після арешту членів угруповання, які базувалися в Лондоні і Хай-Вайкомбі в графстві Бакінгемшир. За словами офіційних осіб КТ, змова була натхненна "Аль-Каїдою" і передбачала підготовку кількох терактів із застосуванням смертників. Під час арештів поліція знайшла відеозаписи мучеництва, на яких члени осередку вихвалялися атакою, а також матеріали таємних операцій у східному Лондоні, які свідчать про те, що члени осередку, які готували рідкі бомби (див. рис.6-3 для ілюстрації того, як були виготовлені рідкі бомби).6



Малюнок **6-3.** Зображення конструкції рідинних СВУ

(Зображення *Daily Mail*)

Під час судового процесу обвинувачення стверджувало, що британський терористичний осередок планував пронести саморобні вибухові пристрої на борт літака і підірвати щонайменше сім авіалайнерів, які вилітали з аеропорту Хітроу на шляху до Північної Америки з більш ніж 1 500 людьми на борту. Окрім пасажирів на борту цих літаків, кількість потенційних жертв повинна враховувати тих, хто перебував на землі і загинув би в результаті цих атак - це питання буде розглянуто пізніше в розділі "Аналіз". Відеозаписи випробувань, проведених урядовими вченими, які були продемонстровані присяжним, показали, що пристрої виробляють вибух, достатньо потужний для того, щоб пробити дірку у фюзеляжі літака.

У травні 2012 року важливу розвідувальну інформацію було отримано з документів, знайдених на прихованому диску у 22- річного австрійця на ім'я Максуд Лодін, якого допитувала поліція в Берліні після повернення з Пакистану. Один документ, написаний Рашидом Рауфом - британським бойовиком "Аль- Каїди", який стояв у центрі терористичних операцій у Великій Британії, - проливає нове світло на змову з метою підриву трансатлантичних авіалайнерів, що вилітали з аеропорту Хітроу в 2006 році. У документі Рауф пише: "Потім ми проаналізували різні машини, які використовувалися для перевірки багажу і людей в аеропортах. Ми виявили, що дуже важко виявити рідку вибухівку. Проаналізувавши, що на борт літака можна взяти концентрований перекис водню, нам спало на думку: а чи можна підірвати водень на борту літака?"

Одразу після зриву змови Сполучені Штати та Канада заборонили проносити в ручній поклажі пасажирів будь-які рідини та гелі, а у Великій Британії взагалі заборонили брати на борт літака будь-яку ручну поклажу, окрім найнеобхідніших речей (наприклад, проїзні документи, гаманці та дитяче харчування). Нові заходи спричинили масові затримки рейсів і призвели до безладу в авіаційному світі, але з часом заборона була запроваджена і в інших країнах, які дозволили пасажирам брати на борт лише невелику кількість рідини або гелю. Нікі Томпкінсон, тодішній директор з питань транспортної безпеки в Міністерстві транспорту Великобританії, високо оцінив співпрацю і координацію Сполучених Штатів, Великобританії і Канади у швидкому реагуванні на цю нову загрозу рідких вибухових речовин. Ці обмеження значною мірою залишаються чинними до тепер.

У 2009 році ватажок змови Абдул Ахмед Алі та двоє його найближчих соратників, Танвір Хусейн і Ассад Сарвар, були визнані винними у змові з метою підриву щонайменше семи авіалайнерів, які мали прямувати до США і Канади. Суддя Високого суду призначив довічне ув'язнення з 30 мінімальними термінами ув'язнення від 32 до 40 років кожний, назвавши цю змову "найбільш серйозною і злісною змовою, коли-небудь доведеною в межах юрисдикції", яку можна порівняти лише з терактами 11 вересня.

##### Рідинний сюжет**:** ідеї та аналізи

Одне з найважливіших питань, яке повинні зрозуміти фахівці AVSEC, - чи була б змова успішною, якби не було попередження розвідки і подальшого зриву операції КТ. Хоча дехто ставить під сумнів життєздатність змови, помічник комісара Енді Хейман, тодішній керівник відділу спеціальних операцій Скотланд-Ярду, писав: "Якби змовників не зупинили, я вважаю, що вони б досягли у спіху".

Дуже ймовірно, що якби змова матеріалізувалася і не була зірвана, терористам було б неважко проникнути через систему перевірки безпеки, що діяла на той час. Той факт, що нові заходи безпеки (наприклад, заборона на рідини і гелі) мали бути швидко затверджені і впроваджені, чітко демонструє, що заходи, які діяли на той час, не були здатні виявити рідкі вибухові речовини або тип складного ініціюючого пристрою, який планували використати терористи. Крім того, один з членів осередку, який працював контролером в аеропорту Хітроу, проінформував своїх колег про заходи безпеки, що були вжиті на той час. Глибока обізнаність членів групи з існуючими заходами безпеки ще більше підвищує ймовірність того, що атака була б успішною. Деталі, розкриті у вищезгаданому документі Рауфа, вказують на те, що осередок проводив значну ворожу розвідку і мав доступ до технологій і процедур виявлення AVSEC, що дозволило членам осередку обрати бажані способи дій. Це важлива інформація для розуміння можливостей противника.

За оцінкою суду, що ґрунтується на даних про пасажиропотік трансатлантичних літаків, в результаті вибухів могло загинути щонайменше 1 500 осіб. Однак кількість жертв була б значно більшою, якби терористи вирішили підірвати свої СВП, коли літаки пролітали над густонаселеними великими містами. Таким чином, ці атаки могли б перевищити кількість жертв, спричинених 11 вересня.

Іншим важливим питанням, яке потребує вивчення, є те, чому рідкі вибухові речовини були визнані новою загрозою в серпні 2006 року, незважаючи на те, що деякі типи рідких вибухових речовин існують вже більше століття. Звичайно, не всі рідкі вибухові речовини придатні для використання терористами проти авіаційних цілей через їхню чутливість і складність доступу. Однак PLX - рідка вибухівка, винайдена під час Другої світової війни - була використана агентами північнокорейської розвідки для підриву літака Korean Air F Light 858 у повітрі біля узбережжя Таїланду 29 листопада 1987 року, в результаті чого загинули всі 115 пасажирів і членів екіпажу. МетоюПівнічної Кореї була дестабілізація регіону напередодні Олімпійських ігор 1988 року в Сеулі. Північнокорейські агенти залишили складний саморобний вибуховий пристрій, що складався з невеликої кількості пластикової вибухівки, захованої в транзисторному радіоприймачі Panasonic, часового механізму і детонатора, а також пляшки віскі з рідкою вибухівкою, у верхньому сміттєвому відсіку на борту літака, а потім висадили літак під час транзитної зупинки. Незважаючи на те, що це був перший випадок використання рідких вибухових речовин проти цивільної авіації, жодних нових заходів щодо виявлення рідких вибухових речовин не було запроваджено. Натомість акцент був зроблений на вжиття заходів для запобігання таємному залишенню особами світлофора на проміжному пункті.

11 грудня 1994 року рідка вибухівка знову була використана для нападу на цивільний літак. У цьому нападі сумнозвісний терорист Аль-Каїди Рамзі Юсеф, який зараз перебуває під вартою за головну роль у першому вибуху Всесвітнього торгового центру в 1993 році, заклав бомбу на рейс 434 Філіппінських авіаліній (PAL), яка здетонувала по дорозі з Маніли до Токіо. Літак пережив вибух і зміг здійснити екстрену посадку в Японії, але один пасажир загинув і ще 10 отримали поранення в результаті вибуху. Юсеф використав нітрогліцерин як вибуховий компонент СВП , сховав рідину у пляшках з-під засобу для очищення контактних лінз з ватними кульками, що слугували стабілізатором, і привів СВУ в дію за допомогою цифрового годинника, двох дев'ятивольтових батарейок і нитки розжарювання лампочки (див. рис. 6-4).



Зображення **6-4.** Реконструкція СВП**,** використаного для підриву рейсу

**PAL 434**

(Зображення від Alchetron)

Пізніше слідчі дізнаються, що вибух літака PAL 434 був пробним запуском набагато смертоноснішої атаки, відомої під назвою "Боїнг". За цим планом Юсеф і ще кілька оперативників з його осередку "Аль-Каїди" планували підірвати 11 літаків, що вилітали з аеропортів Азії і прямували до Сполучених Штатів. Модус операнді знову ж таки полягав у тому, щоб встановити СВУ на цільовому літаку і висадити пасажирів під час транзитної зупинки. СВП, які мали бути використані, були подібні до тих, що були випробувані під час вибуху літака PAL 434, включаючи використання рідких вибухових речовин.

На щастя, змова Юсефа була розкрита в Манілі через оперативні помилки, яких припустився його осередок. Якби змова була успішно реалізована, наслідки могли б бути катастрофічними і подібними до терактів 11 вересня.

Беручи до уваги наведені вище приклади, всі три плани авіаційних атак використовували рідкі вибухові речовини як компонент СВП, оскільки противник знав, що системам безпеки буде надзвичайно складно виявити цей тип загрози. Для політиків у сфері безпеки важливо розуміти, чому використання рідкої вибухівки у змові 2006 року вважалося новою загрозою, як зазначалося раніше. За словами відповідних високопосадовців АВСЕК, є чотири основні причини, чому цій загрозі не було приділено належної уваги до серпня 2006 року:

* + Надмірне розділення створило розрив у знаннях між тими, хто працює в розвідці, і тими, хто займається авіаційною безпекою, що призвело до ситуації, коли недостатньо осіб, які приймають рішення в рамках AVSEC, були достатньо обізнані про життєздатність загрози або протидії їй.14
  + Загальновизнано, що існуючі технології виявлення не здатні виявляти рідкі вибухові речовини і що розробка такої технології займе кілька років.15
  + Багато країн вважали, що загрози, з якими вони стикаються в цивільній авіації, не є значними, і що терористи зосереджені в основному на США та Ізраїлі.16
  + До 11 вересня багато великих авіакомпаній, які мали значний вплив на політику AVSEC, виступали проти нових заходів безпеки, які могли виявитися дорогими і негативно вплинути на обслуговування клієнтів та спрощення процедур.17

Ці чотири причини проливають важливе світло на питання управління ризиками, які впливають на те, як ця загроза розглядається в системі авіаційної безпеки. Перший пункт стосується необхідності для керівників AVSEC мати прямий доступ до розвідувальних даних, що стосуються характеру загроз, які постають перед цивільною авіацією. У відповідь на події 11 вересня багато високопоставлених поліцейських і військових офіцерів переїхали до Домен AVSEC. Це були висококваліфіковані професійні співробітники служб безпеки, але вони мали незначний досвід роботи в галузі авіаційної безпеки або взагалі не мали його. Оскільки вони вивели свої відомства на вищий професійний рівень для протидії загрозам після 11 вересня, зрозуміло, що багато хто з них не мав жодного уявлення про тип вибухівки, яка використовувалась під час терористичних атак проти авіації десять років тому. Це приклад "незнання того, що ми знаємо" - знайомої проблеми у світі розвідки і безпеки, коли організація володіє інформацією, яка могла б покращити її процеси прийняття рішень, але з різних причин ця важлива інформація не була відома або доступна тим, хто міг би на неї вплинути.

Друга причина, пов'язана з відсутністю технологічних можливостей для протидії конкретним загрозам, по суті ігнорувала ризик, пов'язаний з рідкими вибуховими речовинами. Той факт, що не існувало технологій для виявлення рідких вибухових речовин і що розробка таких технологій потребувала б значного часу і коштів, дійсно, слід брати до уваги. Важливо, однак, розглянути інші можливі заходи у процесуальній сфері, які могли б забезпечити певну відповідь на загрозу, пов'язану з рідкими вибуховими речовинами.

Розглянути ризик, а потім вирішити не реагувати на нього доти, доки не буде зрозумілий залишковий ризик, є законним рішенням в управлінні ризиками. Однак, оцінюючи рівень загрози авіаційним інтересам країни, необхідно розглядати авіацію як цілу мережу з потенціалом негативних, каскадних ефектів. Для ілюстрації цього третього пункту повчальним є випадок з "бомбардувальником у нижній білизні". Можна припустити, що Нідерланди в 2009 році оцінили загрозу своїм авіаційним інтересам як низьку і тому прийняли не надто жорсткі заходи безпеки, але потім були здивовані змовою Абдулмуталлаба. Абдулмуталлаб, нігерієць, який проживає в Лондоні, отримав завдання атакувати американський авіалайнер і вирішив напасти на літак, що мав транзитну зупинку в аеропорту Схіпхол. Якби цей план увінчався успіхом, Нідерланди- хоча вони і не були метою атаки - зазнали б негативного впливу в багатьох відношеннях. Нідерланди насправді мають надійну систему AVSEC, а аеропорт Схіпхол вважається лідером у впровадженні нових технологій безпеки. СВП, захована в нижній білизні Абдулмуталлаба, пройшла б через контрольно-пропускні пункти в більшості аеропортів через те, що в 2009 році в аеропортах було встановлено дуже мало сканерів для огляду тіла.

Щодо четвертого пункту, впливу авіакомпаній на політику, що регулює авіаційну безпеку, то це, безумовно, було важливим фактором до подій 11 вересня, і цілком можливо, що комерційні або інші інтереси негативно впливали на рішення щодо політики безпеки. Візьмемо, наприклад, рішення Управління транспортної безпеки США (TSA) 2013 року дозволити пасажирам брати на борт літаків складні кишенькові ножі з лезом менше 2,36 дюймів. Управління транспортної безпеки США прийняло таке рішення з метою посилення контролю і полегшення обслуговування пасажирів, виходячи з логіки, що маленький кишеньковий ніж не становить загрози для літака, оскільки всі літаки мають посилені двері кабіни пілотів, які залишаються зачиненими під час польоту, а бортовий сервіс зазвичай включає металеві столові прилади, які є потенційно такими ж небезпечними. Однак це рішення викликало значний спротив, зокрема, з боку профспілок екіпажів, і врешті-решт Управління транспортної безпеки США було змушене скасувати своє рішення.

##### Комплаєнс або авіаційна безпека**,** орієнтована на загрози Системи

Через величезні пасажиропотоки через аеропорти як на національному, так і на глобальному рівні, спільнота AVSEC зіткнулася з однією з ключових управлінських проблем: визначити рівень безпеки, який дозволить ефективно і в розумні терміни здійснювати перевірку цих пасажирів. Якщо рівень перевірки буде занадто високим, це може негативно вплинути на пропускну спроможність пасажирів. З іншого боку, якщо рівень перевірки буде занадто низьким, то він не зможе запобігти або стримати терористів, які намагатимуться обійти систему. Рівень скринінгу в країні, відомий як стандарт авіаційної безпеки, зазвичай визначається національним регулятором AVSEC. Міжнародна організація цивільної авіації (ІКАО), спеціалізована установа Організації Об'єднаних Націй, слугує глобальним форумом для міжнародної цивільної авіації і визначає міжнародні стандарти авіаційної безпеки. Найважливіша роль ІКАО полягає в розробці та прийнятті стандартів і рекомендованих практик для міжнародної цивільної авіації, які включені в Додаток 17 до Конвенції про міжнародну цивільну авіацію, також відомої як Чиказька конвенція. Зусилля ІКАО, спрямовані на запобігання та протидію незаконному втручанню в діяльність цивільної авіації в усьому світі, мають важливе значення для авіаційної безпеки та майбутнього цивільної авіації. Як міжнародний стандарт, якого повинні дотримуватися всі держави-члени ООН, Додаток 17 -вперше прийнятий у березні 1974 року - регулярно оновлюється, особливо після терористичних атак, серйозних порушень безпеки або значного підвищення рівня загрози.

Велика різниця в ресурсах, які країни можуть інвестувати в авіаційну безпеку, призводить до значних відмінностей у рівні придбаних технологій виявлення та наявності людських ресурсів і підготовки кадрів у кожній країні окремо. У Додатку 17 наведено міжнародний стандарт, який має досить загальний характер і може вважатися найнижчим загальним знаменником для авіаційного скринінгу. Тому багато держав визначили власні національні стандарти перевірки на авіаційну безпеку. Наприклад, Управління транспортної безпеки США визначає стандарт авіаційної безпеки для США, Європейська конференція цивільної авіації - для Європейського Союзу, а Міністерство транспорту Канади - для Канади. Ці три національні авіаційні стандарти є більш надійними і суворими, ніж національний стандарт ІКАО, але навіть ці високі рівні безпеки не завжди здатні впоратися з можливостями супротивника, як показують приклади з практики, наведені в цій главі. Співробітники AVSEC наполегливо працюють і інвестують значні ресурси для дотримання стандартів безпеки. Однак важливо зазначити, що дотримання стандартів не обов'язково означає здатність запобігти, ідентифікувати та подолати загрозу. Існує багато прикладів, коли аеропорти отримують високі бали за результатами аудиту, а потім виявляється, що їхні заходи безпеки не змогли запобігти нападу.

Один із прикладів стався о 20:00 18 лютого 2013 року в аеропорту Брюсселя, коли вісім озброєних людей у масках на двох мікроавтобусах прорвалися через огорожу злітно- посадкової смуги і виїхали на злітно-посадкову смугу на своїх автомобілях. Під час цього зухвалого пограбування автомобілі наблизилися до літака Fokker 100, що прямував до Швейцарії, і злодії, розмахуючи зброєю, захопили літак і викрали діаманти вартістю 50 мільйонів доларів США. Злочинці змогли втекти з аеропорту, не будучи зупиненими, і, на щастя, в цьому інциденті ніхто не постраждав. Однак цей інцидент слід розглядати під іншим кутом зору: що, якби нападники були не злодіями, а терористами? Той факт, що вісім добре озброєних бойовиків змогли непоміченими проникнути в зону виконання польотів, вказує на дуже вразливе місце в системі захисту аеропорту. Тут головним недоліком була огорожа по периметру аеропорту: оскільки вона не була "розумним парканом" - обладнаним датчиками для виявлення вторгнення і попередження про прорив, - зловмисники змогли проникнути за периметр, не будучи виявленими. Якщо немає виявлення, то менш імовірно, що буде ефективне реагування. Важливо відзначити, що ні міжнародний стандарт, ні стандарт AVSEC в ЄС не вимагає від аеропортів встановлювати "розумні" огорожі.

Представник аеропорту наполягав на тому, що безпека повністю відповідала міжнародним стандартам, але підкреслив, що пограбування вийшло за рамки сучасної авіаційної безпеки. У цьому випадку заходи безпеки, спрямовані на стримування або запобігання "потенційним терористам та іншим загрозам, не змогли запобігти рейдам добре озброєних злочинців у стилі командос". Цей інцидент є класичним прикладом аеропорту, який відповідає стандартам AVSEC, але не орієнтується на загрози. Аеропорт, який вирішує правильно інвестувати в розумну огорожу, - це аеропорт, який виходить за рамки дотримання вимог і прагне бути більш здатним протистояти загрозам, з якими він стикається. Варто зазначити, що це той самий аеропорт, який був атакований терористами- смертниками через три роки в 2016 році.

##### Потреба в удосконаленні заходів фізичної безпеки в громадських місцях аеропорту

У той час як злітна смуга, контрольно-пропускні пункти, зал міжнародних прильотів, паспортний контроль і митна зона аеропорту суворо регламентовані і підлягають регулярним перевіркам, громадські зони аеропорту, включаючи узбіччя, термінали реєстрації та зали вильоту, не користуються такою ж увагою з боку регулюючих органів. Як наслідок, рівні безпеки в цих громадських місцях зазвичай визначаються самими аеропортами або підрозділами аеропортової поліції, призначеними для їх охорони, що може призвести до значних розбіжностей у рівнях безпеки між аеропортами навіть в одній і тій же країні. За відсутності регуляторної політики або рекомендацій щодо необхідних рівнів безпеки в громадських місцях, такі критичні питання, як протистояння, бар'єри проти тарану, захист фасадів і мінімальне розгортання озброєної охорони, часто не вирішуються належним чином або на професійному рівні.

Терористичні наземні атаки на аеропорти після 11 вересня мали значний вплив на аеропорти, що зазнали нападу. Одна з таких атак сталася в міжнародному залі вильоту аеропорту Брюсселя 22 березня 2016 року, коли двоє терористів з Ісламської держави (Даеш) здійснили подвійний теракт (третій терорист не зміг привести в дію саморобний вибуховий пристрій у своїй сумці і втік з аеропорту). На додаток до 19 загиблих і понад 80 поранених, масові руйнування в залі вильоту призвели до повного закриття аеропорту на 12 днів, і лише через кілька місяців часткової роботи аеропорт відновив повноцінну роботу. Аеропорт Брюсселя є єдиним міжнародним аеропортом Бельгії, що зробило наслідки закриття ще більш відчутними. Згідно з численними джерелами, аеропорт Брюсселя і міське метро були під неминучою загрозою, що спонукало бельгійську владу розмістити військовослужбовців в аеропорту та інших ключових транспортних вузлах по всьому місту. До нападу співробітники служби безпеки аеропорту не помітили терористів, які здійснювали теракт.

У терористичній атаці н а стамбульський аеропорт імені Ататюрка ввечері 28 червня 2016 року також брали участь три терористи-смертники, як і в атаці на аеропорт Брюсселя, але в цьому випадку терористи з "Ісламської держави" ( ДАІШ) також були озброєні автоматичною зброєю. Хоча такий спосіб поєднання збройного нападу з використанням саморобного вибухового пристрою вже траплявся в минулому - як у випадку руйнівного нападу на міжнародний аеропорт Бандаранаїке в Шрі-Ланці в 2001 році, - напад на аеропорт імені Ататюрка був першим, коли ця тактика була застосована проти великого західного аеропорту. Заходи безпеки в аеропорту Стамбула суттєво відрізнялися від брюссельських, оскільки за попередні 12 місяців у Туреччині спостерігався значний сплеск тероризму, в тому числі шість значних вибухів, здійснених за перші шість місяців 2016 року. Турецькі органи безпеки розгорнули пункти перевірки на в'їздах до терміналів на узбіччі. Розгортання придорожніх контрольно-пропускних пунктів може бути дуже ефективним заходом проти терористів-смертників, оскільки вони сигналізують про стримування і дозволяють виявити загрозу ще до того, як потенційні терористи зможуть увійти на територію терміналу.

Однак, як і в усіх заходах безпеки, тут є свої компроміси. Придорожні пункти огляду можуть також створювати ситуацію "вузького місця", коли люди затримуються в черзі на проходження контролю і стають об'єктом нападу. Основним недоліком придорожніх пунктів огляду є те, що вони негативно впливають на спрощення процедур і обслуговування клієнтів і не завжди сприймаються ключовими зацікавленими сторонами: аеропортами та авіакомпаніями. Під час нападу на аеропорт Стамбула, ймовірно, кількість жертв і збитків, завданих аеропорту, була б значно більшою, якби всі троє терористів- смертників успішно підірвали свої бомби всередині терміналу. Насправді, аеропорт зміг відновити легкі операції на наступний ранок після нападів, на відміну від тривалого закриття, яке пережив аеропорт Брюсселя. Стійкість, продемонстрована операторами аеропорту в Стамбулі, заслуговує на високу оцінку: поліція і сили безпеки, розгорнуті в аеропорту, відважно і швидко відреагували, що сприяло пом'якшенню загрози і мінімізації кількості жертв і збитків, завданих аеропорту.

Останній приклад наземного терористичного нападу на аеропорт пов'язаний з використанням саморобного вибухового пристрою (СВП), що перевозиться на транспортному засобі (VBIED). 30 червня 2007 року двоє терористів на спортивному позашляховику в'їхали в скляні двері головного терміналу (Термінал один) міжнародного аеропорту Глазго. Низька швидкість автомобіля не дозволила йому в'їхати в переповнений людьми термінал. Двоє терористів намагалися підірвати саморобний вибуховий пристрій, але, на щастя, не встигли. Він лише спалахнув і призвів до запізнілого, незначного вибуху. Єдиними жертвами нападу стали два терористи, один з яких загинув, а інший отримав сильні опіки. Незважаючи на відносно низький вплив цієї атаки, питання "а що, якби" знову варто поставити. Що, якби VBIED був краще сконструйований і здетонував? Що, якби транспортному засобу вдалося проникнути в будівлю терміналу? Виходячи з руйнувань і кількості жертв, які спричинили саморобні вибухові пристрої в Брюсселі, цілком ймовірно, що VBIED, якби він здетонував всередині будівлі терміналу, значно перевищив би рівень руйнувань і жертв.

Важливо зазначити, що до нападу в аеропорту Глазго не було жодних протитаранних бар'єрів або стовпчиків вздовж узбіччя. Однак після нападу вздовж узбіччя були встановлені стовпчики, щоб захистити термінал від подібних атак. Зображення узбіччя аеропорту до і після нападу див. на рис. 6-5 і 6-6. Хоча багато аеропортів по всьому світу зараз захищені протитаранними бар'єрами або стовпчиками, багато інших все ще не мають такого захисту. Знову ж таки, це приклад відсутності регуляторної політики щодо громадських зон в аеропортах.



Зображення **6-5.** Аеропорт Глазго на узбіччі до атаки **VBIED** у **2007** році

(Зображення Insider)



Зображення **6-6.** Аеропорт Глазго на узбіччі після атаки **VBIED** у **2007**

році

(Зображення від Insider)

### Рекомендації та найкращі практики для зменшення вразливості

У той час як у третьому розділі аналізуються конкретні приклади терористичних атак на аеропорти та авіацію після 11 вересня і обговорюються можливі першопричини, що вплинули на результати цих атак і змов, у цьому заключному розділі представлені ключові рекомендації, засновані на досвіді та передових практиках, спрямовані на зменшення вразливостей, визначених у цьому розділі.

##### Розробити більш ризик**-**орієнтовану систему скринінгу **AVSEC**

Як зазначалося в попередньому розділі, однією з ключових дилем управління ризиками в авіаційній безпеці є пошук оптимального рівня перевірки, який забезпечить необхідну швидкість пропускної здатності та обслуговування клієнтів, не ставлячи під загрозу здатність запобігати або стримувати терористичні атаки. З одного боку, рівень перевірки, який надає пріоритет ефективному доступу і мінімізує затори на пунктах пропуску в аеропортах, може бути не в змозі виявити або запобігти складній атаці на систему. З іншого боку, застосування протоколу перевірки, який дозволяє виявити навіть найскладніші приховані загрози, може негативно вплинути на пропускну спроможність аеропорту таким чином, що робота аеропорту стане нестабільною. Більшість країн вирішили впровадити "однакову для всіх" систему AVSEC, в якій всі проходять перевірку в однаковий спосіб і на однаковому рівні.

Оскільки багато атак, про які йдеться в цьому розділі, змогли успішно подолати цей тип скринінгу AVSEC, багато регуляторних органів зараз пропагують підхід, що базується на оцінці ризиків. Двоє колишніх адміністраторів Управління транспортної безпеки США, Кіп Хоулі і Джон Пістол, були одними з перших прихильників переходу до моделі авіаційної безпеки, що ґрунтується на оцінці ризиків. Система, заснована на оцінці ризиків, означає, що пасажири, які становлять підвищену загрозу, проходять вищий рівень перевірки, в той час як звичайні пасажири з меншою загрозою перевіряються відповідно до мінімальних стандартів. При цьому рівень фізичного огляду може варіюватися відповідно до потенційного ризику пасажира. Важливим додатковим питанням, пов'язаним з цією рекомендацією, є рішення про те, які інструменти використовувати для виявлення пасажирів з потенційно високим ризиком. Це питання буде розглянуто далі в додаткових рекомендаціях цього розділу.

##### Розробка та впровадження визначень загроз**,** узгоджених з можливостями противника

Основою ефективних систем безпеки в авіації, як і в усіх інших секторах безпеки, має бути правильне визначення критеріїв загроз, на які необхідно реагувати, а потім відповідна підготовка заходів реагування. Робота з безпеки за своєю суттю повинна бути пов'язана із загрозами; без загроз не було б потреби в заходах безпеки. В авіаційному секторі, якби не було терористів або зловмисників зі зловмисними намірами щодо авіаційних об'єктів, то не було б потреби в авіаційній безпеці. Крім того, захист усіх авіаційних об'єктів від усіх видів терористичних загроз вимагав би величезних ресурсів, які - навіть якби вони були в наявності - майже напевно не були б здійсненними або економічно ефективними. Прямим наслідком спроб протидіяти всім можливим загрозам є те, що персонал служби безпеки не буде належним чином зосереджений на відповідних загрозах і, таким чином, забезпечить лише часткове вирішення проблеми. Наприклад, якщо продовжувати розглядати манікюрні ножиці або маленькі кишенькові ножики як загрозу авіаційній безпеці, підвищується ймовірність того, що зусилля, яких докладають співробітники служби огляду для виявлення цих предметів, знизять їхню здатність виявляти інші, більш складні і актуальні загрози.

Важливо, щоб регуляторні органи надавали чітке визначення загрози, щоб менеджери з безпеки та персонал, який працює в безпосередній близькості до неї, точно знали, що саме вони намагаються виявити і подолати. Нечіткі визначення загроз можуть призвести до того, що оперативні працівники неправильно калібруватимуть своє обладнання, або, що ще гірше, якщо загроза не буде чітко визначена, вона може взагалі не бути усунута. Якщо регулятор не визначає таран терміналу як загрозу, то оператори аеропортів можуть не відчувати себе зобов'язаними встановлювати бар'єри проти тарану. Коротше кажучи, визначення загрози має бути кількісним, якісним і заснованим на сценарії, наприклад, збройний напад на термінал з боку супротивника, що складається з двох-трьох терористів, озброєних автоматичною зброєю і СВУ.

##### Використовуйте дані про подорожі пасажирів авіакомпаній для скринінгу на основі оцінки ризиків

Іменні записи пасажирів (PNR) - це комерційні записи для зберігання бронювання авіаквитків і записів, пов'язаних з іншими туристичними послугами. Наприклад, один PNR може містити дані про одного мандрівника, цілу сім'ю або туристичну групу, а також про всі послуги для їхніх подорожей від різних постачальників, таких як авіа- та залізничні перевезення, готелі та оренда автомобілів. Дані PNR можуть бути дуже корисними, оскільки вони розкривають зв'язки пасажира, його діяльність, смаки та вподобання. Дані PNR зазвичай містять номери кредитних карток, номери телефонів, адреси електронної пошти, адреси інтернет-протоколів, а також місце і спосіб оплати. Сфокусований аналіз PNR пасажира може надати важливі вказівки на те, що щось не так і/або не відповідає правилам. Ці ознаки, які іноді називають "*червоними прапорцями",* не завжди означають, що з ними пов'язана незаконна діяльність. Однак історія показує, що майже у всіх випадках перевірки після терактів показують, що "червоні прапорці" були присутні.

Під час терактів 11 вересня Федеральне бюро розслідувань США та Федеральне авіаційне агентство зобов'язали авіакомпанії використовувати комп'ютеризовану систему, яка використовувала як дані PNR, так і прогнозований профіль терориста, відому як Комп'ютерна система попереднього огляду пасажирів (CAPPS). Мета системи полягала у виявленні потенційно небезпечних пасажирів, чиї сумки перевірялися на наявність вибухових речовин і не допускалися до завантаження в літак, поки пасажир сам не підніметься на борт літака. На жаль, основна увага системи CAPPS була зосереджена на перевірці зареєстрованого багажу пасажира; система не мала жодного впливу на рівень перевірки пасажирів та їхньої ручної поклажі на контрольно-пропускних пунктах. У випадку терактів 11 вересня система CAPPS ідентифікувала 11 з 19 викрадачів трьох з чотирьох літаків того фатального дня, але не змогла втрутитися щоб запобігти атакам.

Цей збій є гарним прикладом того, що система AVSEC є негнучкою і жорсткою, оскільки вона змогла виявити, але не адаптуватися до загрози викрадачів-самогубців. Експерти з авіаційної безпеки розуміють, що дані PNR наразі не використовуються на повну потужність. Дані PNR містять потужні індикатори, які слід використовувати для впровадження ризик- орієнтованого підходу д о скринінгу. Для того, щоб застосувати цей підхід, необхідно вирішити законні проблеми конфіденційності і укласти міжнародні угоди щодо обміну та захисту інформації PNR.

##### Інтегрувати поведінкове виявлення Програми

На додаток до використання інформації PNR, ще одним важливим інструментом, який можна використовувати для скринінгу на основі оцінки ризиків, є виявлення поведінки або програми спостереження за пасажирами. Концепція виявлення поведінки працює т а к само, як і використання даних PNR. У той час як дані PNR виявляють індикатори або "червоні плями" в записах про пасажира, виявлення поведінки фокусується на поведінці пасажирів або їхніх контекстуальних обставинах. Важливо зазначити, що ця практика не є расовим профілюванням у будь-якій формі, а скоріше виявленням підозрілої поведінки та діяльності, яка може бути притаманна авіаційним терористам. Індикатори підозрілої поведінки є наслідком того, що терорист перебуває в стані стресу, і включають в себе хвилювання, агресивність та інші прояви поведінки, які відрізняються від поведінки добросовісних пасажирів.

Декілька країн - зокрема, Ізраїль, Сінгапур, Велика Британія, Сполучені Штати та Ізраїль - вже впровадили програми спостереження за пасажирами в аеропортах і д о с я г л и значних успіхів у виявленні злочинної діяльності. ІКАО зареєструвала виявлення поведінки в Додатку 17 до Чиказької конвенції як рекомендовану практику AVSEC для всіх країн.

##### Розробка та впровадження системи громадської безпеки в аеропортах Програми

Інший виклик в авіаційній безпеці полягає в тому, як розширити можливості, не покладаючись на ресурсоємні рішення, які є дорогими і, в більшості випадків, недоступними. Одним із способів досягнення цієї мети є залучення всієї спільноти аеропорту до забезпечення безпеки. Співробітники служби безпеки та їхні команди не зможуть досягти високого рівня безпеки без залучення всіх зацікавлених сторін на об'єкті, в установі або на підприємстві, де вони працюють. Іншими словами, стало загальноприйнятим, що безпека має бути справою кожного, і ця концепція виявилася дуже успішною. Цю ж концепцію можна реалізувати на арені AVSEC з таким же успіхом. Ідея полягає в тому, щоб усі зацікавлені сторони в аеропорту, в тому числі і не пов'язані з безпекою співробітники, робили свій внесок у забезпечення безпеки. Мета полягає в тому, щоб ефективно використовувати ресурси, не пов'язані з безпекою, в якості мультиплікатора для забезпечення безпеки. Хтось може запитати, чому ці співробітники аеропорту повинні робити внесок у забезпечення безпеки на додаток до своєї повсякденної роботи - і без додаткової оплати. Якщо коротко, то в їхніх інтересах, щоб аеропорт був безпечним і захищеним, оскільки терористична атака загрожує не лише їхньому заробітку, але й життю. Тому, за умови правильного пояснення та обґрунтування, можна отримати підтримку більшості працівників на підтримку такої програми.

Програми громадської безпеки в аеропортах не передбачають, що працівники, які не є співробітниками служби безпеки, будуть присвячувати багато часу роботі з безпеки, але коли кожен співробітник робить невеликий внесок у забезпечення безпеки, це підвищує загальний рівень безпеки. Наприклад, квиткові касири, які реєструють пасажирів на рейси з позначкою "f", зазвичай не задіяні в жодному з процесів забезпечення безпеки в аеропорту, але вони більше спілкуються з пасажирами, ніж більшість співробітників служби безпеки в аеропорту, а отже, вони найкраще знають типи пасажирів, які відвідують різні рейси з позначкою "f". За допомогою короткого, цілеспрямованого тренінгу таких квиткових агентів можна навчити виявляти нестандартні індикатори або поведінку пасажирів з червоним ф-лагом, і ці дані можуть бути включені в систему скринінгу, що базується на оцінці ризиків. Іншим прикладом є залучення працівників аеропорту, які працюють на інформаційних стійках в залах аеропорту. Ці працівники проводять значну частину свого часу, спостерігаючи за діяльністю в залах аеропорту і чекаючи, поки пасажири звернуться за допомогою. Знову ж таки, після невеликого навчання ці працівники можуть допомогти службі безпеки аеропорту, виявляючи та повідомляючи про несанкціоновану діяльність. Таке навчання можна проводити з усіма різними групами працівників аеропорту, включаючи продавців, прибиральників, обробників багажу та диспетчерів аеропорту.

Такі типи програм громадської безпеки є високоефективними і значними мультиплікаторами, які покращують місцеву і міжнародну авіаційну безпеку. Для реалізації такої програми необхідна підтримка всіх зацікавлених сторін, а також центральна організація, яка б очолювала, розробляла і впроваджувала таку програму. У Сінгапурі уряд реалізував таку програму в аеропорту Чангі та інших пунктах перетину кордону зі значним успіхом. Програма, відома як інтегрована система перевірки осіб, орієнтована на виявлення загроз (TOPSIS), за перший рік свого впровадження досягла 60- відсоткового збільшення виявлення злочинної діяльності в аеропорту без будь-яких переривання пропускної здатності або пасажирських перевезень. TOPSIS має багато додаткових успіхів у сфері національної безпеки, з якими читачі можуть ознайомитися в Інтернеті. Програми спільнот з безпеки аеропортів, такі як TOPSIS, представляють сучасний підхід до безпеки, який може додати значні ресурси для посилення безпеки аеропортів, роблячи її більш гнучкою і менш передбачуваною для супротивника.

##### Аеропорт Харден Периметр

Хоча останніми роками в аеропортах не було терористичних атак на злітно-посадковій смузі, мали місце інші кримінальні події, пов'язані з проникненням через периметр аеропорту. На додаток до крадіжки діамантів в аеропорту Брюсселя в 2013 році, про яку йшлося раніше в цьому розділі, два помітних випадки проникнення транспортних засобів сталися в аеропортах Ліона, Франція, в 2018 році, і Ван-Найса, Каліфорнія, в 2020 році. Ці інциденти не були пов'язані з тероризмом, але вони наочно демонструють існуючі вразливості повітряного простору і підкреслюють важливість посилення периметра для запобігання можливим терористичним атакам. Звичайно, ми не маємо на меті перетворити периметр аеропорту на фортецю. Потрібно, щоб будь-яка спроба перерізати, перелізти або протаранити периметр викликала тривогу, яка дозволить службі безпеки аеропорту відреагувати і перехопити загрозу, поки вона знаходиться на відстані від терміналів аеропорту або літаків, що здійснюють руління. Деякі аеропорти вже інвестували в надійну огорожу периметра, але для того, щоб підвищити необхідний стандарт для всіх, потрібні регуляторні дії. У наступному розділі буде розглянута потреба в регуляторних діях як наступна рекомендація.

##### Вдосконалення регулювання громадських зон аеропорту

Як зазначалося в розділі, присвяченому наземним атакам, вимоги щодо заходів фізичної безпеки, які слід вживати для захисту наземної частини або громадських зон аеропортів, відсутні або дуже мінімальні. Повинні існувати мінімальні стандарти, що стосуються структури аеропорту, фасадів, захисту узбіччя, транспортних засобів, що залишаються без нагляду, т а озброєної охорони. Ці стандарти будуть особливо актуальними для нових терміналів на стадії попереднього проектування і для модернізації терміналів. Впровадження заходів безпеки на етапі проектування будівельного проекту - це економічно ефективний спосіб досягти бажаного рівня безпеки з мінімальним впливом (низький однозначний відсоток) на загальну вартість проекту.

##### Уникайте надмірного покладання на показання та попередження Розвідка

Досвід показує, що більшість терористичних атак проти авіації відбуваються або без попередження, або за розвідувальними даними, які мають занадто загальний характер, щоб допомогти сфокусуватися на реагуванні AVSEC. Для посадових осіб AVSEC було б розумно дотримуватися базового припущення, що напад на авіаційні інтереси може статися в будь-який час і без будь- якого попереднього попередження розвідки. Також важливо, щоб відповідні розвідувальні дані, пов'язані з авіаційними загрозами і можливостями терористів, надавалися посадовим особам, відповідальним за захист авіаційних об'єктів. Підтримувати пильність і готовність персоналу служби безпеки в період підвищеної загрози відносно легко, тому важливою функцією керівників служб безпеки є використання інструментів, які дозволять підтримувати високий рівень пильності навіть за відсутності попередження від розвідки. Відділи безпеки аеропортів також повинні розвивати власні можливості зі збору розвідувальної інформації, приділяючи особливу увагу незвичайним подіям, що відбуваються в аеропорту, які можуть бути перевіркою безпеки або ворожими концепціями. Ці події слід реєструвати та відстежувати тенденції. Розвідувальною інформацією з аеропортів також слід ділитися з ширшою спільнотою AVSEC, що може допомогти виявити закономірності діяльності.

##### Пріоритетність людського фактору**:** Підбір персоналу та навчання

Цей розділ демонструє, що авіаційна безпека - це складна система, яка має справу зі складними загрозами, використовуючи при цьому сучасні технології. Для того, щоб відповісти на численні виклики, з якими стикається галузь, вкрай важливо, щоб персонал AVSEC, як керівники, так і рядові співробітники, мав належну кваліфікацію і проходив належну підготовку. Протягом багатьох років працівники служби контролю в аеропортах не отримували належної підготовки та винагороди, і в багатьох випадках посада працівника служби контролю в аеропортах була роботою початкового рівня. Такий тип управління персоналом може в кінцевому підсумку призвести до ситуацій, коли вся система може вийти з ладу або зруйнуватися через людську помилку одного працівника служби безпеки, який знаходиться на передовій лінії. Надзвичайна подія, що сталася в міжнародному аеропорту Едмонтона 20 вересня 2013 року, ілюструє цю тезу. Тут працівник служби безпеки аеропорту зупинив 18-річного пасажира після того, як виявив у його ручній поклажі щось схоже на трубчасту бомбу. Пасажир пояснив, що він сконструював цей предмет у минулому як хобі і забув його у своїй сумці. Неймовірно, але інспектор сказав пасажиру, що він може залишити цей предмет на борту літака. Однак пасажир наполягав на тому, щоб виріб залишився у контролера, тож контролер прийняв пристрій і дозволив пасажиру сісти на літак, що прямував до Мексики. Пристрій був шість дюймів завдовжки і два дюйми в діаметрі, начинений порохом. Він мав гвинти з обох боків і триметровий запал, що проходив через нього. Трубчаста бомба лежала в сміттєвому баку разом з іншими конфіскованими предметами, поки через чотири дні диспетчер не повідомив про неї поліцію в аеропорту.

Щоб запобігти повторенню подібних подій і розробити професійну, надійну систему безпеки, важливо найняти потрібних людей, а також навчити і винагородити їх. Навчання, орієнтовані на загрози, або "червоні команди", є ще одним важливим і потужним інструментом для створення і підтримки професійної готовності персоналу AVSEC і зниження рівня людських помилок. Інтеграція технологій надзвичайно важлива для авіаційної безпеки, і вона набуватиме все більшого значення, але без професійних, пильних і мотивованих офіцерів досягнення більш безпечної і менш вразливої авіаційної галузі буде неможливим.

### Висновок

Цей розділ присвячений особливостям сектору цивільної авіації як критично важливої інфраструктури на національному та глобальному рівнях. Авіаційна безпека - це складна система, яка працює у все більш складному середовищі. Терористи продовжуватимуть націлюватися на авіаційні об'єкти по всьому світу з багатьох причин, розглянутих у цьому розділі, і намагатимуться використати різні вразливості, виявлені в різних тематичних дослідженнях. Студенти і фахівці з безпеки та управління ризиками повинні розуміти, що не існує такого поняття, як 100-відсоткова безпека, проте наслідки численних, витончених атак на цивільну авіацію можуть бути руйнівними з точки зору людських жертв і економічних наслідків. Тому досягнення такого рівня безпеки, який пом'якшує ці види загроз, дозволяючи авіаційній галузі здійснювати свою діяльність і досягати поставлених цілей, є вкрай важливим. Різноманітні рекомендації, що обговорюються, надають можливість покращити можливості у сфері авіаційної безпеки. Фахівці AVSEC, а також ті, хто їх підтримує і допомагає їм, повинні постійно шукати шляхи підвищення ефективності, зменшення вразливості і посилення стримування потенційних зловмисників.

# - 7 -

## Залізничні перевезення громадського транспорту

Адріан Дуайєр

У цьому розділі розглядається вразливість залізничного транспорту до терористичних атак. Основна увага приділяється тим методам атак, які використовувалися раніше, але залишаються актуальними. Всюди підкреслюється вразливість, притаманна відкритим транспортним мережам, які також є тісно пов'язаними системами. У таких системах деструктивний інцидент має властивість швидко поширюватися по всій мережі і спричиняти низку непередбачуваних і часто смертельних наслідків. З точки зору Організації Північноатлантичного договору (НАТО), напад на залізничні мережі в країнах-членах НАТО може також порушити військову логістику, цивільний ланцюг постачання і економічне процвітання в цілому. Цей розділ не є оцінкою загроз і не передбачає майбутніх подій у часі чи просторі. Замість цього вона складається з чотирьох розділів і використовує правдоподібність як відповідний лейтмотив для управління ризиками, пов'язаними з тероризмом, в умовах невизначеності.

* + У Розділі 1 розглядається вразливість, притаманна залізниці, і необхідність пропорційного підходу при оцінці ризику в контексті. У цьому розділі обговорюється, як протистояти складнощам загрози з точки зору реагування на сприйняту загрозу в рамках правдоподібності. У ньому окреслено один з підходів до процесу стратегічної оцінки ризиків.
  + У Розділі 2 розглядається багатогранна природа залізничних перевезень, а також подальший розвиток масштабу та обсягу проблеми управління ризиками. У ньому зазначається, що охорона правопорядку та безпека не є взаємозамінними поняттями, і що користь з точки зору громадської безпеки та управління суспільними ризиками є максимальною, коли ці зусилля працюють безперебійно.
  + У розділі 3 використовуються дані тематичних досліджень з Великої Британії, континентальної Європи, США, Японії та Індії, щоб показати, як суб'єкти загроз використовують притаманну їм вразливість. Ці 15 прикладів варіюються від нескладних фізичних нападів до масштабних подій з масовими жертвами.
  + Розділ 4 підсумовує наявні уроки. У ньому зазначається, що певні теми в методах нападу часто повторюються, і що це спостереження особливо актуальне при спробах управляти ризиками в умовах невизначеності. На завершення розділу зазначається, що хоча загроза тероризму є різноманітною, притаманну йому вразливість можна зменшити.

Залізниці вразливі від **Design**

##### Внутрішня вразливість та стратегічна оцінка ризику

Мережі громадського транспорту і вантажних перевезень, що використовують постійну залізничну інфраструктуру, за своєю природою є вразливими до терористичних атак. Тут вразливість пов'язана з відкритим доступом, передбачуваними і жорсткими операційними параметрами, а також багатим на мішені характером операційного середовища. Також важливою є стратегічна важливість соціально-економічних функцій залізниці. Таким чином, головним завданням боротьби з тероризмом є захист пасажирів і залізничних активів, не ставлячи під загрозу основну мету підприємства: сприяти безперешкодному переміщенню людей і товарів у своєчасний і ефективний спосіб. Термін "ефективний" включає в себе поняття безпеки та надійності.

Для ефективного функціонування мережі необхідно передбачати ризики, визначати їх пріоритетність і належним чином управляти ними.1 В рамках виклику КТ встановлення наукової ймовірності прояву зловмисного акту в межах корисних часових і просторових параметрів є проблематичним.В умовах такої невизначеності будь-яке випадкове використання терміну "ймовірність" може вводити в оману і сприйматися як рівень впевненості, який є невиправданим з огляду на масштаби невідомих. На відміну від цього, визначення вірогідності конкретного методу нападу (МН) і його передбачуваного впливу у визначеному контексті є більш всеохоплюючим процесом, який враховує неминучу невизначеність. Інформація про загрозу розглядається на основі обґрунтованого судження, яке ґрунтується на доказах, відповідному досвіді, спеціальних знаннях оперативної обстановки і, за необхідності, на явних припущеннях. На Мал. 7-1 показано взаємозв'язок між цими термінами в контексті визначення ризику.

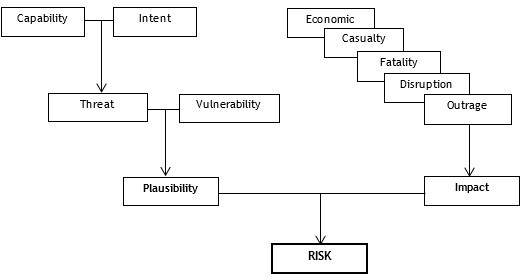


Рисунок **7-1.** Взаємозв**'**язок між термінами в оцінці ризиків

(Діаграма адаптована з сайту Кабінету міністрів Великої Британії)

Розробка стратегічної оцінки ризиків (СОР) передбачає поєднання декількох оцінок ризиків у рамках конкретного контексту, що враховує ймовірні МН у поєднанні з низкою достовірних намірів, які приписують суб'єктам загрози. Цей інклюзивний підхід, що поєднує якісні та кількісні дані, ґрунтується на концепції обґрунтованого найгіршого випадку (RWC). У Сполученому Королівстві RWC - це "найгірший ймовірний прояв даного конкретного ризику (після того, як були в і д к и н у т і малоймовірні варіанти)". Ця форма слів являє собою більш узагальнене використання мови, ніж та, що зазначалася раніше, де зловмисні дії визначалися на основі зміни вірогідності та впливу. Вірогідність застосовувалася лише до нещасних випадків і природних загроз - тобто тих подій, для яких дані вважалися більш повними і надійними.5

При комплексній оцінці ризику на кількісні оцінки вразливості та привабливості об'єкта для суб'єктів загрози впливають попередні зобов'язання та упередженість оцінювачів, що зумовлює потребу в більш інклюзивному та прозорому процесі, який би враховував наступні питання:

* + Які ризики є вірогідними, а не всі, які можна собі уявити
  + Операційний контекст, в якому застосовуються ймовірні ризики, наприклад, на які групи населення вони впливають, як вони можуть комбінуватися, чи є вони просторово або часово специфічними.
  + Яким чином кваліфікується обґрунтування, що підтримує ранжування ризиків

Ситуація, в якій оцінки ризиків не відповідають стратегічним рамкам і ґрунтуються переважно на узагальнених розвідувальних даних, а зацікавлені сторони свідомо чи несвідомо дотримуються різних світоглядів, з меншою ймовірністю призведе до бажаного результату. Така ситуація також являє собою підхід до управління ризиками, який може бути складно виправдати перед обличчям ворожої перевірки. Див. також корисний коментар щодо оцінки та управління ризиками в розділі 13.

Залізничні інциденти, через природу тісно пов'язаної системи, в якій вони відбуваються, мають потенціал до швидкої ескалації в часі і просторі, і ця проблема загострюється, коли відомою або підозрюваною причиною є тероризм. Поява примари тероризму висуває додаткові вимоги до когнітивних ресурсів осіб, які приймають рішення, які часто перебувають під великим тиском. Наприклад, чи первинне повідомлення є завершенням фази атаки чи її початком? Чи терористи все ще перебувають на місці події, чекаючи, щоб скористатися неминучою плутаниною і націлитися на тих, хто реагує? Чи очікуються інші атаки в інших частинах мережі? Всі ці питання є актуальними але достовірних відповідей на них може не бути, що ще більше посилює вплив невизначеності на процес прийняття рішень.7

У цьому розділі на основі 15 унікальних прикладів розглянуто вразливість залізничного транспорту в конкретному контексті та висвітлено деякі варіанти реагування, що ґрунтуються на принципах стійкості. Мета цієї методології - передати суть того, що сталося в цих ситуаціях, у зрозумілій формі та допомогти розвинути передбачення на основі уроків інших. Підхід враховує варіації, пов'язані з тим, як працюють залізниці та як суб'єкти загроз використовують вразливості, що виникають в результаті цього. Приклади зосереджені на тому, що, як свідчить історія, є пріоритетними цілями: пасажири та вразливі елементи доступної інфраструктури, а не вантажі, що перевозяться транзитом.8 Історична спрямованість цих переважних цілей не означає, однак, що деякі види вантажних перевезень - наприклад, ядерні матеріали або певні види хімічних речовин - не мають особливої привабливості для суб'єктів, що загрожують безпеці. Якщо розглядати лінію маршруту (ЛМ), то довгострокове блокування через терористичну діяльність трапляється рідко. Навмисне або поспішне руйнування, особливо монолітних споруд, вимагає досвіду і ресурсів, якими не володіють багато терористів- початківців або навіть деякі вже відомі терористи. Це спостереження є ключовим для раціональної оцінки можливостей і намірів суб'єкта загрози - тобто, ймовірної загрози, яку він може становити. Див. також коментар щодо фізичних загроз у розділі 2.

Серед прикладів, наведених у цьому розділі, відсутній кібертероризм, який є сферою, що викликає все більше занепокоєння. З точки зору мережевих залізничних систем, кібератаки не є ефективним видом МО і на сьогоднішній день не можуть бути прирівняні до атак із застосуванням фізичних засобів, таких як саморобні вибухові пристрої (СВП), вогнепальна зброя і атаки із застосуванням гострої, холодної зброї (СХЗ). Кібератаки, зафіксовані у відкритих джерелах, найчастіше являють собою дії типу "відмова в обслуговуванні", часто пов'язані з вимаганням або отриманням конфіденційних даних.10 У цьому відношенні цінність глав 3-5 і 14, кожна з яких присвячена різним кіберзагрозам і суб'єктам, полягає в тому, що вони надають необхідну інформацію для проведення загальної оцінки ризиків з урахуванням визнаних передових практик, незалежно від намірів зловмисника.

##### Ціль вибору чи Можливість**?**

Потенційні нападники представляють широку аудиторію, включаючи ідеологів, незадоволених, невдоволених і стурбованих. Усіх їх приваблюють залізничні об'єкти, які мають одну або більше з наступних характеристик:

(1) легкодоступні з обмеженими шансами на компрометацію під час ворожої розвідки або безпосередньо перед нападом;

(2) важко захистити від обраної мішені;

(3) може призвести до непропорційних наслідків і висвітлення в ЗМІ відносно невеликої атаки.

Високо мотивовані і багаті на ресурси терористи можуть здійснити майже одночасні напади на переповнені потяги в столицях, як, наприклад, теракт в Токіо 1995 року, вибухи в Мадриді 2004 року і вибухи в Лондоні 2005 року (приклади 11, 10 і 9 відповідно). На протилежному кінці спектру, ошукані і слабкі люди, які завжди краще озброєні, ніж їхні нічого не підозрюючі жертви, можуть просто вибрати найближчу станцію до свого будинку або роботи для нападу (див. приклади 4-7). Зауважте, що в одному з таких випадків самотній суб'єкт, який розпочав криваву атаку з використанням СББ проти цивільних осіб, врешті-решт був затриманий чоловіком, який озброївся бивнем нарвала, а інший - вогнегасником, доки не прибула озброєна поліція і не нейтралізувала нападника.

Широта цього континууму привабливості є викликом для тих, хто намагається побудувати послідовне обґрунтування, за допомогою якого можна було б визначити пріоритетність ризиків і розподілити обмежені ресурси. В основі цього континууму лежить невизначеність, оскільки залізниця є експансивною мішенню, відкритою для цілого ряду міністерств оборони. Особливо на продромальній фазі майбутньої атаки мотиви і наміри суб'єкта загрози можуть бути незрозумілими. Як робоче припущення, зусилля, які терористи мають докласти для досягнення певної мети, і те, чи вважають вони, що інвестиції варті цих зусиль, можуть вплинути на вибір цілі. Цей аналіз витрат і вигод може бути особливо застосовним, коли витрати для суб'єкта загрози розраховуються в широкому сенсі, включаючи необхідні зусилля, що сприймаються як здійснення складної атаки, перспективи компромісу і шанси досягти бажаного результату. Цей розрахунок, можливо, є однією з причин - а можливо, і причиною того, що залізниця так часто використовується як вектор для невибіркових атак з масовими жертвами, а не для справді стратегічних операцій, спрямованих проти елементів критичної національної інфраструктури.

З історичної точки зору, бомбардування переповнених поїздів і станцій є добре відомою тактикою терору. Наприклад, у 1800-х роках у Лондоні Ірландська республіканська армія (ІРА) особливо активно діяла на залізниці та поблизу неї. У "S-плані" ІРА ("S" - саботаж) початку ХХ століття зазначалося, що транспортна інфраструктура є "чи не найважливішою з усіх" цілей для нападу, оскільки спричинені нею "серйозні руйнування матимуть паралізуючий вплив на кожну галузь промислового і комерційного життя". Особливо очевидні в сучасній ідеології джихадистів, але також привабливі для суб'єктів, які керуються іншими мотивами, м'які залізничні об'єкти є надійними цілями для вибору (див. приклади 9-11). Багатолюдні громадські місця - це середовище, де агресивний дух суб'єкта загрози може подолати відсутність планування, обмежені технічні навички і мізерні ресурси (див. приклади 4-7). Існують також численні приклади слабких атак, які не досягли очікуваної мети, але, тим не менш, призвели до значних соціальних потрясінь і дезорганізації та викликали значний суспільний резонанс (див. приклади 8 і 12). Вплив не пов'язаних між собою низькорівневих інцидентів може легко об'єднатися, щоб підвищити занепокоєння як серед користувачів залізниці, так і серед тих, хто реагує на інциденти. За відсутності стійкого підходу до управління ризиками, уникнення ризику перед обличчям нечітко визначеної загрози може паралізувати послуги, закрити станції, поставити поїзди в незручне положення (таким чином, перешкоджаючи відновленню роботи), спричинити перехресні перебої в роботі різних видів транспорту і створити незручності для великих верств населення (див. приклад 13). Передбачуваним наслідком такого підвищеного занепокоєння є перенесення ризику, особливо якщо користувачі залізниці переходять на менш безпечні види транспорту.

Неприйняття ризику характеризується реакцією, яка:

(1) є непослідовною, наприклад, евакуація станції після загрози вибуху, не знаючи, чи існує бомба або інша небезпека, або де вона може бути розташована;

(2) містить елементи відчутної інерції рішень, коли перевага надається загальному плану, а не управлінню ризиками в конкретному контексті (наприклад, вказуючи один і той самий пункт евакуації для всіх небезпек, від пожеж до бомб і всього, що між ними);

(3) втілює непотрібну надмірну реакцію, виправдану вкрай вибірковим і спекулятивним принципом запобіжності.

Розглянемо приклад Умара Фарука Абдулмуталлаба, терориста, який зашив вибуховий матеріал у свої шорти, щоб обійти заходи перевірки в аеропорту. Див. детальний опис цього випадку в розділі 6. Цей езотеричний МЗ , спрямований проти літака у світловому діапазоні, дехто екстраполював як такий, що має відношення до залізничного транспорту масового користування. У їхньому аналізі відсутнє будь-яке визнання того, що доступ до поїздів і станцій не передбачає обов'язкового огляду спідньої білизни пасажирів. Тим не менш, ресурси були, хоча і тимчасово, перенаправлені на легко уявляється, але неправдоподібне використання трусів з вибухівкою, що активуються користувачем, які носяться в інтимній обстановці, і мають низьку потужність.

Підсумовуючи, можна сказати, що залізничні мережі легкодоступні і складні для захисту, і навіть незначна атака може призвести до масштабних руйнувань, неспівмірних з витраченими зусиллями. Є всі підстави вважати, що суб'єкти загроз розглядають залізничні мережі таким же чином. Наступний розділ розширює дискусію, характеризуючи природу операційного залізничного середовища і контекстуалізуючи деякі з основних викликів в управлінні ризиками.

### Багатогранна природа залізниць

##### Складність

Термін "залізниця" є загальновизнаним, але знайомство з ним не завжди є синонімом розуміння. Складні і рідко піддаються структурним змінам, залізничні системи функціонують як одно- і мультимодальні вузли і лінії зв'язку та сприяють виконанню цілого ряду різноманітних функцій. Ці функції включають комерційну та промислову діяльність, роздрібну торгівлю, офісні та рекреаційні простори, а також місця для соціальних зустрічей. Чим складніша система, тим ширший спектр проблем в управлінні ризиками, які необхідно подолати. Огляд розробки стратегій управління ризиками див. у главі 13. Нижче наведено деякі складнощі, притаманні залізницям:

* + Громадський простір важко регулювати. Архітектура безпеки залізниць означає, що багато усталених технологічних рішень, які використовуються в інших сферах, є:

-нездійсненними, оскільки фізичну структуру важко модифікувати:

-непрактичні, оскільки усталена культура використання залізниць є вкоріненою;

-не бажані через передбачувані негативні наслідки скупчення людей (від ковзання, спотикань і падінь до ненавмисного створення додаткової зони вбивств). Аналіз авіаційної безпеки в розділі 6 містить багато цікавих паралелей з цього приводу.

* + Особистість тих, хто користується цією системою, здебільшого невідома. З практичної точки зору, неможливо уявити, що в рамках існуючої культури залізничних перевезень пасажири прибуватимуть або зможуть прибути за кілька годин до поїздки і проходитимуть перевірку особи.
  + Існують лише мінімальні перевірки для обмеження того, що люди мають при собі та в багажі. Через величезний пасажиропотік і передбачувані ризики перешкоджання вільному пересуванню, такі як скупчення людей в обмеженому просторі, важко забезпечити дотримання обмежень.
  + Управління великими обсягами залізничних перевезень за розкладом (пасажирських і вантажних) вимагає точної і централізованої координації. Особливо в умовах зловмисних дій, ця точність може бути використана для створення єдиних точок відмови. Залізничні системи охоплюють величезну географічну територію, і межі між залізницею і навколишнім середовищем - і навіть між різними елементами однієї і тієї ж мережі - буває важко визначити. Без належної уваги можна загострити робочі відносини і створити некорисні війни за територію та юрисдикційні проблеми.
  + Значна частина розосередженої інфраструктури доступна з мінімальними фізичними перешкодами через санкціоновані та несанкціоновані точки доступу. Межі доступу часто є відокремленими, і їх проблематично захистити навіть від випадкових порушників. З точки зору пасажирських перевезень, доступ до мережі через станцію з низьким рівнем ризику майже напевно сприятиме безперешкодному пересуванню до місць з більш високим рівнем ризику.
  + Існує багато нормативних і похідних зацікавлених сторін, і навряд чи існує єдина ієрархія пріоритетів. Ця динаміка особливо помітна, коли залізничні послуги перетинають місцеві, регіональні або національні кордони.
  + Пасажири не є згуртованою групою. Діапазон поведінки, яка вважається нормальною, може бути дуже широким, а індивідуальна або групова реакція на нестабільність системи може бути непередбачуваною. Як основні зацікавлені сторони, їх, як відомо, важко залучити, і без особливої обережності заходи зі зниження ризиків можуть спровокувати збільшення ризиків.
  + Підтверджені або підозрювані терористичні інциденти завжди є чистими споживачами ресурсів КТ. Наприклад, реагування, описане в прикладі 9, вимагало тривалої передислокації сил і засобів не лише з Лондона, але й з усієї Англії, Шотландії та Уельсу.

##### Регуляторний та політичний Напрямок

Залізниці працюють в рамках політичного керівництва на місцевому, регіональному та національному рівнях, а також стикаються з іншими конкуруючими комерційними імперативами. Хоча навряд чи це вплине на діяльність з управління ризиками в рамках негайного реагування після атаки, політичні укази можуть обмежити прийняття операційних рішень за обставин, коли нові і більш широкі політичні цілі прискорюють або затримують повернення до звичайного режиму роботи (BaU). Такі непередбачувані ситуації, коли політичні, операційні та комерційні імперативи зливаються воєдино, виграють від того, що вони заздалегідь плануються і в принципі узгоджуються всіма зацікавленими сторонами. Це означає, що бажано досягти широкого консенсусу до того, як передбачувані події стануть реальністю, і, звичайно, до того, як будь-яка схильність до несхильності до ризику обмежить можливості, що існують. Прикладами такого підходу є використання шаблонів для прийняття рішень або меморандумів про взаєморозуміння, що визначають умови, необхідні для закриття залізничних перевезень у відповідь на пряму зловмисну загрозу або пов'язаний з нею інцидент, відновлення роботи, якщо ця загроза не реалізується, і управління процесом повернення до нормальної роботи після нейтралізації загрози.

##### Охорона правопорядку та безпека

Що стосується практик, відомих як охорона правопорядку та безпека, то коли ролі та обов'язки переплутані, виникає вразливість. Охорона правопорядку в чистому вигляді означає підтримання миру і верховенства права. Активне забезпечення правопорядку, безумовно, здатне протидіяти тероризму, а також стримування, виявлення або витіснення її прихильників, але не ізольовано. Успіх більш вірогідний там, де функціональна структура оптимізована для охорони правопорядку на залізниці як специфічного завдання, а також там, де накопичена і зберігається організаційна пам'ять. Він менш очевидний, коли залізниця є просто ще одним електоратом в рамках загальних зусиль з охорони правопорядку. На відміну від цього, безпека є ширшим поняттям, яке включає в себе ряд фізичних і процедурних заходів, необхідних для того, щоб зробити напад менш імовірним, а будь-яке реагування - більш ефективним. Як вид діяльності, що відноситься до КТ, безпека, швидше за все, буде здійснюватися під керівництвом галузі - під керівництвом або без керівництва регулятора або поліції - але завжди координується в рамках загальних зусиль з КТ. Користь з точки зору громадської безпеки та управління суспільними ризиками є максимальною, коли ці зусилля діють злагоджено. Цей бажаний результат найбільш ймовірний, коли інформація, необхідна для управління виявленими вразливими місцями, передається офіційними каналами, що включають канали комунікації як зверху вниз, так і знизу вгору. За необхідності, обмін чутливою інформацією, ймовірно, можливий лише в рамках службової необхідності за участю довірених партнерів. У цьому відношенні створення штучних бар'єрів - таких як групи безпеки, які виключають залізничних експертів лише тому, що вони не є професіоналами у сфері безпеки, - є передбачувано контрпродуктивним. Про ефективний обмін інформацією та розвідданими див. главу 11.

Залізничні мережі були задумані в той час, коли тероризм, хоч і не був невідомим, але, безумовно, був менш помітним і менш потужним, ніж у двадцять першому столітті. Багато станцій не піддаються встановленим режимам безпеки, наприклад, тим, що передбачають фізичний обшук і високу залежність від технологій виявлення. Використання стаціонарних детекторів, як особливо проблематичний приклад, ґрунтується на існуванні узгоджених експлуатаційних вимог, які відповідають на такі питання, як буде підтримуватися пропускна спроможність пасажирів під час обробки або використання даних про виявлення? Якщо обробка сигналу не є миттєвою, де може перебувати суб'єкт позитивного результату, коли буде зафіксовано тривогу, і як тоді буде ідентифіковано та визначено його місцезнаходження без затримок? Який очікуваний результат, якщо виявлено загрозу, пов'язану з СВП, вогнепальною зброєю або СБЗ, але суб'єкт загрози вже досягнув середовища, багатого на цілі? Якщо відомо, що рівень достовірності технології виявлення нижче 100 відсотків, то яку цінність має система? Які заходи, такі як додатковий персонал і пов'язане з ним навантаження на навчання, фізична безпека і пом'якшення наслідків вибуху, необхідні для отримання позитивних результатів? Існують також більш широкі питання питання: хто встановлює стандарти використання? Хто забезпечує дотримання стандартів? І, що не менш важливо, хто оплачує капітальні та поточні витрати?

##### ЗМІ Вплив

Напади, спрямовані проти залізничного транспорту, через характер небезпек, які вони несуть, і "жахливий ризик", який вони представляють, легко зрозумілі зацікавленим сторонам і широким верствам населення. Такі події - через те, що вони просякнуті смертністю, - незмінно висвітлюються в основних ЗМІ та соціальних мережах, що є додатковою привабливістю для суб'єктів, які несуть загрозу. Навіть у 2005 році цифри перегляду, опубліковані BBC, показали, що понад 50 відсотків британського населення дивилися випуски *новин BBC News* у день вибухів у Лондоні 7/7 (див. приклад 9). Це спостереження набуває особливої актуальності зараз, оскільки всепроникні відеозаписи з камер телефонів і миттєві повідомлення стали основними джерелами інформації. Фізичний напад привертає увагу там, де одна лише риторика може не привернути уваги, а інцидент, гідний уваги ЗМІ, дозволяє суб'єктам загрози продемонструвати свою владу в наочний і недвозначний спосіб. Більше того, суспільний інтерес і обурення (див. терміни на рис. 7-1) сприяють додатковому розголосу, що є додатковим пропагандистським бонусом. Кожен новий напад слугує нагадуванням про попередні звірства, і всі вони пов'язані спільною темою залізниці та вразливості її пасажирів. Цією готовою асоціацією можна маніпулювати далі, використовуючи тактику бінарного тероризму: поєднання фізичних атак з попередніми або наступними повідомленнями з погрозами, що передають неправдиву інформацію.

Терористичні сигнали такого типу посилюють спектральну природу загрози для залізничного транспорту (див. приклади 3 і 13), часто стаючи вектором, за допомогою якого увага громадськості відволікається від звірства до передбачуваних невдач у реагуванні. Визнання того, що такий вплив є основним елементом мотивації суб'єкта загрози, ще більше посилює важливість уникнення надмірної реакції, мінімізації руйнувань і прискорення повернення до нормального життя шляхом якнайшвидшого відновлення залізничного сполучення. Цей результат досягається найефективніше

коли ризик оцінюється в контексті, коли процес оцінки є інклюзивним (а не безпідставно чи цинічно вибірковим), і коли невизначеність визнається як неминучий наслідок боротьби зі зловмисними діями.

### Ймовірні методи атаки **(MoA)** в залізничному середовищі

Цей розділ розвиває теми, висвітлені в попередніх розділах, розглядаючи вразливість у контексті, використовуючи приклади інцидентів. Ці приклади ілюструють вірогідні та репрезентативні, а не лише нещодавні випадки ВП. У сукупності ці приклади підтверджують твердження про те, що контрзаходи, засновані на неправильному визначенні проблеми, можуть бути неефективними, спричиняти низку непередбачуваних негативних наслідків і бути проблематичними для захисту в разі судового оскарження. На відміну від наступних розділів, цей розділ починається з розгляду події, не пов'язаної з тероризмом у всіх аспектах, окрім як у свідомості деяких присутніх та ЗМІ, яким вони давали інтерв'ю.

Страх перед тероризмом

#### Приклад 1: Вибух електронної сигарети в лондонському метро (2014)

Приблизно о 9:00 ранку чоловік-пасажир поїзда метро на станції Ченсері-Лейн був здивований, коли його сумка-чоловік видала гучний "хлопок" і почала випускати дим. Зазирнувши всередину, він побачив, що його електронна сигарета, яка заряджалася через USB-порт комп'ютера, вийшла з л а д у . Корпус акумулятора розірвався через внутрішній тиск, що спричинило шум і дим. У той час як він був певною мірою заспокоєний побаченим, інші пасажири не були. Нижче наводимо цитату зі статті, опублікованої в газеті Huffington Post:

Пасажири кричали і вибігали зі станції Ченсері-лейн у центрі Лондона, а інші плакали після того, як о 9:30 ранку сталася тривога через загрозу безпеці. "Ви просто припускаєте найгірше, чи не так?" сказав [очевидець]. "Чесно кажучи, я не знав, що сталося".

Співробітники платформи були попереджені і поспілкувалися зі здивованим власником сумки. Він поводився нормально і запропонував логічне пояснення подій. Він показав співробітникам обвуглені залишки своєї електронної сигарети та комп'ютер.

На той момент не було видно ні вогню, ні диму. Не було жодних ознак навмисного вибуху або того, що електронну сигарету було модифіковано чи пристосовано для створення зброї. Співробітники, з якими він розмовляв і які перевірили записи з камер відеоспостереження, переконалися, що це був незначний нещасний випадок, і, відповідно до їхньої підготовки з питань безпеки, вони не повідомили про подію як про підозрілу поведінку. Рух потягів було відновлено з мінімальною затримкою.

Одночасно з прагматичним процесом оцінки, який проводив персонал на рівні платформи, пасажири, які самостійно евакуювалися, розповідали у Твіттері про свій досвід "підриву в метро". Ці повідомлення викликали інтерес ЗМІ, спрямований на поліцію та залізничного оператора. Через характер первинної інформації, що з'явилася в соціальних мережах, інцидент також привернув увагу спеціалізованих підрозділів комп'ютерної томографії. Одна зі свідків повідомила, що почула сильний вибух і люди кричали "бомба", коли з рюкзака почав виходити дим. Проте, як було відомо співробітникам і міліції на станції, не було ні рюкзака, ні потужного вибуху. Дійсно, не було ніякої бомби.

Ранні стадії залізничної аварії, особливо ті, що супроводжуються пожежею, вибухом або сходженням з рейок, можуть одразу відрізнити від терористичного акту. Здатність розпізнати ключові характеристики з перших повідомлень з місця події є конкретною причиною того, чому тісні робочі стосунки між залізничними операторами і службами реагування на КТ є бажаними і корисними. Використання спеціальних знань про те, як повинна працювати система - і, відповідно, що є небажаним, але нормальним, на відміну від дійсно несподіваного і підозрілого - є безцінним з точки зору колективної здатності відокремлювати сигнал від шуму (див. коментарі щодо ранніх повідомлень про вибух у прикладі 9). Перебої у наданні послуг незмінно привертають увагу ЗМІ, а страх перед тероризмом може викликати певну форму зараження серед розрізнених користувачів залізниць, провокуючи доброзичливі, але неправдиві повідомлення на великій території. Розвиток культури безпеки, в яку інвестує персонал, що знаходиться на передовій, є одним із засобів управління цією непередбачуваною ситуацією, як показано на прикладі 8.

##### Саботаж і напади на лінію маршруту **(LoR)**

Більшість випадків механічного або електричного саботажу залізничної інфраструктури, як правило, мають кримінальний характер, рідко керуючись терористичними методами. Враховуючи вразливість джерел живлення, сигнального обладнання, стрілочних переводів і постійних шляхів загалом, це можна вважати дивовижним. Існують приклади, коли групи, що займаються одним питанням, і окремі особи розміщують предмети на колії або намагалися закоротити чи спалити електричні кабелі. У 1995 році у Сполучених Штатах організація, щ о називала себе "Сини гестапо", втрутилася в роботу залізничних колій на віддаленій ділянці. Диверсанти підробили електричні з'єднання, щоб помилково вказати, що колія не пошкоджена. В результаті локомотив і 12 вагонів зійшли з рейок, а три вагони злетіли на 10 метрів у яр. Одна людина загинула і 60 отримали поранення. Незважаючи на людську трагедію, ця подія згадується найчастіше через її рідкісність, а не через її наслідки. Зовсім недавно джихадистські видання пропагували саморобний спусковий пристрій, виготовлений з бетону і сталі, що важить лише кілька кілограмів. Цей заклик до дії, схоже, не спрацював, оскільки жодного поїзда не було пущено під укіс (див. приклад 2). З практичної точки зору, на відміну від встановлення СВП (потенційно швидкого і більш ефективного варіанту атаки), механічний саботаж може зайняти багато часу, вимагати участі кількох виконавців на місці і, можливо, певних інсайдерських знань. Можливо, саме з цієї причини вибухівка залишається зброєю вибору (див. приклад 3).

#### Приклад 2: Привид джихаду Derailer

У 2017 році джихадистська публікація наголошувала на доцільності пуску під укіс поїздів у США і Канаді за допомогою спеціального пристрою, розміщеного вздовж лінії зіткнення. Тактичне використання такого пристрою, включаючи оптимальне розміщення, вибір часу атаки і приховування, детально не розглядалося. Метод також вимагав значних зусиль з точки зору будівництва об'єкта, що передбачало заливку бетонного клину, армованого заздалегідь виготовленою сталлю. Незважаючи на початковий ажіотаж у засобах масової інформації та деяких розвідувальних колах, стало очевидно, що існують простіші і більш правдоподібні варіанти сходження з рейок, як показують дані про залізничні аварії. Також було далеко не ясно, чи відповідав описаний об'єкт своєму призначенню.

#### Приклад 3: Британський досвід лоР Атаки

У 1991-2001 роках ІРА відповідальна за майже 70 інцидентів на залізниці, 30 відсотків з яких були спрямовані на об'єкти ЛЗ. Окрім залізничних колій, об'єктами нападів також були сигнальне обладнання, пов'язані з ними об'єкти інфраструктури і, рідше, але безуспішно, мости. У більшості випадків підривники використовували ізольованість обраних місць як тактичну перевагу. Приховування пристроїв, якщо такі були, було елементарним. В одному випадку СВП, яку просто поклали на баласт, але в безпосередній близькості від нього до рейки, підірвавшись під потягом, який щойно тимчасово зупинився. Варто також зазначити, що через використання ІРА пристроїв з таймером затримки і можливість змін у русі поїздів за розкладом, неможливо було точно знати, де саме перебуватимуть поїзди в момент підриву. Хоча сходження з рейок не було конкретним наміром терористів, доречно зазначити, що в кількох випадках можливість сходження з рейок на високій або низькій швидкості, схоже, була справою випадку.

Хоча деякі місця були обрані з високим рівнем популярності та інтенсивності торгівлі людьми, багато інших цілей були віддаленими і малозначущими. Очевидним було те , що терористи використовували стратегічну дорожню мережу для подорожі до залізничних цілей, часто отримуючи доступ там, де існуючий пункт пропуску та позашляхова стоянка збігалися. Цей тип аналізу був отриманий завдяки знанню місцевої залізниці та розслідуванню після інциденту. Він виявився особливо корисним при реагуванні на неоднозначні загрози вибухів, дозволяючи визначити пріоритетні зони інтересу і зосередити увагу на заходах реагування. Можна припустити, що саме "загартовування" середовища на вокзалі - включно зі стримуючим і доказовим впливом відеоспостереження, режимами перевірки вокзалів і поїздів, а також проактивними поліцейськими патрулями - відволікло терористів і перенаправило їхню увагу. Британський досвід показує, що такі заходи добре спрацювали у пріоритетних громадських місцях. Що стосується величезної кількості віддалених і відокремлених місць уздовж ЛЗ, то такі заходи були менш практичними.

В інших частинах світу, очевидно, що особи, які мали намір вчинити масові вбивства, часто використовували пристрої з командним управлінням і СВП, що спрацьовували від руху поїзда. Командний елемент - наприклад, дріт, радіо- чи телефонний сигнал або якийсь датчик - гарантував, що потяг, який рухається, перебуває в місці нападу або поруч із ним і наближається до нього на високій швидкості. Вибрані місця часто використовували імпульс поїзда, який штовхав вагони в більш небезпечну ситуацію. У країнах, які беруть участь у широкомасштабних громадянських або локальних конфліктахабо перебувають на межі таких конфліктів, характерним є збройний напад на тих, хто вижив. Варіації на цю тему мали місце в Таїланді, на Індійському субконтиненті, в Єгипті, Алжирі т а Південній Африці.

##### Фізичні напади на людей

Як тактика тероризму, напад на людей із застосуванням смертоносної сили є відносно новим методом, пов'язаним із залізницями, і з'явився відносно недавно. Можливо, він був натхненний пропагандою відсікання голів, яку можна знайти в Інтернеті, але ще можна припустити, що привабливість полягає в легкій доступності великих ножів, сокир та іншої подібної зброї. У Китаї ця тактика була застосована під час нападу в стилі буйства в 2014 році, причому з певним помітним ефектом. У Західній Європі та США, однак, очевидно, що так само, як "камінь б'є ножиці", пістолет поліцейського б'є ніж терориста (прикметно, що зброя СББ використовувалася для нападів із засідки на поліцейських і викрадення їхньої вогнепальної зброї). Очевидно також, що напади в обмеженому просторі дають певну тактичну перевагу суб'єкту загрози. Однією з помітних тенденцій, грубою, але іноді ефективною спробою знизити ефективність будь-якого збройного поліцейського або військового реагування, стало відкрите носіння предметів, призначених для імітації саморобного вибухового пристрою (PBIED). Виявилося, що несправжній саморобний вибуховий пристрій має обмежену захисну цінність від підготовлених пострілів, особливо за умови дотримання належних правил ведення вогню.

#### Приклад 4: Інцидент у Великобританії (2018)

У новорічну ніч самотній нападник здійснив неспровокований і спонтанний напад з ножовими та різаними ранами на двох людей на вокзалі Вікторія в Манчестері. Перед нападом нападник декламував ісламські вірші. На місце події швидко прибув один офіцер поліції, але електрошокер, карабін і засоби фізичного стримування виявилися напрочуд неефективними. Лише за підтримки додаткових офіцерів нападника вдалося втихомирити і заарештувати. У нападника було два ножі, один в руці, інший при собі. Під час інциденту він неодноразово вдарив ножем поліцейського. Навіть коли його заспокоювали, він не підкорявся і продовжував виголошувати просторікування в стилі джихадистів. За повідомленнями, чоловік страждав на психічні розлади.

#### Приклад 5: Французький інцидент (2017)

Рано вранці в неділю в жовтні чоловік, озброєний, як було описано, двома м'ясницькими ножами, один з яких був захований в рукаві, напав і вбив двох молодих жінок поблизу залізничного вокзалу в Марселі. Нападник був негайно затриманий військовослужбовцями, які несли службу на вокзалі, за підтримки ряду таємних поліцейських підрозділів. Пізніше відповідальність за інцидент взяла на себе Ісламська держава (Даєш). Нападник, наркозалежний злочинець дрібного масштабу, не був радикально налаштований в рамках формальної структури осередку.

#### Приклади 6 і 7: німецькі інциденти (2016)

Близько 21:00 18 липня самотній молодий чоловік - афганський біженець, місцевий житель - напав на пасажирів приміської залізниці в Німеччині. Він був озброєний сокирою та ножем. Під час відносно короткого нападу троє людей були серйозно поранені і щонайменше двоє інших отримали менш серйозні травми. Потяг не працював на повну потужність і, отже, не був багатим на мішені середовищем, але це був замкнутий простір. Джерела ЗМІ повідомили про інцидент як про релігійно мотивований через те, що молодик нібито вигукував, а також через те, що він був прихильником Ісламської держави (ДАІШ). Він був застрелений поліцією, коли зійшов з поїзда і напав на озброєних офіцерів.

Рано вранці 10 травня нападник-одинак здійснив неспровокований напад з ножем на приміській залізничній станції на півдні Німеччини. Нападником виявився громадянин Німеччини віком близько двадцяти років. Щонайменше четверо людей отримали поранення, одне з них - смертельне. Як зазначалося в рамках попередніх інцидентів SBB, стверджується, що під час нападу нападник приєднався до джихаду. За допомогою кийків співробітники поліції змогли впоратися з ним без жодного пострілу. Незрозуміло, чому нападник обрав відносно невелику приміську станцію і чому він напав приблизно о 5:00 ранку, напередодні пікового періоду поїздок. Можна припустити, що вибір цілі був ідіосинкратичним. Чоловік не був знайомий з місцевістю, а час нападу може бути пов'язаний з тим, що після прибуття о 1:38 нападник не зміг знайти готель, тому просто повернувся до місця свого прибуття. Проблеми з психічним здоров'ям були визнані важливими з огляду на поведінку чоловіка.

У сукупності ці приклади ілюструють, що вибір цілі може бути ідіосинкратичним за своєю природою. Зокрема, багато зловмисників до скоєння нападу залишаються непоміченими, а будь-яка дивна активність поглинається широким спектром поведінки, що вважається нормальною для залізниці. На континуумі доступності зловмисників іноді приваблювали об'єкти, які в рамках будь-якого формального процесу оцінки загрози можуть вважатися маргінальними. У кожному з розглянутих тут випадків вразливість, притаманна залізничному транспорту, була усунена завдяки швидким і рішучим діям поліції, яка або патрулювала місцевість, або виїжджала на місце події як мобільний ресурс.

##### Саморобні вибухові пристрої **(**СВП**)**

Існують численні приклади нападів з використанням СВП на пасажирів, рухомий склад та інфраструктуру залізниць. Там, де людський капітал є обмеженим або цінним з інших причин, ручні, а іноді й транспортні СВП з таймером, встановлені на транспортних засобах залишаються переважним способом ведення вогню. Якщо ціль вважається важкодоступною або захищеною в інший спосіб, використовується зброя, що стоїть окремо, або саморобні вибухові пристрої, що доставляються ззовні. Якщо підривники мають намір віддати власне життя, незалежно від мотивів, можуть бути використані СВП, що ініціюються командуванням. Пристрої, що ініціюються командою, використовувалися там, де ціль була мобільною. Варіації на визначені теми включають ті, що перелічені нижче:

* Атаки без попередження (імовірно, відсутність попередження має на меті максимізувати втрати)
* Атаки, яким передує точне попередження (ймовірно, для мінімізації жертв, а також як засіб заявити про свою "моральну" позицію, якщо атака піде не за планом)
* Атаки, яким передує попередження, що містить завідомо неправдиву інформацію, щоб максимально дезорганізувати ситуацію та/або створити зону вбивств на передбачуваних маршрутах евакуації та в місцях збору людей і перекласти відповідальність (див. соціально інженерні атаки в прикладі 13).
* Атаки з використанням декількох пристроїв, налаштованих на одночасну роботу або на шаблонну затримку
* Напади із застосуванням різних типів СВП (наприклад, фугасні СВП упереміж із запалювальними, СВП на транспортних засобах і ручні СВП, а також СВП із затримкою в часі, захищені схемами протидії поводженню з ними)

Особливістю нападів на вокзалах є те, що саморобні СВП, встановлені в громадських місцях, часто були помічені (іноді викрадені) ще до того, як вони спрацювали. Ця реальність, схоже, спонукала зловмисників іноді навмисно розміщувати пристрої там, де їх з меншою ймовірністю помітять і швидко повідомлять про них (наприклад, у сміттєвих баках і кабінках туалетів). Протягом 1990-х років у Великій Британії випадки залишення бомб у громадських місцях на вокзалах різко зменшилися завдяки формалізованому режиму перевірки вокзалів, що здійснювався навченим залізничним персоналом, який працював за чітко розробленим планом, а також усуненню місць приховування, особливо сміттєвих баків. Ця ініціатива принесла неочікуваний безпековий бонус з точки зору стримування: прибирання сміття персоналом у яскравому одязі посилило враження, що громадський простір є "своїм". Супутні заходи включали структуровану кампанію з інформування пасажирів про ризики, пріоритетні поліцейські патрулі, приурочені до заходів з безпеки персоналу, та посилене охоплення відеоспостереженням.

#### Приклад 8: СВП низького рівня/низької складності, Лондон (2016)

Вранці у четвер, 20 жовтня, пасажири поїзда Ювілейної лінії помітили невеликий рюкзак, який був залишений на видноті біля подвійних дверей поїзда. Протягом кількох зупинок на нього не звертали уваги, але на станції Canary Wharf пасажир підняв рюкзак і передав його машиністу, який поклав його в кабіну поїзда. Лише під час руху поїзда у машиніста виникли підозри, і, зрештою, він викликав поліцію. Після оцінки, проведеної фахівцями, команда зі знешкодження вибухонебезпечних предметів (ЗВП) знешкодила саморобний, але життєздатний саморобний вибуховий пристрій з таймером, що містив обмежений склад малої вибухової речовини. Підсумовуючи, цей інцидент включає наступні основні моменти:

* Конструкція СВП була примітивною, але передбачала додаткове осколкове ураження.
* Схоже, що час нападу не був обраний у піковий період пасажиропотоку, і потяг не працював на повну потужність.
* Сумка була залишена на видноті, тому інші пасажири бачили, як її власник виходив з поїзда.
* На відміну від більш успішних атак (див. приклади 9-10), використовувався лише один пристрій невеликої маси.
* Предмет не підлягав жодному цілеспрямованому процесу оцінки, доки його не оглянула поліція.

Залишається незрозумілим, чому сумку перемістили, передали водієві, а потім – всупереч інструктажу, задокументованим протоколам і очікуванням - розмістили в кабіні. Це було зроблено, незважаючи на нерівномірний розподіл ваги по відношенню до об'єму сумки і, що викликає більше занепокоєння, видиму присутність проводки, модифікованого електромеханічного настінного годинника, сухої батареї та проводів, що входили в колбу термоса. Потенційно, це був приклад того, що Фройденбург визначив як атрофію пильності, оскільки це сталося в період, коли вибухи поїздів у Лондоні стали рідкісними подіями.31 Використовуючи дані з розгалуженої лондонської мережі відеоспостереження, швидко відбувся арешт молодого чоловіка з аутизмом, чий інтерес до зброї був визначений як помилковий, а не як терористичний, і він був заарештований. Однак були представлені докази того, що злочинець читав онлайн-публікацію сумнівної технічної якості, яку, тим не менш, пов'язували з Аль-Каїдою.

#### Приклад 9: Експансивна атака, Лондон (2005)

Вранці 7 липня четверо молодих людей потягом вирушили зі своїх рідних графств до Лондона. Після прибуття на залізничний вузол (Кінгс-Крос) троє з них сіли на різні потяги метро. Через вісім хвилин після початку подорожі, і лише коли вагони проїжджали через тісний простір відносно неглибокого тунелю, було підірвано перші два саморобні вибухові пристрої. Третій вибух стався на глибині 500 метрів у дуже глибокій ділянці тунелю. За оцінками, ці три вибухи сталися протягом менш ніж однієї хвилини. Четвертий підривник н е встиг сісти на потяг до того, як його спільники привели в дію свої пристрої; йому довелося купити нову батарею для СВП, яку він мав при собі, але, можливо, він був менш цілеспрямованою людиною. Оскільки рух поїздів було призупинено, він сів у автобус і привів у дію свій саморобний вибуховий пристрій невдовзі після початку поїздки. Чотири вибухи сталися протягом однієї години, причому бомби в поїздах тимчасово згрупувалися приблизно о 8:50 ранку, а бомба в автобусі спрацювала о 9:47 ранку. Перші повідомлення спочатку були пов'язані з випадковим відключенням електроенергії – повторюваною і передбачуваною проблемою з електропостачанням -але поліцейські, які перебували в безпосередній близькості, розпізнали ознаки вибуху: характерний шум, підземний струс і пил, що вилітав з тунелів. Було не одразу зрозуміло, скільки поїздів постраждало, оскільки надходили численні повідомлення про одні й ті ж інциденти. Протягом 25 хвилин всі потяги були зупинені на платформах, а незабаром після цього розпочалася повна евакуація - відповідно до добре відпрацьованого плану. На цьому етапі в Інтернеті з'явилися зображення кривавої бійні, зняті камерами телефонів.

Люди, вимушені покинути станції метро, що швидко закривалися, утворили великі натовпи на вулицях. Деякі намагалися продовжити свою подорож на таксі або автобусах, інші чекали на відновлення руху поїздів. Деякий час було незрозуміло, чи готуються інші напади, і надходили численні повідомлення про підозрілу поведінку. Ця невизначеність посилилася, коли здетонував четвертий саморобний вибуховий пристрій, що запізнився. Через швидку евакуацію з потягів метро, численні сумки, залишені без нагляду, потребували перевірки поліцією, що ще більше розтягувало ресурси і спричиняло додаткові збої в роботі. Переважна більшість залишених без нагляду сумок була швидко виявлена за допомогою спеціального залізничного протоколу оцінки, який називається H-O-T. Ця проста евристика, розроблена на початку 1990-х років, має на меті відокремити шум - виявлення залишеної без нагляду сумки в середовищі, де такі випадки трапляються часто, - від сигналу, що в сумці може міститися СВП. Використовуючи евристику H-O-T, навчений залізничний персонал або поліція зосереджуються за трьома аспектами, що мають відому актуальність.33 Чи захована річ? Дуже мало пасажирів, які забувають свої речі, спочатку ховають їх. Чи є предмет очевидно підозрілим за зовнішнім виглядом або за обставинами його виявлення (див. зразок 8)? Чи є предмет типовим для того, що зазвичай знаходять у відповідному середовищі?

Після оперативно-розшукових заходів поліції та швидкої передислокації додаткових офіцерів, елементи підземної мережі почали поетапно відкриватися пізніше того ж дня. Загалом було вбито 52 людини, ще більше людей отримали тяжкі поранення.34 Оскільки місця інцидентів у метро були особливо жахливими і складними, ті елементи мережі, які постраждали безпосередньо, залишалися закритими протягом декількох тижнів. Причиною цього збою були не стільки пошкодження від вибухів, скільки протоколи, які використовувалися для управління місцем злочину.

#### Приклад 10: Експансивна атака, Мадрид (2004)

11 березня терористи встановили 13 саморобних вибухових пристроїв у приміських потягах, що прямували до Мадрида. Бомби, які візуально не відрізнялися від звичайного багажу, були закладені під час очікування поїздів на відносно віддалених приміських станціях. Між 7:35 та 7:40 ранку (примітка: час варіюється залежно в і д джерела) 10 вибухових пристроїв здетонували в чотирьох потягах на лінії приміських поїздів C-2, що прямували з Гвадалахари до станції Аточа. Кожен СВП містився в ручній поклажі. Окрім 10 бомб, що здетонували, сапери знешкодили ще три пристрої, в тому числі один, знайдений серед покинутого багажу через кілька годин після вибуху. Бомби були активовані таймером і мали вибухнути через 30 хвилин. Оскільки в кожному з поїздів їхало приблизно по 700 осіб, вагони були переповнені. Свідки згадують, що бачили, як у потяг заносили сумки, але ніхто з них не вважав ці дії достатньо підозрілими, щоб повідомити про них у поліцію.Перший вибух (з трьох в одному поїзді) стався в приміському поїзді, який вже прибув на станцію Аточа, в результаті чого загинуло 29 о с і б і 176 отримали поранення. Пізніше в поїзді було виявлено четвертий СВП, який сапери знешкодили. Наступні вибухи сталися в іншому приміському поїзді, який відставав від графіка на дві хвилини. Цей потяг рухався до Аточі, коли вибухнули чотири бомби, зупинивши поїзд приблизно за 500 метрів від місця вибуху першої бомби, в результаті чого загинуло 59 людей і ще 200 отримали поранення. Майже одночасно два вибухи сталися в третьому потязі, а ще через деякий час сапери знешкодили ще два саморобні вибухові пристрої. Внаслідок цих вибухів загинуло 67 людей, ще 200 отримали поранення. Трохи далі від Аточі одна бомба вибухнула у вагоні поїзда, в результаті чого 20 людей загинули і 50 отримали поранення. Протягом кількох тижнів після нападу ще 26 людей померли від отриманих поранень. Загалом вибухи забрали понад 200 життів.

Притаманна залізничному транспорту вразливість, пов'язана з громадським транспортом, була очевидною у прикладах Лондона і Мадрида. Терористи проникали в залізничну мережу в місцях, де заходи безпеки були незначними, і використовували поїзди для доставки СВП в більш важливі місця. Той факт, що пасажири в Мадриді спостерігали за тим, як залишали сумки у вагонах, в яких вони їхали, але нічого не робили, свідчить про серйозні недоліки в панівній культурі безпеки (див. приклад 8). На відміну від Лондона, залізничне сполучення з Аточею не було призупинено, а на місці злочину працювали надзвичайно швидко. В Іспанії, здавалося б, надійний підхід до управління ризиками означав, що мінімізація збоїв і прискорення повернення до нормального життя були встановленими політичними та оперативними пріоритетами. Як і в прикладі 9, після нападів були посилені заходи безпеки і присутність поліції, але, на відміну від Лондона, військові сили були невід'ємною частиною гучної поліцейської функції.

##### Швидкодіючі отруйні Небезпека

Швидкодіючі отруйні речовини найтісніше, але не виключно, асоціюються з хімічною зброєю. На сьогоднішній день відносно неефективне і нечасте використання цієї зброї терористами важко пояснити, особливо з огляду на їхні декларовані наміри і продемонстровану готовність здійснювати напади з великою кількістю жертв за допомогою інших засобів. Однак, якщо порівняти це з відомими і доведеними можливостями вибухових речовин, з'являється обґрунтування, засноване на прагматизмі. Основоположний приклад інциденту, що вплинув на залізничний громадський транспорт , стався в Токіо і описаний нижче.

#### Приклад 11: Токійський метрополітен (1995)

Атака 20 березня - це було ресурсномістке злочинне підприємство, пов'язане з виробництвом наближеного до зарину, летючого нервово-паралітичного агента часів Другої світової війни. Коли нападники вручну розпорошили кілька контейнерів у кількох поїздах, що рухалися трьома різними лініями, але кожен з яких проходив через одну вузлову станцію, це призвело до серйозного інциденту масового характеру. Напад розпочався приблизно о 8:00 ранку в будній день. Перші повідомлення про людей у біді в переповнених поїздах не одразу були розцінені як передвісники того, що мало статися; керівництво залізниці спочатку вважало, що причиною має бути нещасний випадок. Незважаючи на зрозумілу невпевненість серед тих, хто реагував, варто зазначити, що місцеві новини повідомили про інцидент о 9:00 ранку, а міжнародні новини підхопили цю історію о 9:12 ранку. Приблизно через 90 хвилин після викиду зарину було оголошено про атаку і запроваджено посилені заходи безпеки. Протягом дня понад 4 000 людей звернулися за медичною допомогою, причому деякі з них принесли із собою зараження в лікарню. Плутанина була настільки великою, що один заражений потяг завершив свій рейс, а потім почав зворотній шлях до місця інциденту.

Відносно низька ефективність нервово-паралітичної речовини в поєднанні з її неефективним вивільненням означала, що очікувана летальність була значно знижена. Пакетики, в яких містилася речовина, проколювали вручну - після чого нападники розбігалися, - а розповсюдження залежало від випаровування летючої рідини, що накопичувалася в пакетику. Сучасні цифри різняться, але здається ймовірним, що переважна кількість жертв, які самі повідомляли про себе, насправді були "добре занепокоєні". На відміну від численних вибухів поїздів у Мадриді та Лондоні, кількість жертв була відносно невеликою, оскільки протягом перших 24 годин померло вісім осіб з 1000, у яких були виявлені клінічні симптоми. Протягом багатьох років багато жертв померли від довготривалих наслідків отруєння. Цей інцидент висвітлив відносну непідготовленість залізниці та служб реагування до роботи з високо летючими, швидкодіючими і нерозпізнаваними хімічними небезпеками, зокрема, до проблем виявлення, ідентифікації та моніторингу. Ці труднощі призвели до того, що багато рятувальників заразилися, не знаючи про це, а заражені евакуйовані не були ні ідентифіковані, ні проконтрольовані. Ці проблеми призвели до значних випадків вторинного зараження серед водіїв таксі, людей на вулицях і персоналу лікарень.

Після нападу в Токіо хімічна міна стала основним предметом занепокоєння КТ. Хімічні атаки, як правило, розглядаються разом з біологічними, радіологічними і, що дещо дивно, ядерними загрозами. Об'єднання цих чотирьох унікальних небезпек в одну абревіатуру - ХБРЯ - маскує дуже різні виклики і відносну правдоподібність, пов'язані з окремими небезпеками, які ця абревіатура намагається охопити. Якби атака на Токіо включала в себе біологічну небезпеку з довшим інкубаційним періодом (вимірюваним днями або тижнями), масштаби подальшої надзвичайної ситуації у сфері охорони здоров'я могли б бути величезними. За винятком джихадистської пропаганди (так званий "Мубтакар" ) , подібні хімічні атаки не відбувалися в США або Європі (хоча деякі бази даних реєструють інциденти, пов'язані з розпиленням подразнюючих аерозолів, під заголовком "хімічна атака", що не дуже корисно). У менших масштабах нервово-паралітичні речовини використовувалися для політичних вбивств, не пов'язаних із залізничним транспортом.

Очевидно, що під час нападу в Токіо організаційна несподіванка була важливим фактором, який не дозволив відреагувати на те, що повідомлялося з численних місць інциденту. Крім того, непостійний характер загрози значною мірою сприяв швидкому поверненню до нормального життя, особливо у порівнянні з тривалою тривалістю дезактивації після зараження будівель сибірською виразкою (біологічною) в США восени 2001 року. Практичні контрзаходи, прийняті на сьогоднішній день, значною мірою зосереджені на забезпеченні того, щоб потенційні жертви

(1) могли розпізнати ознаки і симптоми нападу,

1. визнати негайну необхідність вийти на свіже повітря і зняти всі забруднені предмети одягу (незважаючи на існування проблем, пов'язаних зі скромністю, несприятливою погодою і можливістю невиконання вимог),
2. дочекатися порад фахівців і не діяти як вектор вторинного забруднення.

Усвідомлюючи необхідність прискорення повернення до нормального стану, деякі системи підземного залізничного транспорту регулярно використовують обладнання для моніторингу для визначення екологічних умов у вразливих місцях. Ця діяльність забезпечує базові показники порівняно з критерієм, який є нормальним для даного робочого середовища, і підвищує обізнаність користувачів з обладнанням для виявлення, ідентифікації та моніторингу.

##### Вогнепальна зброя

Масштабні інциденти із застосуванням вогнепальної зброї в поїздах або на вокзалах трапляються рідко. Все частіше джихадисти використовують автоматичну зброю в наступальних діях під час нападів в аеропортах і деяких мародерських атак, але зазвичай не на вокзалах. Деякі суб'єкти загрози мають при собі холодну зброю для особистого захисту, але рідко використовують її як основну зброю для нападу.

#### Приклад 12: Напад на потяг 7alys, Бельгія та Франція (2015)

21 серпня озброєний нападник вийшов з туалету поїзда, що курсував за маршрутом Амстердам - Париж. У нього була штурмова гвинтівка зі складним прикладом (що дозволило йому сховати її в ручній поклажі), кілька запасних магазинів, самозарядний пістолет, ніж і контейнер з легкозаймистою рідиною. Маючи дуже обмежені можливості, але проявляючи неабияку мужність, пасажири поїзда спробували затримати чоловіка. Одна людина отримала ножові поранення, в іншу стріляли з пістолета, але обійшлося без жертв. Нападник не зміг підготувати свою штурмову гвинтівку до надійного пострілу, оскільки не зміг звільнити зупинку. Як наслідок, він був зупинений пасажирами, яких мав намір вбити. Аналізуючи цей інцидент, стає очевидним, що елемент несподіванки і вибір беззбройних людей у переповненому і обмеженому просторі надає стрільцям явну тактичну перевагу. Ця перевага поширюється як на жертв, так і на озброєних людей, особливо якщо неможливо швидко визначити точне місцезнаходження поїзда, що рухається.

Цей інцидент піднімає серйозні питання щодо обґрунтованості офіційних рекомендацій про те, що потенційні жертви не повинні протистояти озброєному нападнику, а повинні тікати і ховатися. Незрозуміло, як пасажири повинні слідувати цій пораді в потязі, що перебуває в експлуатації. Так само, незважаючи на похвальну імпровізацію деяких членів поїзної бригади, така ситуація не була передбачена, і жодних контрзаходів не було вжито. Зокрема, деякі працівники поїзда, схоже, були приголомшені подією і не брали активної участі в її вирішенні.

Можливо, не існує єдиної причини низького рівня застосування вогнепальної зброї проти залізничних цілей, особливо з огляду на її використання в інших умовах, але можна припустити, що непомітні СВП сприймаються як більш ефективні. Все більш ефективні і цілеспрямовані дії краще озброєних і краще підготовлених сил реагування також можуть розглядатися як більш надійний фактор стримування, ніж це було раніше.

##### Соціальний Інжиніринг

У цьому розділі вже згадувалося про соціальну інженерію - тобто, про те, як викликати хибні переконання, змушуючи жертв діяти всупереч власним інтересам, - і наводилися приклади, коли зловмисники використовували фальшиві PBIED, щоб відволікти як жертв, так і тих, хто реагує. Частіше зустрічається використання загрозливих повідомлень, таких як повідомлення про те, що напад неминучий і люди повинні бути евакуйовані. Ця тактика також зустрічається в шахрайських схемах вимагання та лише дуже рідко такі повідомлення надходять від терористів. Навіть коли встановлюється причинно-наслідковий зв'язок, інформація, що міститься в цих повідомленнях, буває різної якості або навіть навмисно оманливою.

#### Приклад 13: Бінарний тероризм ІРА, Сполучене Королівство

Наступний приклад, взятий із сучасного випуску новин, є репрезентативним для реальних повідомлень про замінування. Він ілюструє низку труднощів, які часто виникають одночасно, коли поліція або інші фахівці з управління ризиками намагаються виокремити сенс інформації. Серія схожих, але не ідентичних повідомлень ознаменувала початок кампанії бінарного тероризму, що тривала понад 10 років. За цей час британська поліція отримала 10000 повідомлень про замінування залізниць, але менше 1% з них призвели до подій, які вони, як стверджувалося, передвіщали. Перше повідомлення в рамках нової кампанії - отримане після того, як один вибуховий пристрій вже здетонував - було описано таким чином:

Перед тим, як бомба вибухнула у сміттєвому баку на вокзалі Вікторія під час ранкової години пік, абонент з ірландським акцентом повідомив владі: "Ми - Ірландська республіканська армія. Бомби вибухнуть на всіх головних станціях через 45 хвилин [...]". . . . Після першого вибуху було отримано щонайменше 19 хибних дзвінків, що змусило британську транспортну поліцію почати обшук станцій.

У повідомленнях з погрозами, надісланих рано вранці в будній день, мішенями були названі всі вокзали Лондона, але були атаковані лише два вокзали (і залишається незрозумілим, чому одна детонація сталася до того, як надійшла перша погроза). Кодування повідомлення в такий спосіб могло мати на меті привернути увагу поліції до центральних лондонських вокзалів, не розкриваючи, яких саме - акт, який, можливо, мав на меті максимізувати дезорганізацію, водночас підтримуючи заяву про добрі наміри. Його значення, однак, було витлумачено відповідно до загально прийнятої залізничної термінології, а просторовий дескриптор означав будь-яку станцію на будь-якій залізничній магістралі. Ця двозначність у поєднанні з неточним посиланням на "у Лондоні" суттєво збільшила кількість потенційних місць, що зазнали впливу, з одиниць до кількох сотень.

Також важливим був вплив шуму на процес декодування і розуміння того, що насправді означало повідомлення. Третя особа отримала погрозу до того, як її передали в поліцію - процес, який посилював невпевненість у справжності повідомлення. В іншому інциденті було відзначено, що формулювання погрози про замінування було передано в усній формі від абонента, який зателефонував, до менеджера, чиї слова були записані третьою особою, і лише після цього повідомлення надійшло до поліції. У цьому прикладі - і як це часто буває після реального вибуху - поліція була змушена одночасно реагувати на шум від конкуруючих погроз невідомого походження, які виявилися містифікаціями.

Для суб'єкта загрози цінність цього МО полягає в тому, що він використовує будь-яку схильність до уникнення ризику і, як такий, являє собою мультиплікатор сили. Гостра вразливість особливо помітна там, де плани дій на випадок надзвичайних ситуацій недостатньо розроблені або мають загальний характер, і де принцип обережності є позицією за замовчуванням. Численні приклади загроз вибухів на залізничному транспорті призводили до значних перебоїв у роботі, а іноді й до жертв, що пояснювалися виключно нескоординованістю евакуаційних заходів. Така ситуація може прискорити повторення погроз і призвести до нерегульованого перенесення ризиків. У меншій, але значній кількості випадків інерція у прийнятті рішень призводила до того, що людей переміщували з місця відносної безпеки в місце гострої небезпеки. Цей небажаний результат виникає тоді, коли особи, які приймають рішення, не намагаються відрізнити правдиві повідомлення від містифікацій, тобто оцінити достовірність загрози, про яку йдеться в повідомленні.

##### Змішані методи Атаки

В одному з двох наведених нижче прикладів (Лондон) напад і з застосуванням змішаних типів зброї був передбачений, і в рамках скоординованого плану реагування були виділені відповідні ресурси, зокрема, озброєна поліція. На головному вокзалі, де стався напад, було вжито заходів для обмеження доступу автотранспорту і розроблено міжвідомчий план дій на випадок надзвичайних ситуацій. Найголовніше, що ті, хто прибув на місце події, були краще озброєні, ніж терористи, що мародерствували. В іншому випадку (Мумбаї) напад на МО був несподіваним і був здійснений добре озброєними, добре підготовленими нападниками, які проявляли швидкість і цілеспрямовану агресію. Різні результати очевидні.

#### Приклад 14: Прилегла до лондонського вокзалу Брідж-

***Стейшн (2017)***

Пізно ввечері 3 червня на пішоходів поблизу станції Лондонський міст скоїв наїзд мікроавтобус транзитного типу. Троє чоловіків вийшли з транспортного засобу і попрямували до Боро-маркету, комерційного та житлового району, що прилягає до станції. Вони негайно розпочали серію фізичних нападів, використовуючи довгоклинкову зброю, яка була прикріплена до їхніх зап'ясть клейкою стрічкою. Вогнепальна зброя не застосовувалася, саморобні вибухові пристрої не використовувалися. На поясах чоловіків були помічені об'ємні предмети, які, як припускали, були саморобними вибуховими пристроями, але пізніше з'ясувалося, що це були муляжі. Всі нападники були нейтралізовані озброєною поліцією протягом приблизно 10 хвилин. Під час безчинств було вбито семеро людей і 48 поранено, в тому числі беззбройний патрульний поліцейський залізничної поліції. Станція Лондонський міст не стала об'єктом нападу, але була швидко закрита і евакуйована, а з огляду на її близькість до місця злочину, станція залишалася закритою до наступного тижня.

#### Приклад 15: Центральний вокзал Мумбаї (2008)

Атака 26 листопада включала майже одночасні інциденти, ініційовані високомобільними, високомотивованими, добре підготовленими і добре озброєними суб'єктами загрози. Кілька груп атакували кілька об'єктів за дуже короткий проміжок часу. До таких дій належать: збройні напади із застосуванням ручних гранат, викрадення автомобілів, стрілянина на дорозі, використання саморобних вибухових пристроїв з таймером, цілеспрямовані вбивства озброєних поліцейських та окремих іноземців, невибіркові вбивства, захоплення будівель, а також барикадування та захоплення заручників. До цього розділу відносяться події на вокзалі Чхатрапатіг Шиваджі Термінус (ЧШТ), центральному залізничному вокзалі Мумбаї. Ця станція була передбачувано переповнена людьми і багата на мішені, і невелика кількість нападників діяла протягом приблизно 25 хвилин. Починаючи з пізнього вечора, понад 50 людей було вбито і понад 100 поранено, причому більшість жертв припадає на перші шість хвилин нападу. Втрати в результаті КНТ становлять приблизно третину від усіх жертв, зафіксованих під час цього інциденту. Така велика кількість жертв підкреслює вразливість переповненої людьми станції, де мало місць, де можна негайно сховатися від обстрілу або кінетичних ефектів. Серія атак тривала кілька днів, загалом майже 60 годин, перш ніж нападники були нейтралізовані. Незважаючи на початкові заяви про те, що столицею блукали понад 20 терористів, насправді було 10 активних стрільців, дев'ять з яких були вбиті.

Цей напад був масштабним і новим, якщо порівнювати його з попередніми інцидентами в Мумбаї, які призвели до подібних масштабних людських жертв, але з використанням саморобних вибухових пристроїв (СВП). Швидкість і агресивність нападу приголомшили перших реагуючих на залізничному вокзалі; вони не очікували збройного нападу, не були навчені діяти в ситуації, з якою зіткнулися, і не були озброєні або захищені, щоб протистояти нападникам на рівних умовах. Прикметно, що нападники активно уникали тих, хто міг відповісти тим же , швидко розриваючи контакт, коли стикалися з серйозною протидією. КНТ продемонструвала вже згадану вразливість, про яку ми говорили вище. Високий рівень невизначеності означав, що ті, хто реагував, не могли ані одразу зрозуміти, що відбувається на місці, ані здійснити узгоджену реакцію на це. Затримка з реагуванням була неминучою через велику кількість повідомлень, які поліція мала опрацювати. Під час початкової плутанини на КНТ до місця нападу потрапило ще більше людей, як пішоходів, так і на потягах, що прибували, які неможливо було зупинити. До того часу, як було організовано допомогу, нападники-мародери встигли перейти до наступних цілей.

### Розробка уроків Доступно

Розділ тематичних досліджень ілюструє різноманітні усталені МП, до яких залізниці залишаються вразливими, і до яких терористи тяжіли в минулому. Питання про те, чи будуть вони робити це знову, виходить за рамки цього розділу, за винятком того, що суб'єкти загрози часто повертаються до МВ, вважаючи, що вони працювали на інших, особливо там, де виявлені вразливі місця залишаються неусунутими. Варіації в методології атак, коли вони виникають, стосуються, як правило, масштабу, майстерності або сфери застосування, а не новизни чи оригінальності. Така ситуація є проблематичною, оскільки вразливості, які використовують зловмисники, є невід'ємною частиною того, як залізничні системи були спроектовані для роботи. За винятком нападу в токійському метро, можна виділити наступні теми:

* + Напади на людей найчастіше відбуваються із застосуванням вибухівки, часто з додаванням осколкових боєприпасів. Вогнепальна зброя та інші напади з близької відстані із застосуванням СБЗ вийшли на перший план в останні роки, а рішучі нападники, схоже, свідомо обирають тактику змішування та поєднання мінно-вибухових засобів як цілеспрямовану.
  + Атаки на стаціонарні об'єкти інфраструктури відбувалися переважно з використанням вибухівки, а іноді й легкозаймистих матеріалів. Механічні диверсії були відносно рідкісними.
  + Напади на потяги під час руху включали вибухи у вагонах або на шлях прямування поїзда. У деяких регіонах світу для нападу на тих, хто вижив, застосовували вогнепальну зброю, а інколи і граблі на поїздах, що проїжджали повз.

Слід припустити, що терористи продовжуватимуть використовувати свої сильні сторони і слабкі місця в урядах і установах країн-членів НАТО і країн-партнерів. Якщо не брати до уваги атаки в зонах бойових дій або поблизу них, де можливості і потенціал терористів можуть бути значними, аналіз інцидентів на залізничному транспорті свідчить про те, що події з великою кількістю жертв відбуваються відносно рідко. Це не означає, що прагнення потенційних або вже діючих терористів не є високими, або що можуть мати місце несподівані і тимчасові успіхи. Особливе занепокоєння викликають інциденти, які поєднують в собі вже сформовані способи вчинення терористичних актів, коли вони відбуваються одночасно або поступово, що викликає особливе занепокоєння. Вони є застереженням проти розробки оцінок ризиків, які враховують лише одну конкретну МД (див. приклад 15) без урахування того, як реагувати в ситуаціях, що включають декілька МД. Наявність окремих планів дій на випадок нападів з використанням СБЗ, вогнепальної зброї та СВП дуже відрізняється від реагування на сценарій, в якому вони відбуваються одночасно. Терористи вважають хитромудро розроблені МОД, більшість з яких містять багато обіцянок, не відповідають дійсності і, після ретельної оцінки, часто виявляються неправдоподібними. У зв'язку з цим необхідно бути обережним, щоб не переоцінити масштаби проблеми управління ризиками, коли новизна генерує тепло, а не світло. На ефективність вжитих контрзаходів впливає цілий ряд змінних, і жоден з варіантів не є панацеєю, що зумовлює необхідність комплексного підходу. Як легко помітити, якщо високий рівень безпеки застосовується лише до деяких центральних пунктів, то мало що може перешкодити зловмисникам проникнути в мережу на її периферії і використовувати поїзди для доступу до обраних цілей (див. приклади 9-10). Реалізація цінності будь-яких інвестицій у фізичну безпеку значною мірою залежить від якості концепції операцій та визначених операційних вимог, в рамках яких вони здійснюються.

Розглядаючи колективну сутність наведених тут прикладів, можна навести вагомі аргументи проти цільового посилення, яке призводить до перетворення відкритих залізниць на укріплені цитаделі, навіть якщо така зміна була б можливою без знищення суспільних благ, яких очікують користувачі залізниць і від яких залежить економіка. Замість цього, щоб підтримувати надійну позицію БКЗ перед обличчям невизначеної загрози, простір повинен належати тим, хто в ньому працює і користується ним, включаючи спеціальні засоби безпеки і поліцію.

Див. рекомендації в розділі 6 щодо програм безпеки в аеропортах. Розвиток сильної культури безпеки може обмежити свободу пересування суб'єкта загрози і підвищити ймовірність розпізнавання підозрілої діяльності. Як наслідок, повідомлення про занепокоєння стають більш значущими через контекст, з яким вони чітко пов'язані (див. приклад 1). Крім того, організаційне реагування буде більш згуртованим і стійким, оскільки зацікавлені сторони поділяють приблизно однаковий світогляд і залучені в процес управління ризиками (спостереження, яке також є вагомим аргументом на користь спеціалізованої, а не універсальної охорони правопорядку на залізниці). Масштаб цього завдання не слід недооцінювати. Як підкреслювалося в цьому розділі, невід'ємною частиною процесу розробки контекстно - орієнтованого АПЗ є здатність узгодити мету залізничних операцій з раціональною оцінкою впливу ймовірних загроз. Це завдання вимагає значного внеску з боку тих, хто розуміє, як функціонує залізниця як мережа громадського транспорту, а не лише як абстрактний виклик безпеці.

### Висновок

Використовуючи дані тематичних досліджень, проведених у залізничному середовищі, у цьому розділ і розглянуто низку сучасних дискусій щодо пропорційних, прагматичних та ефективних варіантів управління ризиками, пов'язаними з тероризмом. Ми розглянули природу вразливості, притаманної залізничним операціям, і визначили необхідність чіткого розуміння того, які ризики є релевантними і в якому контексті. Описаний процес вимагає залучення багатьох зацікавлених сторін, деякі з яких можуть дотримуватися різних попередніх зобов'язань. Ця реальність посилює два фактори: (1) вимогу до інклюзивного, послідовного і прозорого процесу оцінки ризиків і (2) переваги розробки доктрини управління ризиками, включаючи шаблони для активного прийняття рішень в умовах невизначеності, заздалегідь узгоджені з відповідними зацікавленими сторонами. Протидія таким різноманітним загрозам, спрямованим проти таких різноманітних цілей, передбачає:

* + Прийняття прагматичного і, наскільки це можливо, прозорого та інклюзивного підходу до стратегічної оцінки ризиків.
  + Забезпечення того, щоб отриманий в результаті СТРА був підготовлений професіоналами, які чітко розуміють, як найкраще досягти основної мети об'єднаних залізничних послуг.
  + Розробка концепції операцій, яка відповідає вразливим місцям та ймовірним загрозам, виявленим у конкретному контексті.
  + Розвиток культури безпеки, в рамках якої всі зацікавлені сторони мають змогу поділяти приблизно однаковий світогляд.
  + Не дозволяти невизначеності сприяти інерції рішень.

Тут не варто недооцінювати ані привабливість залізничних операцій для терористів - особливо багату на мішені природу переповнених поїздів і станцій з інтенсивним пасажиропотоком, - ані проблеми управління ризиками без шкоди для корисності. Всі варіанти потребують застосування в контексті, особливо в тісному середовищі залізничної мережі, оскільки будь-яка ізольована швидка перемога рідко є синонімом постійного фіксованого результату. В рамках домінуючих культурних норм і суспільних очікувань більшість залізниць побудовані як постачальники транспортних послуг за принципом "прийшов і пішов", і ця функціональна реальність не піддається структурним змінам в короткостроковій або навіть середньостроковій перспективі. Як зазначив один високопосадовець у британському Кабінеті Міністрів після вибухів у Лондоні 2005 року, пояснюючи, чому терористи не проходили перевірку документів чи багажу при в'їзді в залізничну мережу, "Ви повинні бути в змозі подорожувати, якщо ваша мета - подорожувати".45 Це твердження означає, що перевірка статусу кожного пасажира при забезпеченні майже восьми мільйонів поїздок щодня була нездійсненним завданням. Ця заява була відвертим визнанням того, що завжди існуватиме динамічна напруга між потребами операторів громадського транспорту, в тому числі практичними обмеженнями, з якими вони стикаються, і тими, хто відповідає за боротьбу з тероризмом. У цьому розділі викладено один з підходів до узгодження таких розбіжностей як засобу більш ефективного управління ризиками і більш надійного підтримання позиції ПВК.

# - 8 -

## Стійкість водного сектору

**і справа "Метрополітен Вашингтон**

Стів Бібер

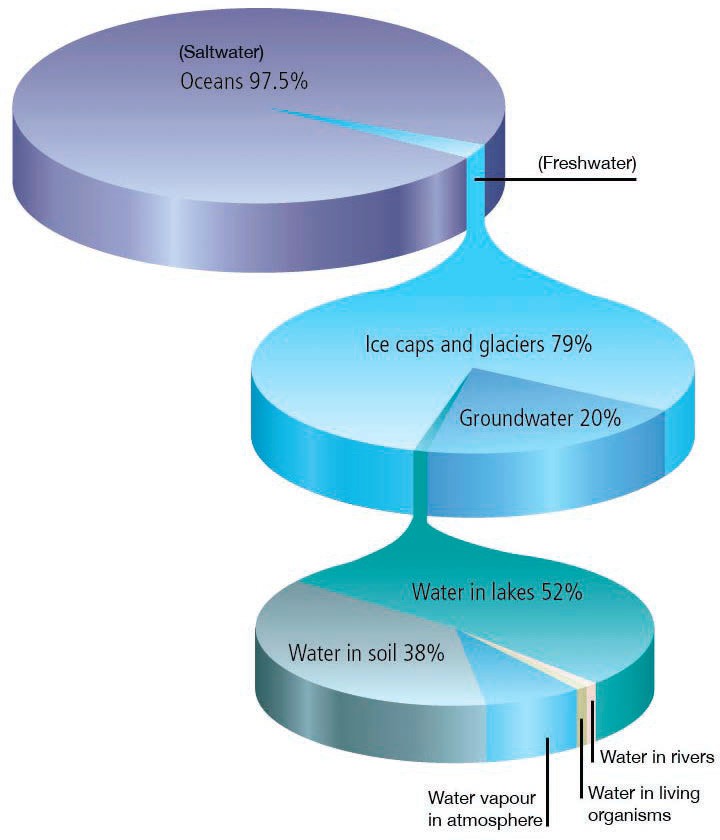
У більшості урбанізованих суспільств вода сприймається як належне, і мало хто замислюється над тим, наскільки крихким може бути постачання цього життєво важливого ресурсу. Однак надзвичайні ситуації з водою, такі як зупинка очисних споруд, забруднення джерела води або стихійне лихо, можуть призвести до значних руйнувань у суспільстві та інфраструктурі, функціонування якої залежить від води. Більшість інших секторів критичної інфраструктури, а також повсякденне життя людей значною мірою залежать від водного сектору. Як наслідок, наслідки надзвичайних ситуацій, пов'язаних з водою, можуть бути значними і проявлятися миттєво, без попередження, в залежності від характеру події. Таким чином, безпека та стійкість водного сектору є ключовим компонентом цивільної готовності країни, що може мати військові та міжнародні наслідки. Терористичні загрози водопостачанню або забруднення джерел води в результаті терористичного акту можуть вплинути на здатність країни перекидати і утримувати свої збройні сили, а також проектувати військову міць, коли це необхідно. З точки зору Організації Північноатлантичного договору (НАТО), загрози водному сектору в одній державі-члені можуть мати хвильові ефекти, які обмежують або зменшують військову мобільність НАТО і проектування сили на підтримку її основних завдань. Тому важливо розуміти ризики у водному секторі і знаходити шляхи їх ефективного пом'якшення. Хоча цей розділ присвячений водному сектору США і використовує тематичне дослідження одного з найважливіших столичних регіонів країни, він є корисною основою для розуміння, адаптації і застосування іншими членами Альянсу і партнерами до своїх конкретних обставин.

З цією метою ця глава включає п'ять основних розділів: (1) огляд водного сектору; (2) визначення ризиків та загроз для водного сектору; (3) основні кроки у плануванні стійкості; (4) ілюстрація викликів та рішень щодо ініціатив з безпеки та стійкості на прикладі Вашингтону, округ Колумбія; та (5) рекомендації щодо розвитку безпеки та стійкості водного сектору.

### Розуміння води Сектор

Вода для пиття, купання, виробництва електроенергії, виробництва та інших цілей є цінним товаром. Як показано на рисунку 8-1, кількість доступної прісної води на Землі становить лише половину одного відсотка всієї води на Землі.1 Якщо говорити про кількість, придатну для пиття, то якби світовий запас прісної води становив 100 літрів, то придатний для пиття запас прісної води становив би лише близько 0,003 літра, або половину чайної ложки. В індустріально розвинених країнах, однак, термін "вода *з-під крана"* часто використовується, коли мова йде про речі, які так само вільно і легко доступні, як і вода. У Сполучених Штатах вода недорога і в достатку, а середня потреба на душу населення становить близько 80-100 галонів на людину в день. Більша частина цієї води використовується для непитних потреб, таких як приготування їжі, купання, змив туалету і прання.

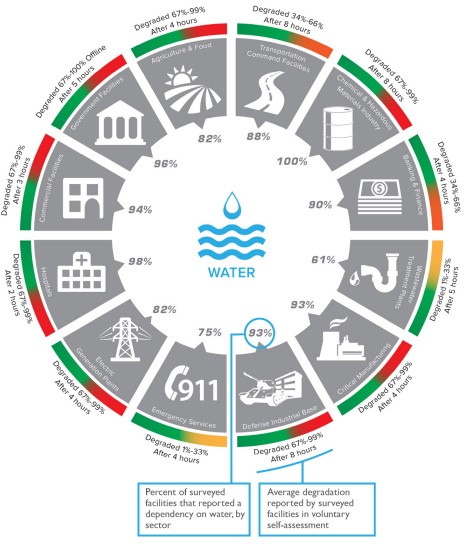
Центри з контролю та профілактики захворювань США визначили доступність чистої, безпечної води та санітарії як одне з десяти найбільших досягнень у сфері охорони здоров'я за останнє сторіччя. Інженери Абель Вольман і Лінн Енслоу в 1919 році визначили правильну формулу обробки громадського водопостачання хлором, і приблизно через 10 років широке впровадження хлорування, фільтрації і поліпшених санітарних систем по суті ліквідувало такі хвороби, що передаються через воду, як черевний тиф, дизентерія, холера, та гепатиту А. Навіть попри ці покращення, хвороби, що передаються через воду, все ще є причиною сотень тисяч смертей щороку через брак чистої води та санітарії. Це суворе нагадування про те, що коли трапляється стихійне лихо, однією з найнагальніших потреб громад є вода для пиття, санітарії, гігієни та пожежогасіння.



**Малюнок 8-1. Земна вода**

(Графік Групи Світового банку)

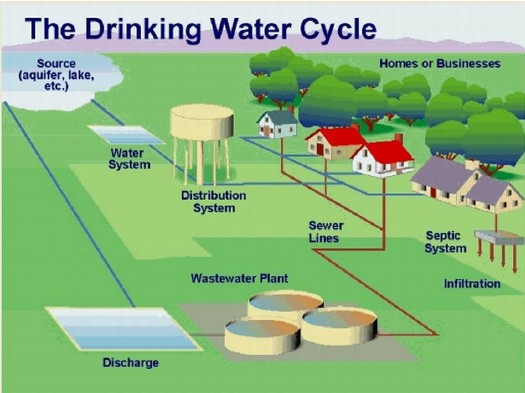
Оскільки всі інші сектори критичної інфраструктури залежать від водного сектору, Міністерство внутрішньої безпеки США (DHS) визначило водне господарство як сектор життєзабезпечення. Взаємозв'язок між секторами життєзабезпечення та іншими секторами критичної інфраструктури описано в розділі 1. Дослідження, опубліковане Національною консультативною радою з питань інфраструктури у 2016 році, містить ключові висновки про важливість водної інфраструктури, особливо про те, як втрата послуг водопостачання може вплинути на інші об'єкти критичної інфраструктури та спричинити різні види порушень. Зокрема, дослідження показує, що "серед опитаних об'єктів критичної інфраструктури, які залежать від води для основної діяльності, послуги погіршуються на 50 і більше відсотків протягом восьми годин" після припинення водопостачання або водовідведення. На Рисунку 8-2 показано взаємозв'язок між втратою води та погіршенням якості послуг у різних секторах.8 Незважаючи на значну залежність від водного сектору, багато власників та операторів об'єктів критичної інфраструктури не мають належних планів щодо альтернативних джерел водопостачання та водовідведення. Більш детальну інформацію про характер залежностей і взаємозалежностей та їх важливість для розробки стратегій управління ризиками див. у розділі 12.



**Рисунок 8-2. Залежність сектору від води**

(Графік розроблений Національною консультативною радою з питань інфраструктури США. Інформація, представлена на графіку, базується на обмеженій вибірці з 2 661 добровільних оцінок об'єктів, проведених у період з січня 2011 року по квітень 2014 року, Звіт про стійкість сектору МНБ США, 2014)

У Сполучених Штатах понад 90 відсотків населення покладаються на одну з близько 153 000 систем громадського водопостачання, які забезпечують чисту воду в домівках і на підприємствах. З цих систем більшість людей (понад 80 відсотків) покладаються на кілька великих або дуже великих водних систем, таких як річки, озера, водосховища або підземні води, які очищуються перед тим, як розподіляються споживачам, для отримання питної води. Решта американського населення користується питною водою з приватних підземних свердловин. Після використання вода потрапляє до системи очищення стічних вод. Приблизно для 75 відсотків американців це означає, що вони користуються громадською системою збору та очищення стічних вод. Більшість з тих, хто користується комунальною системою водовідведення, отримують послуги від однієї з 382 великих і дуже великих систем очищення стічних вод, що обслуговують великі міста з населенням понад 100 000 осіб, або від однієї з приблизно 16 000 менших систем, що обслуговують менш населені міста. Решта 25 відсотків людей покладаються на індивідуальні, локальні або невеликі громадські кластерні (септичні) системи очищення стічних вод. На рис. 8-3 зображено кругообіг води та взаємозв'язок між джерелом, розподілом і очищенням води.



**Малюнок 8-3. Цикл питної води**

(Діаграма, розроблена Розширенням МФСА при Університеті Флориди)

Щоб уявити ці відносини в перспективі на місцевому рівні, понад п'ять мільйонів людей у столичному регіоні Вашингтон обслуговують 18 великих очисних споруд, 13 постачальників питної води та 27 дистриб'юторів. Ці водоканали володіють, експлуатують і обслуговують близько 16000 миль каналізаційних труб, 14500 миль водогонів питної води і понад 114000 пожежних гідрантів. Один з об'єктів, станція поглибленого очищення стічних вод "Блу Плейнс", обслуговує понад два мільйони людей і в середньому обробляє близько 300 мільйонів галонів стічних вод на день.

### Ризики та загрози для водного сектору Сектор

Власники та оператори систем питного водопостачання та водовідведення повинні управляти своїми активами таким чином, щоб ефективно реагувати на профіль ризиків. Пріоритети в управлінні ризиками для кожного підприємства визначаються такими факторами, як місце розташування, розмір, активи та специфічні ризики. Загальні ризики та загрози для водного сектору можна розділити на дві великі категорії. Перша категорія - це навмисні загрози, такі як кібератаки; руйнування (фізичне або через кібератаки) частин системи; забруднення питної води різними хімічними речовинами, токсинами, мікробами або радіоактивними сполуками; забруднення очищеної води в системі розподілу. Друга категорія - природні загрози або ненавмисні події - включає екстремальні погодні умови та зміни клімату; старіння інфраструктури; випадкове забруднення питної води, наприклад, розливи нафти або токсичних матеріалів, переповнення каналізаційних мереж; випадкове забруднення очищеної питної води, наприклад, технологічні збої на очисних спорудах або людський фактор, несправність пристрою запобігання зворотному потоку, втрата тиску, що призводить до витоку забрудненої води.

Концепція навмисного нападу або терористичної загрози на водопостачання не є новою. Невдовзі після нападу на Перл-Харбор у 1941 році директор Федерального бюро розслідувань (ФБР) Дж. Едгар Гувер писав, що "серед комунальних підприємств об'єкти водопостачання є особливо вразливою точкою атаки для іноземного агента через стратегічну позицію, яку вони займають у підтримці обертання коліс промисловості та у збереженні здоров'я і морального духу американського населення".14 У січні 2002 року, невдовзі після терористичних атак 11 вересня, повідомлення з відкритих джерел та попередження від Національного управління ФБР

Центр захисту інфраструктури вказав, що члени Аль-Каїди "шукали інформацію про методи управління водопостачанням і водовідведенням" і "цікавилися інсектицидами і засобами боротьби зі шкідниками", що, можливо, свідчить про їхню зацікавленість у забрудненні водопостачання. Нещодавно глобальний аналіз, проведений у 2018 році дослідниками Міжнародного університету Флориди, показав, що тероризм, пов'язаний з водою, збільшився на 263% з 1970 по 2016 рік, причому 68% цих інцидентів сталися в період після 9/11.16 У Таблиці 8-1 наведено кілька таких нещодавніх атак, більшість з яких - спроби отруїти джерела водопостачання пестицидами, які є у вільному продажу і які відносно легко дістати.

**Таблиця 8-1. Нещодавно задокументовані водні атаки**

|  |  |
| --- | --- |
| **Напади на водні ресурси** | |
| **Рік** | **Опис** |
| 2002 | У Римі заарештовано чотирьох членів салафітської "Групи проповіді і боротьби" за зберігання хімічних речовин, фальшивих документів і детальних планів водопровідної мережі в районі посольства США. |
| 2002 | У Денвері заарештовано двох агентів Аль-Каїди, які планували отруїти водні ресурси. |
| 2004 | ФБР і Міністерство національної безпеки попереджають, що терористи намагаються завербувати працівників водоочисних станцій в рамках проекту з отруєння питної води. |
| 2006 | Резервуар з водою в Трінгу, Англія, навмисно забруднений гербіцидом. |
| 2006 | Стрихнін (пестицид) навмисно випускають у данське штучне озеро. |
| 2007 | 201 людина в Китаї померла після вживання води, яка була навмисно забруднена фторацетамідом (пестицидом). |
| 2008 | У Варні, штат Вірджинія, був заарештований чоловік, який мав при собі два флакони ціаніду і намагався отруїти систему водопостачання. |
| 2008 | Система водопостачання табору бірманських біженців у Таїланді (з населенням 30 000 осіб) навмисно отруєна гербіцидом. |
| 2009 | На Філіппінах угруповання *Frente Moro de Liberación Islámica* отруює джерела води, якими користуються урядові солдати та населення. |

|  |  |
| --- | --- |
| **Атаки на водні ресурси (продовження)** | |
| **Рік** | **Опис** |
| 2010 | Маоїстські повстанці отруїли ставок у регіоні Кашмір, який Центральні резервні сили поліції використовували як джерело питної води. |
| 2010 | В Англії двох неонацистів засудили за кількома пунктами звинувачення в тероризмі, включаючи виготовлення касторки і змову з сербськими нацистами з метою отруєння водних ресурсів, якими користуються мусульмани. |
| 2011 | Документи, вилучені під час рейду з метою вбивства Усами бен Ладена, розкривають плани отруєння водних ресурсів. |
| 2011 | У Кадісі, Іспанія, чиновники запобігли змові з метою отруєння водних ресурсів у відповідь на смерть Усами бін Ладена. |
| 2012 | Два 5000-літрові резервуари з питною водою в Австралії навмисно отруєні діуроном (гербіцидом). |
| 2012 | Сотні дівчаток в афганській школі захворіли після навмисного отруєння системи водопостачання. |
| 2015 | П'ять осіб, пов'язаних з Ісламською державою (Даєш), заарештовані в Косово за підозрою в плануванні отруєння водосховища. Влада Косова перекрила водопостачання десяткам тисяч людей у Приштині, щоб перевірити воду на вміст забруднюючих речовин. |

Малоймовірно, що атака на джерело питної води (наприклад, річку, озеро чи водосховище) буде успішною через великий об'єм води, розведення забруднюючих речовин та їх видалення шляхом водопідготовки. Атака на систему розподілу питної води, однак, має вищу ймовірність заподіяння шкоди. Наприклад, під час однієї з таких атак у 1984 році члени релігійного культу забруднили резервуар водопостачання в місті Даллес, штат Орегон, що призвело до 750 підтверджених випадків зараження сальмонелою. Хоча ймовірність атаки з високими наслідками може бути низькою, терористична загроза для систем водопостачання є реальною.

Як і всі інші сектори, водне господарство стикається зі зростаючою кіберзагрозою для своїх промислових систем управління, бізнес-систем, електронної пошти та інформаційно-технологічної інфраструктури. Широкий спектр суб'єктів загроз, включаючи національні держави, екстремістів і злочинців, користуються перевагами зростаючої залежності від інформаційно-технологічних систем і підключення до них для здійснення атак і досягнення своїх цілей. Огляд різних кіберзагроз та суб'єктів див. у розділах 3-5. У лютому 2021 року кібератака на водоочисну станцію в Олдсмарі, штат Флорида, мала на меті підвищити рівень гідроксиду натрію - хімічної речовини, що використовується для очищення води, і була здійснена саме у водному секторі. Незважаючи на те, що втручання було швидко виявлено, а рівень хімічних речовин повернувся до норми, цей приклад ілюструє, як навіть недосвідчені хакери можуть отримати доступ до програмного забезпечення та систем управління у водному секторі, підключених до Інтернету, наражаючи на небезпеку джерела води та людей.

У категорії ненавмисних загроз столичний регіон Вашингтона, як і інші регіони світу, відчуває на собі вплив зміни клімату. Згідно з Планом дій з питань клімату та енергетики столичного округу Вашингтон до 2030 року, "температура і рівень води в річці Потомак зростають і продовжуватимуть зростати. Екстремальні погодні явища та збільшення кількості екстремально спекотних і холодних днів збільшать ризики для здоров'я, моделей використання енергії, середовищ існування рослин і тварин та інфраструктури".20 Ці зміни вплинуть на системи питного водопостачання та водовідведення, і їм необхідно буде скоригувати стратегії управління, щоб захистити свою інфраструктуру від пошкоджень, продовжуючи при цьому відповідати вимогам щодо кількості та якості води.

У багатьох країнах НАТО значна частина водної інфраструктури була побудована на початку двадцятого століття. Значна частина цієї застарілої інфраструктури вже досягла або незабаром досягне кінця свого терміну експлуатації і потребує заміни або модернізації. У столичному регіоні Вашингтон одним з таких прикладів є компанія WSSC Water, яка обслуговує мешканців штату Меріленд в округах Монтгомері та Принс-Джордж з 1918 року. Понад 40 відсотків з 11 000 миль підземних труб WSSC Water мають вік понад 50 років. Термін експлуатації цих старих труб закінчився, але їх заміна - при середній вартості заміни 1,4 мільйона доларів за милю - є дуже дорогим і довготривалим проектом.21 Заміна застарілої інфраструктури є першочерговим питанням, яке необхідно зважити на інші потенційні загрози.

### Підходи водного сектору до забезпечення стійкості Планування

Існує багато ресурсів та підходів до планування стійкості у водному секторі. У Сполучених Штатах Америки План для водного сектору - додаток до Національного плану захисту інфраструктури, опублікований у 2007, 2010 та 2015 роках Міністерством національної безпеки та охорони навколишнього середовища (DHS) та Міністерством охорони довкілля Агентства з охорони навколишнього середовища (EPA) - розглядає стратегії захисту критично важливої інфраструктури на основі оцінки ризиків для підприємств питного водопостачання та водовідведення. Він описує процеси та заходи, спрямовані на підвищення стійкості сектору та підготовку до запобігання, виявлення, реагування та відновлення після загроз. План ґрунтується на системі управління ризиками, яка встановлює цілі та завдання, визначає інфраструктуру для захисту, оцінює та аналізує ризики для цієї інфраструктури, впроваджує заходи з управління ризиками та вимірює ефективність цих заходів. План також встановлює чотири цілі для водного сектору:

(1) підтримувати захист здоров'я населення та навколишнього середовища;

(2) визнавати та зменшувати ризики;

(3) підтримувати стійку інфраструктуру; та

(4) посилити комунікацію, охоплення та довіру громадськості.

Для кращого розуміння та зменшення ризиків у сфері водопостачання та водовідведення було розроблено кілька керівних документів та стандартів для водного сектору. На веб-сайті Американської асоціації водогосподарських підприємств розміщені деякі найсучасніші стандарти, які можна отримати за невелику плату. Три з цих стандартів, які також можуть бути корисними для членів і партнерів НАТО, наведені нижче:

(1) Стандарт аналізу та управління ризиками для захисту критично важливих активів для управління ризиками та стійкістю систем водопостачання та водовідведення (AWWA J100);

(2) Практика безпеки для експлуатації та управління (AWWA G430);

(3) Практика готовності до надзвичайних ситуацій (AWWA G440).

Крім того, EPA також розробило деякі інструменти оцінки ризиків для підприємств питного водопостачання та водовідведення всіх розмірів, які можуть допомогти визначити найвищі ризики для критично важливих операцій та знайти економічно ефективні рішення для зменшення цих ризиків. Два корисні інструменти, доступні на веб-сайті EPA, - це Інструмент самооцінки вразливості та Інструмент оцінки кліматичної стійкості та обізнаності - додаток для оцінки ризиків для водоканалів.

У Сполученому Королівстві події та ризики, пов'язані з повенями, посухою, екстремальними холодами та зміною клімату протягом останнього десятиліття, поставили під сумнів здатність водопостачальних компаній надійно надавати послуги з водопостачання та водовідведення і, як наслідок, збільшили увагу до питань стійкості. Як наслідок, уряди Англії та Уельсу поклали на Управління з регулювання водних послуг (Ofwat) відповідальність за вирішення питань стійкості у регулюванні водного сектору. Закон "Про воду" 2014 року вимагав вжиття заходів для "просування мети забезпечення стійкості", і Ofwat розробив політичну відповідь, щоб визначити вимоги до водопостачальних компаній щодо підвищення стійкості послуг водопостачання та водовідведення, використовуючи концепцію "кругової стійкості". Ofwat використав цілісну концепцію стійкості - здатність запобігати, справлятися та відновлюватися після різного роду збоїв - яка фокусується на трьох ключових аспектах стійкості організації: корпоративному, фінансовому та операційному.25 Корпоративний вимір - це процеси управління, підзвітності та забезпечення якості в організації, а також її здатність передбачати тенденції та мінливість у своїх бізнес-операціях. Фінансовий аспект розглядає вплив фондів та активів організації, тоді як операційна стійкість фокусується на інфраструктурі організації та здатності і навичках керувати цією інфраструктурою. Нарешті, британська дослідницька організація Water Industry Research опублікувала Посібник з належної практики, який надає водопостачальним компаніям рекомендації щодо планування та окреслює рамки для скринінгу ризиків, оцінки стійкості, планування стійкості та впровадження рішень щодо забезпечення стійкості.26

У цьому розділі представлено короткий огляд компонентів найкращих практик, що містяться в рамочних програмах США та Великої Британії з планування стійкості у водному секторі. У наступному розділі, присвяченому тематичному дослідженню водного сектору Національного столичного регіону (НСР) США, Рада урядів метрополії Вашингтон (COG) адаптувала та використала деякі з цих найкращих практик у своїй оцінці стійкості системи водопостачання. Спочатку COG охарактеризувала систему, що включало опис і розуміння фізичної інфраструктури системи водопостачання в НСР, оцінку її роботи в контексті нещодавніх ризикових подій і визначення підходу до оцінки ризиків.

Наступний крок, скринінг та оцінка ризиків, включав скринінг та оцінку загроз, які становлять ризик для послуг, розгляд того, як критичні активи та системи реагують на ці загрози, оцінку потенційного рівня переривання надання послуг та оцінку потенційних втрат через переривання надання послуг. Потім КГЗ провела детальну оцінку стійкості, щоб оцінити існуючий (базовий) рівень стійкості, визначити та оцінити потенційні ініціативи для підвищення стійкості, а також визначити альтернативи, використовуючи аналіз витрат і вигод протягом усього життєвого циклу. Останній крок, впровадження рішень з підвищення стійкості, спрямований на розробку та реалізацію ініціатив з покращення стійкості, надійності, резервування, реагування та відновлення.

### Випадок столичного регіону Вашингтона Дослідження

##### Передумови та Цілі

Столичний регіон Вашингтон, різноманітний і динамічний регіон зі столицею країни в окрузі Колумбія, оточений округами в передмісті Меріленда і на півночі Вірджинії. Тут проживає понад 5,5 мільйонів людей, а економіка регіону є однією з найбільших в країні, і прогнозується, що до 2045 року тут з'явиться понад мільйон нових мешканців та робочих місць. У такому високоурбанізованому регіоні, як столичний Вашингтон, надзвичайна ситуація з водою може призвести до значних регіональних порушень, оскільки можливості перекидання питної води через річку Потомак або в райони, де може виникнути дефіцит, обмежені через сегментовану природу водопровідних систем регіону. Залежно від сценарію, наслідками такого регіонального відключення води може стати втрата водопостачання від кількох днів до більш ніж місяця, тоді як оціночні прямі та економічні наслідки можуть становити кілька мільярдів доларів.

Починаючи з 2007 року, Уряд України, працюючи з водоканалами по всьому регіону, провів три дослідження щодо резервування систем водопостачання та розподілу води. Основною метою цих досліджень було оцінити здатність регіональної системи водопостачання протистояти надзвичайним ситуаціям та визначити потенційні інженерні вдосконалення для підвищення загальної надійності системи. Останнє з цих досліджень, завершене у 2016 році, є основною темою цього розділу.

У дослідженні 2016 року було використано методологію, засновану на оцінці ризиків, і застосовано найкращі галузеві практики для оцінки потенційних сценаріїв збоїв, їхнього впливу на водопостачання, соціальні та економічні наслідки, а також потенційні ініціативи щодо пом'якшення наслідків. Цей проект, виконаний командою Black & Veatch, провідної компанії в галузі водного інжинірингу, оцінив потенційні вдосконалення для підвищення стійкості регіональних систем водопостачання та оцінив надійність і безпеку питної води від джерела до крану з регіональної точки зору. Працюючи з персоналом Уряду України та іншими учасниками проекту, компанія Black & Veatch запланувала серію семінарів з червня 2015 року по березень 2016 року для водоканалів регіону. Семінари заклали основу для успішного дослідження шляхом (1) встановлення цілей проекту та робочих відносин з ключовими водоканалами; (2) визначення рівня обслуговування, якого необхідно досягти в умовах надзвичайних ситуацій; (3) опис аварійних ситуацій, які можуть призвести до масштабних відключень водопостачання; (4) кількісна оцінка ймовірності виникнення аварійних ситуацій, тривалості відключень та кількості постраждалих споживачів; (5) визначення заходів з покращення інфраструктури для пом'якшення наслідків відключень водопостачання у випадку потенційних аварійних ситуацій; (6) оцінка та визначення пріоритетності заходів з покращення інфраструктури з огляду на рентабельність інвестицій та переваги до регіональної стійкості; і (7) досягнення консенсусу щодо плану вдосконалення, який оптимізує зниження ризиків з урахуванням вартості та рівня надання послуг.

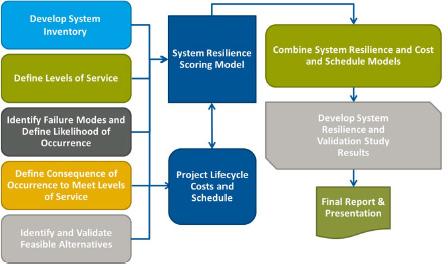
Для забезпечення послідовності та спільного розуміння в дослідженні використовуються такі важливі терміни та визначення:

* *Рівень обслуговування* (LOS): набір цілей, які визначають якість послуг, що надаються
* Вплив *LOS*: недосягнення цілей LOS для певної кількості людей протягом певного часу через сценарій відмови та пов'язані з ним відмови активів
* *Подія*: подія, наприклад, забруднення, пожежа або катастрофічна відмова активу, яка може бути першопричиною і спричинити вплив на рівень втрат.
* *Сценарій відмови*: ланцюжок інцидентів, що виникають через подію, яка створює або посилює вплив LOS
* *Відмова активів*: конкретні активи системи водопостачання, які виходять з ладу в рамках сценарію відмови
* *Прямі витрати*: безпосередній фінансовий вплив сценарію відмови, включаючи витрати на ремонт або заміну обладнання
* *Економічні витрати*: побічні збитки та витрати, не спричинені безпосередньо сценарієм відмови
* *Фінансові витрати*: поєднання прямих та економічних витрат
* *Ініціативи з удосконалення*: капітальні проекти, які можуть зменшити ймовірність або наслідки сценарію відмови

##### Оцінка ризиків та моделювання

Ключовим елементом аналізу стійкості є аналіз ризиків. Огляд міркувань і стратегій оцінки та управління ризиками див. у главі 13. Відповідно до загальноприйнятої практики оцінки ризиків, у цьому дослідженні ризик розраховувався шляхом множення ймовірності настання події на наслідок її настання. На перших семінарах компанія Black & Veatch працювала з водоканалами, щоб визначити різні події, які можуть призвести до тривалої втрати водопостачання, та оцінити ймовірність настання таких подій, а також їхні наслідки. Кількісна оцінка ризику та стійкості для багатьох потенційних ініціатив та портфелів вимагає певного процесу для забезпечення послідовної оцінки досліджуваних альтернатив.

З цією метою на рисунку 8-4 проілюстровано підхід до дослідження на макрорівні, тоді як решта розділу пропонує більш детальний опис кожного кроку цього процесу.



**Рисунок 8-4. Процес дослідження системи водопостачання НКР**

(Діаграма від Black & Veatch)

###### Крок 1: Розробка системи Інвентаризація

Оцінка стійкості регіональної системи вимагала розуміння існуючих окремих систем водопостачання НКР. Перед проведенням оцінки ризиків та моделюванням необхідно було провести інвентаризацію існуючих критично важливих регіональних систем водопостачання в НКР, таких як водоочисні споруди, джерела сирої води, водосховища, насосні станції та ключові взаємозв'язки. Також були отримані прогнози щодо чисельності населення та попиту на воду, а також будь-які наявні попередні дослідження та плани водоканалів, що брали участь у проекті. Система водопостачання регіону ефективно задовольняє потреби НКР за нормальних умов експлуатації. Регіональні угоди та оперативна координація між водоканалами щодо використання неочищеної води річки Потомак, резервної неочищеної води, потужностей очищеної води, готовності до надзвичайних ситуацій та взаємодопомоги ще більше підвищують надійність системи. Прогнози чисельності населення підготовлений COG, оцінює помірне, але тривале зростання до 2040 року в усьому регіоні.28

На основі цих демографічних прогнозів у 2015 році в дослідженні водопостачання у Вашингтоні було оцінено здатність існуючої системи водопостачання NCR задовольнити прогнозований попит до 2040 року. Дослідження дійшло висновку, що за умов, подібних до сильних історичних посух, і за відсутності впливу зміни клімату, "існуюча система водопостачання зазнає значного навантаження, що вимагатиме обов'язкових обмежень водокористування" у столичному регіоні Вашингтона до 2035 року. У регіоні вивчили кілька варіантів покращення зберігання та транспортування сирої води (наприклад, перетворення кар'єрів на позарічкові водосховища), щоб забезпечити додатковий захист від ризиків посухи. Ці варіанти будуть розроблятися і вдосконалюватися в міру того, як ризик посухи і вплив зміни клімату стануть більш зрозумілими.

Що стосується водоочисних потужностей, то регіон має достатню кількість очисних споруд для задоволення максимальних денних потреб до 2040 року. Через сегментовану природу різних систем водопостачання можливості перекачування очищеної води через річку Потомак і в райони, де може виникнути дефіцит, є обмеженими. Наприклад, у разі виходу з ладу водоочисної станції, можливість перекачування води з інших очисних споруд для задоволення попиту в постраждалому районі може бути обмеженою.

###### Крок 2: Визначення рівнів обслуговування (LOS)

Аналіз стійкості на рівні системи вимагає принаймні одного базового показника для оцінки ефективності існуючої системи та порівняння її з майбутніми, альтернативними системами. Для цього дослідження резервування регіональної системи водопостачання базовим показником була здатність споживачів отримувати питну воду в разі виникнення аварійних ситуацій. Зокрема, в процесі семінару було визначено, що здатність задовольняти середні зимові потреби під час надзвичайних ситуацій була визначена як LOS.

Для визначення LOS для кожного водоканалу були розраховані оцінки середнього зимового попиту 2040 року. Цей LOS в принципі узгоджується з регіональними угодами, такими як Розподіл низького стоку річки Потомак Угода про водопостачання та План реагування на посуху в системі річки Потомак міста Вашингтон та План водопостачання та попередження посухи в системі річки Потомак. Ці угоди передбачають розподіл водозаборів пропорційно до середнього зимового виробництва води кожним комунальним підприємством, коли діють обмеження.

###### Крок 3: Визначте несправність Режими

Після визначення LOS був проведений семінар за участю водоканалів для визначення типів основних подій, які можуть вплинути на ці рівні для великої кількості споживачів. Було розглянуто та проаналізовано численні події, включаючи посуху, землетруси, забруднення річок, суховійні вітри, кібератаки, відключення електроенергії та крижані бурі. Терористичні атаки не були виділені як подія, хоча деякі з розглянутих подій (наприклад, кібератаки, забруднення річок та відключення електроенергії) могли бути спричинені тероризмом. Оскільки це дослідження зосереджене на регіональній стійкості, сценарії збоїв, оцінені в ньому, повинні або спричинити відключення води в усьому регіоні більш ніж на 24 години, або вплинути на важливі взаємозв'язки між системами водопостачання, що призведе до відключення води на великих ділянках розподільчої системи більш ніж на 24 години. На основі цих критеріїв дослідницька група відібрала 10 аварійних ситуацій для оцінки, як показано в таблиці 8-2.

Деякі сценарії аварій, включаючи такі події, як регіональне відключення електроенергії, вітрова буря, крижаний шторм, холодні погодні явища та кібератаки, були відсіяні з початкового переліку на основі семінарів та подальших обговорень з відповідними комунальними підприємствами. Зрештою, вибір сценаріїв збоїв для оцінки залежить від багатьох факторів, таких як залучені водоканали, існуючі інвестиції в резервування системи та поточний рівень загроз.

**Таблиця 8-2. Події та сценарії збоїв**

|  |  |
| --- | --- |
| **Подія** | **Сценарії невдач** |
| Прорив водопроводу | Великий прорив водопроводу через річку Потомак |
| Забруднення в річці Потомак | Розлив нафти в річці Потомак - зачіпає обидва береги |
| Розлив нафти в річці Потомак зачіпає західний берег |
| Розлив нафти в річці Потомак зачіпає східний берег |
| Розлив хімікатів у річці Потомак - постраждали обидва береги |
| Вогонь! | Пожежа на водоочисній станції - західний берег річки |
| Пожежа на водоочисній станції - східний берег річки |
| Авіакатастрофа | Падіння літака на водоочисну станцію - західний берег річки |
| Падіння літака на водоочисну станцію - східний берег річки |
| Забруднення водосховища | Забруднення резервуару питної води |

###### Крок 4: Визначення ймовірності виникнення (LOO)

Для проведення аналізу стійкості та ризиків необхідно визначити ймовірність настання обраних аварійних подій. Неможливо з упевненістю передбачити майбутні події, тому один із семінарів був присвячений визначенню обґрунтованих оцінок LOO на основі досвіду водоканалів, що брали участь у дослідженні, та інших підприємств галузі. Для цілей аналізу стійкості найважливішим аспектом є оцінка LOO для різних подій відносно одна одної та розрахунок величини відмінностей. Наприклад, комунальні підприємства, що беруть участь у цьому дослідженні, зазнали розливів нафти в річці Потомак за останні кілька десятиліть, але падіння літака на водоочисну станцію не відбулося і, інтуїтивно, є набагато менш вірогідним. Отже, події забруднення річки Потомак нафтою не були оцінені як такі, що за ймовірністю подібні до падіння літака на очисні споруди.

У цьому дослідженні було визначено п'ять рівнів LOO, які забезпечили достатньо великі інтервали для моделювання стійкості. У цьому дослідженні LOO визначався як такий, що має місце один раз протягом певного періоду, наприклад, один раз на 30 років. У Таблиці 8-3 показано п'ять рівнів LOO, що розглядалися в дослідженні, їх визначення та додатковий опис для розглянутих частот.32

Для використання в підході до моделювання стійкості дослідницька група працювала з COG, щоб пов'язати конкретний рівень LOO з кожним сценарієм відмови, описаним вище. Всі рівні LOO розглядалися окремо для кожного сценарію відмови, але тільки помірний (раз на 30 років) і дуже низький (раз на 250 років) рівні з'явилися для кінцевих частот.

**Таблиця 8-3. П'ять рівнів ймовірності виникнення (LOO)**

|  |  |  |
| --- | --- | --- |
| **Рейтинг** | **Визначення** | **Частота** |
| Дуже високий | Існують прямі докази або суттєві непрямі докази того, що сценарій невдачі розпочався та/або є ймовірність його реалізації. | Один раз на рік |
| Високий | Відомо, що сценарій провалу існує, непрямі докази вказують на його ймовірність, а ключові докази важать більше на користь ймовірності, ніж на користь малоймовірності. | Раз на 10 років |
| Помірний | Відомо, що сценарій провалу існує, непрямі докази вказують на його ймовірність, а ключові докази мають більшу вагу в бік малоймовірного, ніж ймовірного. | Раз на 30 років |
| Низький | Сценарій відмови не може бути виключений, але немає переконливих доказів того, що він стався або що існують умови чи недоліки, які можуть призвести до його розвитку. | Раз на 100 років |
| Дуже низький | Кілька подій повинні відбутися одночасно або послідовно, щоб спровокувати відмову. Більшість, якщо не всі, події дуже малоймовірні. | Раз на 250 років |

###### Крок 5: Визначення наслідків події (COO) для забезпечення рівня обслуговування

Оцінка ризику вимагає поєднання ймовірності виникнення з відповідними наслідками. Для розробки ЦП для різних сценаріїв відмов у цьому дослідженні команда оцінила вплив на систему НКП у порівнянні з середнім рівнем попиту в зимовий період, який був визначений на етапі 2. Для цілей цього дослідження, якщо сценарій аварії призведе до того, що комунальне підприємство не зможе постачати питну воду на рівні середньостатистичного попиту в зимовий день, то споживач вважатиметься таким, що зазнав відключення. Відключення споживачів внаслідок подій, розглянутих у цьому дослідженні, можуть тривати кілька годин або днів, тому в дослідженні кількість споживачів, які зазнали відключення, поєднувалася з очікуваною тривалістю відключення (у днях) для кожного сценарію аварії. Щоб кількісно оцінити ЦВВ, дослідницька група помножила кількість споживачів, що зазнали відключення (населення), на тривалість відключення (у днях). Результат, який називається "дні відключення населення" (POD), був розрахований для кожного зі сценаріїв збоїв у дослідженні.

Щоб забезпечити узгодженість моделювання протягом 100-річного періоду, дослідження спиралося на ключове припущення: воно використовувало прогнозовані потреби у воді та оцінки чисельності населення у 2040 році для кожного з комунальних підприємств незалежно від того, в якому році може відбутися потенційний сценарій відключення. Це припущення дозволило використати загальноприйнятий набір даних про населення для розрахунку впливу відключень протягом модельованого періоду. Важливо відзначити одне спрощення для цього дослідження, яке полягало в оцінці ризиків лише для побутових споживачів. Критично важливим споживачам і об'єктам, а також перебоям, які можуть вплинути на забезпечення виконання місій на військових об'єктах, не присвоювалися більші ваги. Аналіз, який зосереджується на критично важливих клієнтах або забезпеченні місії, може призвести до іншого визначення пріоритетів для вдосконалення.

У дослідженні також було проведено кількісну оцінку ризику за допомогою методології, яка поєднує прямі та непрямі витрати для розрахунку ризику, пов'язаного з кожним сценарієм виходу з ладу. Прямі витрати - це безпосередні фінансові наслідки сценарію відмови (наприклад, витрати на ремонт або заміну обладнання). З точки зору моделювання, прямі витрати не розглядаються ініціативами в дослідженні. Наприклад, існують витрати на ремонт, пов'язані з проривом водогону, але вони не запобігають прориву. Натомість, вони слугують для зменшення кількості СРП після реалізації сценарію аварії. Непрямі (економічні) витрати є супутніми збитками для сценаріїв аварій і не включають прямі витрати. У цьому дослідженні економічні витрати були розраховані шляхом застосування показника витрат на душу населення в день до пов'язаних з ними POD, спричинених сценарієм відмови. У дослідженні було використано оцінку 114,38 доларів США на день як загальний вплив через втрату послуг з питного водопостачання на душу населення.33

###### Крок 6: Визначте та перевірте здійсненні альтернативи

Після визначення сценаріїв аварій та встановлення ймовірності і наслідків їх виникнення, дослідження визначило ініціативи з удосконалення, які спрямовані на зменшення ризиків для системи водопостачання, пов'язаних зі сценаріями аварій. Визначені альтернативи були потенційними контрзаходами, які могли б пом'якшити або запобігти наслідкам сценарію аварії. Альтернативи були відібрані шляхом аналізу сценаріїв аварій та визначення підходів до зниження POD. Обговорення з представниками водоканалів, інженерний досвід та знання системи NCR сприяли розробці відповідних альтернатив. Потім дослідницька група розглянула різні концептуальні альтернативи з комунальними підприємствами-учасниками під час низки зустрічей. Всі потенційні покращення були представлені та розглянуті під час семінару з альтернативних варіантів покращення та під час подальших обговорень з комунальними підприємствами, щоб зосередити увагу та вдосконалити потенційні варіанти покращення для подальшого розгляду.

Для кожного сценарію збоїв дослідницька група розробила модель балансу маси водопостачання на основі електронних таблиць та умов після покращення. Ця модель була використана для оцінки переваг кожного потенційного покращення з точки зору наданої потужності та скорочення дефіциту водопостачання в кожній зоні попиту. Вигода від покращення була розрахована як скорочення POD від умов базового сценарію. Типи покращень, що оцінювалися, включали зберігання води за межами річки, покращення транспортування води, транспортування очищеної води та взаємозв'язок між водоканалами. Для кожного варіанту покращення було розраховано кошторис витрат на капітальні та експлуатаційні витрати, а також витрати на технічне обслуговування. Також були розраховані графіки реалізації з урахуванням типових термінів, необхідних для планування, проектування, отримання дозволів та будівництва для кожного варіанту покращення.

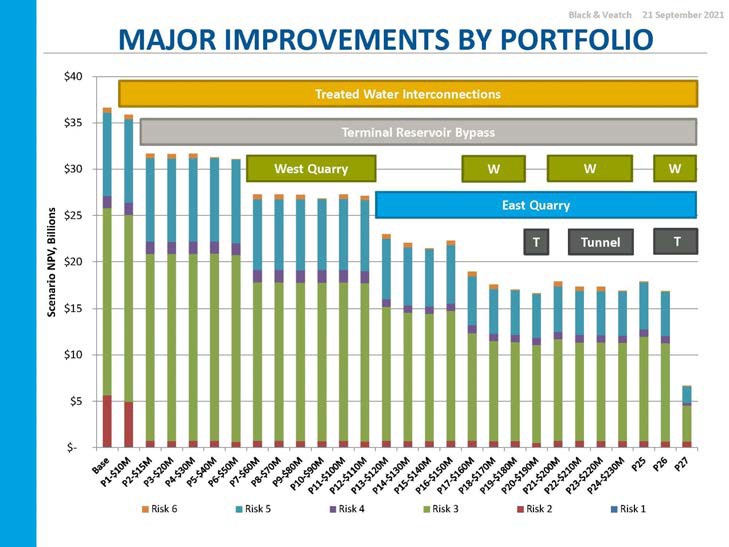
Модель стійкості системи, що використовується в цьому дослідженні, - це модель на основі Microsoft Excel, яка використовує аналіз Монте-Карло для розрахунку ризику сценарію, в якому НКР не впроваджує заходи з підвищення стійкості протягом досліджуваного періоду. Цей сценарій є базовим. Оскільки ризик і потенційний вплив на час простоя були краще зрозумілі і кількісно оцінені, були розроблені потенційні варіанти вдосконалення інфраструктури для зменшення відключень і ризику, пов'язаного з базовим сценарієм. Ці потенційні покращення були розглянуті, відібрані та розроблені за участю відповідних водоканалів. Загалом було розроблено 18 потенційних вдосконалень, які були оцінені на предмет їхньої користі з точки зору зменшення кількості POD для кожного сценарію відмов. Дослідницька група також розробила кошторис витрат на будівництво, експлуатацію та технічне обслуговування, а також графіки впровадження з урахуванням часу, необхідного для планування, проектування та будівництва.

###### Результати

Оцінка базового сценарію дала чисту приведену вартість монетизованого ризику в існуючій системі в розмірі 37 млрд. доларів США протягом 100-річного періоду моделювання. Вартість 37 мільярдів доларів складається з ризику, пов'язаного з 10 аварійними подіями, описаними раніше в Кроці 3 (див. таблицю 8-2): велика аварія водогону (0,11 мільярда доларів), забруднення річки Потомак нафтою (20,1 мільярда доларів), забруднення річки Потомак нафтою на східному березі річки (1,31 мільярда доларів), забруднення річки Потомак хімічними речовинами (9 мільярдів доларів), пожежа на великій водоочисній станції (0,5 мільярда доларів), а також забруднення водосховища (5,56 мільярда доларів). Події, пов'язані із забрудненням річки Потомак, становлять значну частину загального ризику, який несе існуюча система водопостачання Північної Кароліни.

У цьому дослідженні було показано, що зберігання води за межами річки у поєднанні з перекачуванням неочищеної води або вдосконаленням перекачування очищеної води є ефективними ініціативами зі зниження ризиків. Кожне потенційне вдосконалення було індивідуально змодельоване для визначення його переваг протягом 100-річного періоду моделювання. Отримані в результаті співвідношення витрат і вигод були розроблені і використані для ранжування удосконалень. Потім удосконалення були згруповані в портфелі удосконалень для обраних для досягнення максимально можливого співвідношення витрат і вигод. Загалом було визначено та змодельовано 27 індивідуальних портфелів, які охоплюють діапазон капітальних витрат від 1 мільйона доларів США до приблизно 330 мільйонів доларів США, як показано на рисунку 8-5. Як і очікувалося, результати моделювання свідчать про зниження загального ризику зі збільшенням рівня витрат.

Результати моделювання ризиків створюють основу для об'єктивної оцінки потенційних варіантів покращення ситуації з точки зору їх вартості протягом життєвого циклу та переваг стійкості для регіону. Аналіз ризиків показав, що загальний монетизований чистий приведений ризик становить 37 мільярдів доларів США за 100-річний період моделювання, і підкреслив, що забруднення річки Потомак є причиною значної частини загального ризику, який несуть водні системи регіону. Дослідження показало, що цілеспрямоване зберігання неочищеної води в поєднанні з перекачуванням неочищеної води та покращенням перекачування очищеної води, які зазвичай вважаються типом покращень "без жалю", є найефективнішими ініціативами зі зниження ризиків, тоді як забезпечення більшого обсягу зберігання неочищеної води є найкращим довгостроковим покращенням.



**Рисунок 8-5. Основні покращення за портфелями**

(Джерело: Black & Veatch)

Хоча тематичне дослідження системи водопостачання в Північно-Канадському регіоні є унікальним для столичного регіону Вашингтона, воно забезпечує основу і процес аналізу ризиків і стійкості, які члени і партнери НАТО можуть адаптувати і використовувати для проведення подібних досліджень своїх систем водопостачання. У заключному розділі надаються рекомендації щодо того, як члени і партнери Альянсу і партнерів можуть посилити безпеку і стійкість місцевої і національної інфраструктури водопостачання.

### Рекомендації та дії для розгляду

Вода відіграє важливу роль у житті цивільного населення країни і в здатності її збройних сил проводити повний спектр військових операцій від мирного часу до конфлікту. Повсякденні зручності (такі як прийняття душу, приготування кави, чищення зубів, годування сім'ї, відвідування туалету і прання білизни) часто сприймаються як належне, але вони залежать від води. Інфраструктура, необхідна для очищення і транспортування питної води і стічних вод, значна частина якої знаходиться під землею і поза полем зору, має важливе значення для роботи підприємств і підтримки інших важливих секторів інфраструктури, включаючи військові об'єкти і місії. Коли водопостачання суттєво порушується на кілька годин або довше, лікарні можуть закриватися, готелі і ресторани припиняти роботу, заводи зупинятися, а військові об'єкти і прилеглі громади страждатимуть від перебоїв у водопостачанні. Вода є життєво важливим ресурсом для громад у всьому світі, і, як обговорюється в цьому розділі, важливо вживати заходів для захисту водної інфраструктури від таких загроз, як тероризм, кібератаки, зміна клімату тощо. З цією метою члени і партнери НАТО можуть здійснити чотири життєво важливі кроки для того, щоб зробити свою водну інфраструктуру більш безпечною і стійкою.

По-перше, вони можуть налагодити регіональну співпрацю та координацію з надійними партнерами для планування водопостачання та водовідведення. Скоординоване регіональне планування має багато переваг, включаючи можливість розподіляти вигоди, ризики та витрати на ресурси. Довірчі відносини також можуть стати основою мережі взаємодопомоги, що допоможе водоканалам реагувати на надзвичайні ситуації та відновлюватися після них.35

По-друге, вони можуть провести оцінку стану водної інфраструктури, використовуючи підхід, заснований на оцінці ризиків. Цей підхід дозволяє комунальним підприємствам проводити інвентаризацію активів, виявляти активи з високим рівнем ризику та визначати, які активи матимуть найбільші наслідки виходу з ладу з точки зору критично важливих споживачів, кількості постраждалих споживачів та інших факторів. В умовах бюджетних обмежень цей крок може бути відносно недорогим підходом, який у майбутньому можна поступово розширити до повноцінної програми управління активами.36

По-третє, вони можуть використовувати ризик-орієнтований підхід, щоб збалансувати зниження ризиків та витрати. Кожне водоканал або власник чи оператор інфраструктури, що залежить від води, має унікальний профіль ризику. Оцінюючи альтернативи зниження ризиків, важливо кількісно оцінити рівень обслуговування, необхідний у надзвичайних ситуаціях, ймовірність відмови та наслідки відмови, а також шукати синергію між альтернативами зниження ризиків.

По-четверте, вони можуть планувати з урахуванням довгострокового бачення. Капітальна модернізація інфраструктури водопостачання коштує дорого, іноді в межах сотень мільйонів доларів. Після завершення будівництва типовий термін експлуатації може становити 50 років і більше. Отже, інвестиції в заходи з підвищення стійкості, що здійснюються зараз, повинні передбачати майбутні умови - зокрема, зростання населення, попиту на воду і загрози, пов'язані зі зміною клімату або екстремальними погодними умовами, - щоб отримати очікувані вигоди і повернути інвестиції.

Посилення безпеки і стійкості водної інфраструктури серед членів і партнерів НАТО є величезним викликом. Як ілюструє тематичне дослідження, застосування підходу до планування стійкості, заснованого на оцінці ризиків, може забезпечити міцну основу для встановлення пріоритетів і визначення часу і обсягів фінансування інвестицій в інфраструктуру задля посилення здатності організації або регіону адаптуватись і реагувати на потреби у воді під час надзвичайних ситуацій.

# - 9 -

## Стійкість комунікацій

Кріс Андерсон

Комунікації формують критично важливу основу сучасного світу, об'єднуючи більше людей і більше пристроїв, ніж будь-коли раніше. Переваги цього гіперзв'язного суспільства зумовлюють дедалі більшу залежність від безпечних, надійних і стійких комунікацій. Потенційні супротивники Організації Північноатлантичного договору, безумовно, розуміють важливість комунікацій - тих, проти яких вони прагнуть напасти, і тих, якими вони самі користуються, - тому дуже важливо повністю розуміти цей сектор, ризики, що постають перед ним, і найкращі способи пом'якшення цих ризиків. У цьому розділі ці життєво важливі питання розглядаються в чотирьох розділах:

* + Огляд комунікаційного сектору
  + Загрози комунікаціям: обговорення способів, за допомогою яких цілісність, доступність або конфіденційність комунікаційних систем можуть бути порушені або скомпрометовані
  + Тематичні дослідження: ключові спостереження та уроки, винесені з кількох нещодавніх прикладів інцидентів - природних і техногенних, кібернетичних і кінетичних, - які були спрямовані на системи зв'язку та пов'язану з ними інфраструктуру.
  + Рекомендації: пропозиції щодо підвищення стійкості комунікацій до терористичних атак та інших загроз

### Сектор комунікацій Огляд

Цей огляд забезпечує основу для кращого розуміння важливості комунікацій для національної безпеки та готовності до надзвичайних ситуацій, поточного стану сектору та майбутніх тенденцій, а також загальних важливих характеристик сектору та їхнього впливу на безпеку і стійкість.

##### Критично важливий для національної безпеки та готовності до надзвичайних ситуацій

Стійкий і надійний зв'язок має фундаментальне значення для національної безпеки та готовності до надзвичайних ситуацій. Комунікації, в тому числі публічні комерційні мережі, відіграють у цьому критично важливу роль:

* + Національне командування і управління, військові операції, розподіл розвідданих і оповіщення
  + Цивільна оборона, правоохоронні органи та координація дій служб швидкого реагування
  + Готовність та стійкість громадян під час кризи

Життєво важлива комунікація між центральним урядом і військовими, в тому числі секретна і несекретна інформація, передається комерційними каналами зв'язку. Хоча військові комунікації тактичного рівня, як і раніше, використовують повністю некомерційні засоби зв'язку, такі як канали передачі даних на полі бою і тактичні радіостанції, більшість іншого федерального і військового трафіку, в тому числі національні мережі командування і управління, збір і обробка розвідувальних даних, аналіз великих обсягів даних, автоматизація і мультимедійний голосовий і відеозв'язок, вимагають високої пропускної здатності і низької затримки, які часто найкраще задовольняються за допомогою комерційних провайдерів. У багатьох випадках цей життєво важливий урядовий трафік проходить поряд або навіть змішується з цивільним трафіком через ті ж самі комерційні оптоволоконні лінії і центри обробки даних, які підтримують цивільний зв'язок.

На місцевому рівні цивільна оборона, правоохоронні органи та інші служби швидкого реагування також використовують комбінацію самокерованих систем зв'язку і комерційних мереж для підтримки оперативної координації. Традиційні засоби зв'язку перших реагуючих еволюціонували від базових двосторонніх наземних мобільних радіостанцій до широкого спектру радіочастотних і волоконно-оптичних засобів голосового зв'язку і передачі даних. Навіть ці наземні мобільні радіосистеми зараз є високоінтегрованими системами, які включають комірчасті мережі і використовують волоконно-оптичні і супутникові технології для передачі даних і зв'язку з іншими мережами і системами передачі даних.

Сполучені Штати розгортають і вдосконалюють FirstNet, Національну широкосмугову мережу громадської безпеки, яка має стати високошвидкісною загальнонаціональною бездротовою широкосмуговою мережею, призначеною для надання послуг з передачі голосу, відео і даних для підтримки громадської безпеки. FirstNet має стати надійною, високозахищеною і сумісною комунікаційною мережею для органів громадської безпеки і служб швидкого реагування, що дозволить їм швидко отримувати більше інформації і допоможе їм приймати більш швидкі і якісні рішення. Комерційні оператори пропонують подібні послуги "рівня громадської безпеки" поліції, пожежним, рятувальним службам і службам реагування по всій території США і багатьох країн-членів НАТО. Оскільки вимоги до місій швидкого реагування дедалі більше включають дані з відеокамер, автономних транспортних засобів і датчиків Інтернету речей (IoT), потреби в пропускній здатності і затримці для служб реагування, швидше за все, і надалі зумовлюватимуть попит на дедалі потужніші і складніші мережі для їх підтримки.

Комунікації також мають важливе значення для індивідуальної готовності громадян. Під час надзвичайних ситуацій громадяни повинні отримувати своєчасні та точні новини, а також інструкції від посадових осіб щодо заходів, яких вони повинні вжити, таких як евакуація, укриття на місці та повідомлення "будьте напоготові...". Основним засобом отримання громадянами такої інформації є радіо і телебачення (ТБ). Радіо і телебачення корисні своєю простотою, забезпечуючи канал зв'язку "один до багатьох". Відносно низькі енергетичні вимоги до радіо роблять його чудовим засобом для виживання, навіть автономного, спілкування з масовою аудиторією.

Стільниковий зв'язок витіснив стаціонарну телефонію на більшості ринків, але обидва ці види зв'язку є важливими інструментами для громадян, щоб перевірити, як справи у членів сім'ї, і звернутися по допомогу в разі потреби. Навіть коли стаціонарний телефонний зв'язок занепав, високошвидкісний зв'язок для дому стрімко зростає, надаючи споживачам по всьому світу доступ до безлічі контенту на вимогу, в тому числі до величезної кількості інформації про громадську безпеку.

У системах оповіщення про надзвичайні ситуації використовуються як радіо-, так і стільниковий зв'язок, що забезпечує надійні, стійкі канали зв'язку для передачі критично важливої інформації про надзвичайні ситуації для громадян. У Сполучених Штатах система бездротового оповіщення про надзвичайні ситуації використовує мобільний зв'язок для передачі інформації про надзвичайні ситуації, а система екстреного оповіщення забезпечує оповіщення за допомогою радіо і телевізійного мовлення. Починаючи з червня 2022 року, стаття 110 Європейського кодексу електронних комунікацій зробить обов'язковим для всіх країн-членів Європейського союзу розгортання

система оповіщення населення за допомогою телефонних мереж для оповіщення всіх, хто знаходиться в певній місцевості, про кризу, що триває, або катастрофу, що насувається.1

##### Спільний сектор Характеристики

Сучасні мережі зв'язку - це дуже сітчасті, надзвичайно стійкі багатомодові мережі. Збої в роботі обладнання або пошкодження волоконно-оптичних кабелів, як правило, легко перенаправляються з мінімальним впливом на кінцевих користувачів або взагалі не впливають на них. Найслабшою ланкою в мережі зв'язку часто є "остання миля" до конкретного споживача або підприємства. Цей останній відрізок, незалежно від того, чи забезпечується він мідними лініями, оптоволоконним кабелем або через ефір, часто є одноканальним з'єднанням, особливо в сільських і менш густонаселених регіонах, і тому не забезпечує стійкість через резервування, як у більш щільному середовищі або спеціально розроблених стійких комунікаційних архітектур.

Останні кілька десятиліть спостерігається відхід від більшості аналогових засобів зв'язку на користь пакетних комунікаційних технологій. Сьогодні більшість комунікацій, навіть проста голосова телефонія, оцифровується, пакується і передається цифровими мережами передачі даних. Цей перехід відбувся у дротовому голосовому зв'язку, коли на початку 2000-х років телефони з передачею голосу через Інтернет-протокол (VoIP) стали звичним явищем. У мобільному просторі стільниковий зв'язок 3G забезпечив початкове розширення можливостей передачі даних на мобільні пристрої, а перехід на VoIP для основних голосових дзвінків відбувся разом з переходом на 4G. Перехід на цифрове мовлення також здійснив революцію в телерадіомовленні. Стандарти HD-радіо дозволяють чотирьом радіостанціям спільно використовувати один радіоканал, забезпечуючи при цьому кристально чистий звук, а цифрове телебачення уможливило трансляцію сигналів високої чіткості в ефірі. Телевізійний стандарт наступного покоління, Advanced Television Systems Committee 3.0, дозволить передавати дані через Інтернет, що дасть змогу надавати розширене оповіщення про надзвичайні ситуації, яке включатиме карти, графіку, гіперпосилання та інші дані для кращого інформування про надзвичайні ситуації і спрямовувати конкретні заходи реагування на них на рівні громади.

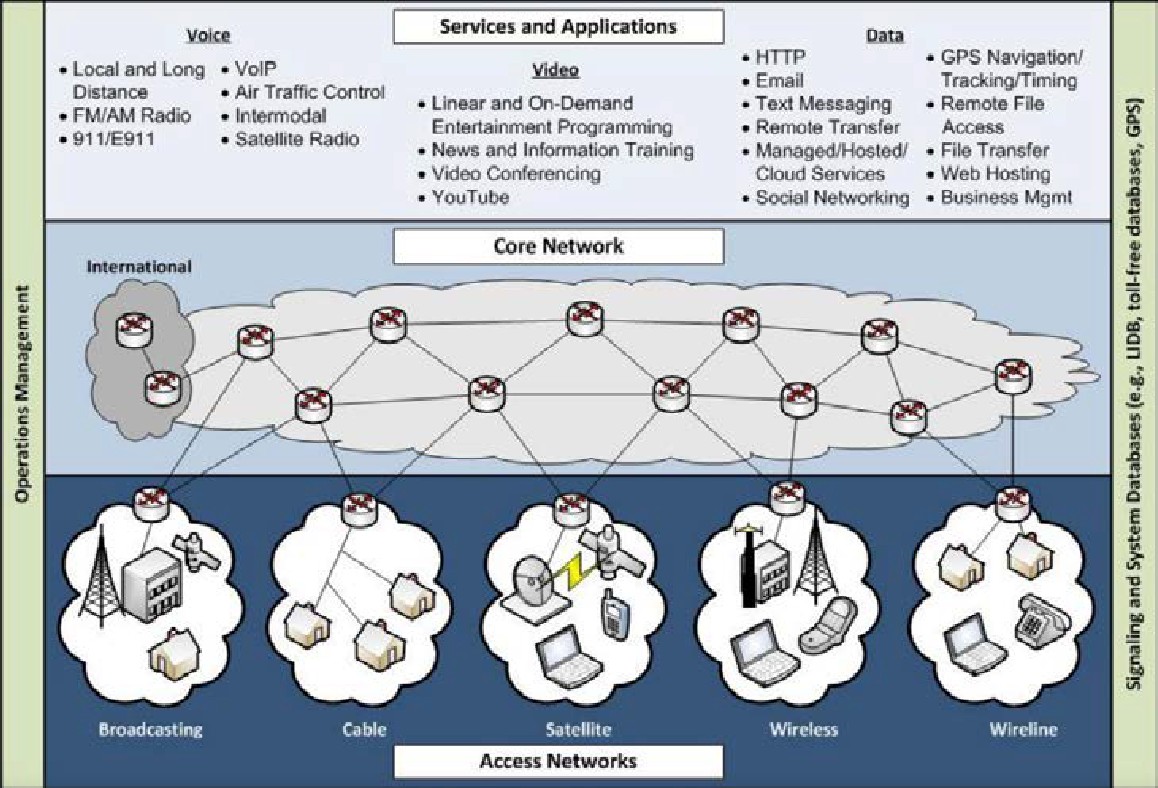
У більшості країн широкий спектр галузевих сегментів і кілька сильних компаній означають висококонкурентний ринок зв'язку, на якому швидкі інновації використовуються для отримання конкурентних переваг. У той же час, мережеві провайдери часто взаємно залежні від інфраструктури один одного в місцях розміщення, для транзитного зв'язку і навіть для зв'язку з клієнтами на останній милі, тому координація між провайдерами є регулярною і повсякденною справою.

Як сектор життєзабезпечення, комунікаційні мережі тісно інтегровані з іншими секторами критичної інфраструктури, причому багато секторів мають значну залежність від комунікацій. Огляд секторів життєзабезпечення та їхнього зв'язку з іншими секторами критичної інфраструктури див. у розділі 1. Водночас, сектор зв'язку сильно залежить від електроенергії, особливо від надійного комерційного електропостачання. Під час катастроф і перебоїв в електромережі або в місцях, де немає надійного електропостачання, системи зв'язку покладаються на місцеву генерацію, що робить доступ до палива (бензину, дизельного палива, а іноді і пропану) для генераторів життєво важливим для забезпечення стійкості комунікацій. Така локальна генерація робить безпеку генераторів і паливних баків вкрай важливою, а доступ до віддалених об'єктів для заправки і ремонту генераторів - першочерговим завданням.

Галузь зв'язку також тісно інтегрована з сектором інформаційних технологій (ІТ), який забезпечує апаратне та програмне забезпечення, необхідне для роботи сучасних комунікаційних мереж. Провайдери зв'язку, ІТ-компанії і навіть виробники контенту співпрацюють і конкурують між собою, пропонуючи масивні можливості обробки даних через хмарні сервіси, периферійні обчислення і мережі доставки контенту. Провайдери тісно співпрацюють з постачальниками обладнання та програмного забезпечення для управління безпекою та стійкістю ланцюгів поставок.

##### Галузь зв'язку Сегменти

У широкому контексті сектору зв'язку окремі сегменти або підгалузі комунікацій мають унікальні елементи, але водночас мають спільні характеристики, описані вище. У багатьох випадках компанії приватного сектору зосереджуються на конкретному підсекторі, хоча конвергенція комунікацій означає, що підсектори часто інтегруються в ширші багатосегментні системи. Малюнок 9-1 ілюструє сектор зв'язку та роль, яку відіграють різні сегменти галузі в цій архітектурі.2



**Рисунок 9-1. Модель архітектури сектору зв'язку**

(Діаграма Міністерства внутрішньої безпеки США)

Сегмент дротового зв'язку складається з мереж з комутацією каналів і пакетною комутацією на основі мідних, оптоволоконних і коаксіальних транспортних засобів. Сегмент дротового зв'язку включає мережі передачі даних і телефонії приватних підприємств, основну магістраль Інтернету (включаючи підводні кабельні мережі) та телефонну мережу загального користування з комутацією каналів зв'язку. Магістральні мережі дротового зв'язку в основному завершили перехід до опорних мереж на основі оптоволокна з комутацією пакетів, використовуючи для зв'язку "останньої милі" поєднання оптоволокна, коаксіального кабелю і витої пари. Ця сучасна волоконно-оптична інфраструктура має важливе значення для підтримки дуже високої пропускної здатності, необхідної для передачі голосу, відео і даних, які вимагають державні, корпоративні та приватні клієнти.

Мережі стільникового зв'язку бездротового сегменту зазнали значної еволюції завдяки появі мереж 2G, 3G, 4G, а тепер і впровадженню мереж 5G. Як і в сегменті дротового зв'язку, більшість послуг стільникового зв'язку, навіть базових голосових послуг, тепер є пакетним трафіком Інтернет-протоколу. Мережі 4G революціонізували те, як стільникові мережі надають послуги передачі даних індивідуальним клієнтам. Мережі 5G покращать цей зв'язок і, що, можливо, ще важливіше, розширять його, включивши в нього очікуване масове поширення пристроїв Інтернету речей. Окрім стільникового зв'язку, бездротовий сегмент також включає в себе бездротові точки доступу, послуги персонального зв'язку, мікрохвильовий зв'язок "точка-точка", високочастотне радіо, неліцензійний бездротовий зв'язок та інші комерційні та приватні радіослужби.

Супутниковий сегмент також зазнає трансформаційних змін. Традиційний супутниковий ринок залишається важливим, оскільки великі дорогі платформи надають надійний набір послуг з передачі даних, голосу, відео і зондування, але поєднання дешевших ракет-носіїв і дуже мініатюрних платформ (іноді відомих як "CubeSat") призвело до сплеску інновацій в технологіях і додатках малих супутникових мереж. Космічні послуги з визначення місцезнаходження, навігації і часу (PNT) від американської Глобальної системи позиціонування (GPS) і європейського сузір'я "Галілео", а також російської системи ГЛОНАСТ і китайської BeiDou стали тісно інтегровані в широкий спектр операцій в критично важливих секторах інфраструктури.

Сучасна кабельна індустрія надає набагато більше, ніж просто телебачення, пропонуючи високошвидкісний широкосмуговий доступ і цифрову телефонію через гібридні оптоволоконно-коаксіальні мережі. На додаток до споживчих послуг, кабельні провайдери можуть також надавати корпоративні мережі передачі даних і транзитні послуги для операторів стільникового зв'язку.

Сегмент телерадіомовлення включає в себе безкоштовні та передплатні ефірні радіо- та телевізійні станції, які пропонують аналогові та цифрові аудіовізуальні програми та послуги передачі даних. Перехід від аналогових до цифрових послуг на телебаченні та радіо дозволяє передавати більше даних, використовуючи менше спектру, що потенційно вивільняє спектр для інших цілей. Одним з таких прикладів є зусилля США, спрямовані на "перепакування" надвисокочастотних телевізійних станцій у менший діапазон частот, щоб перерозподілити спектр для інших цілей. Радіо- і телевізійні станції також транслюють потокове мовлення і додатковий програмний контент через Інтернет. З точки зору готовності до надзвичайних ситуацій слід зазначити, що традиційне радіомовлення є, мабуть, найбільш стійким засобом комунікації з великими групами населення під час надзвичайних ситуацій, оскільки радіостанції недорогі і не потребують великої потужності, а також тому, що місця розташування передавачів мають відносно великі зони мовлення за умови достатньої потужності передавача.

### Загрози для комунікацій

##### Стихійні лиха

Стихійні лиха можуть серйозно порушити або зруйнувати комунікаційні мережі або через пряме пошкодження об'єктів, веж і кабелів, або через порушення можливості постачання електроенергії. У Сполучених Штатах урагани і пов'язані з ними погодні явища спричиняють значний місцевий, а іноді і регіональний вплив на системи зв'язку, оскільки сильний вітер може пошкодити повітряні кабелі та лінії електропередач, а вітер, ліс і штормові хвилі від найпотужніших штормів руйнують основну мережеву інфраструктуру. У деяких регіонах землетруси загрожують системам зв'язку через пошкодження фізичних об'єктів або руйнування кабелів під землею, вздовж мостів та інших смуг відводу, а також потенційно впливають на підводні кабелі та наземні станції. Незалежно від типу катастрофи і ступеня початкового пошкодження, мережі зв'язку можуть продовжувати деградувати і в наступні дні після катастрофи, оскільки операції з розчищення завалів часто призводять до подальшого пошкодження повітряних і підземних волоконно-оптичних ліній, а неможливість доступу до об'єктів (через фізичні перешкоди або комендантську годину) обмежує можливість заправляти генератори на місці і обслуговувати основне обладнання об'єкта. Космічна погода також може значно погіршити роботу систем зв'язку. Під час інтенсивної космічної погоди чутлива електроніка з більшою ймовірністю може бути пошкоджена зарядженими частинками. Іони, що потрапляють на супутники, можуть виводити з ладу датчики, пошкоджувати сонячні батареї, погіршувати роботу електропроводки та іншого обладнання. Крім того, сильні геомагнітні бурі можуть порушити радіочастотні сигнали, такі як GPS, супутникове телебачення, високочастотне радіо і навіть частоти AM-мовлення. На екстремальних рівнях космічна погода може викликати протікання струму через довгі металеві об'єкти, включаючи залізничні системи, трубопроводи і мідні кабелі.

##### Фізичні атаки

Як і будь-яка інша критична інфраструктура, об'єкти зв'язку та кабельні канали є вразливими до фізичних атак. Віддалені об'єкти інфраструктури, такі як вежі зв'язку, гірські ретрансляційні станції та волоконно-оптичні лінії далекого радіусу дії, важко захистити. Більші об'єкти, такі як центральні офіси та інші об'єкти розміщення операторів зв'язку, як правило, краще захищені фізичними заходами, відеоспостереженням, резервними системами та іншими заходами стійкості, але все одно можуть зазнати значних наслідків у разі пошкодження або руйнування. Супутникові шлюзи і наземні станції також можуть бути вразливими до атак.

Радіочастотні системи зв'язку - в тому числі мережі стільникового зв'язку, космічні служби PNT, супутниковий зв'язок і мікрохвильовий зв'язок - також вразливі до глушіння, підміни і перехоплення. З них глушіння вимагає найменшої технічної складності, оскільки, як правило, полягає в простому перекритті цільового сигналу більш потужним генератором шуму. Спуфінг схожий на глушіння, за винятком того, що зловмисний сигнал імітує характеристики цільового сигналу, намагаючись ввести неправдиві дані в систему зв'язку (наприклад, військові засоби, які змушують приймачі PNT генерувати неточні рішення про місцезнаходження або час).

Перехоплення не має на меті перешкодити комунікації, а націлене на конфіденційність інформації, що передається мережею.

Підводні кабелі мають унікальні особливості. Вони є найбільш вразливими на мілководді біля берега, на ділянці від місця висадки кабелю до берега. Хоча супутникові і глибоководні частини підводних кабелів зазвичай знаходяться поза межами досяжності терористичних організацій, сучасні супротивники на рівні національних держав можуть мати засоби для безпосереднього ураження навіть найбільш захищеної критично важливої інфраструктури зв'язку - не лише глибоководних кабелів за допомогою глибоководних підводних апаратів, а й космічних об'єктів за допомогою протисупутникової зброї.

Окрім навмисних атак, на комунікаційні мережі можуть впливати і випадкові пошкодження. Підземні комунікаційні канали можуть бути пошкоджені або зруйновані під час розкопок або буріння, якщо не дотримуватися протоколів пошуку кабелів і техніки безпеки. Розчищення завалів після стихійних лих і реконструкція, зокрема, можуть поставити комунікаційні мережі під загрозу через стислі терміни відновлення і більш хаотичний характер робіт. Підводні кабелі, особливо на мілководді, були пошкоджені в результаті промивання та постановки на якір.

##### Кібератаки

Системи зв'язку також вразливі до низки кібератак. Більш детальну інформацію про кіберзагрози та суб'єктів див. у розділах 3-5. Комунікації унікальні тим, що можуть бути як об'єктом кібератаки, так і вектором, через який здійснюється атака на інші об'єкти критичної інфраструктури або системи. Розподілені атаки на відмову в обслуговуванні намагаються зробити віртуальні ресурси недоступними або скомпрометувати захисні заходи, завантажуючи мережеві ресурси фальшивою інформацією, яка споживає пропускну здатність і обчислювальні ресурси. Деякі кібератаки намагаються скомпрометувати інформаційні системи в Інтернеті, щоб порушити цілісність або конфіденційність даних. У деяких випадках зловмисники намагаються перехопити контроль над системами, щоб захопити або контролювати роботу об'єктів критичної інфраструктури або інших життєво важливих систем. Атаки з вимогою викупу спрямовані на отримання прибутку шляхом вилучення життєво важливих записів і систем у користувачів, а потім вимагають плату за звільнення систем і даних.

### Кейс Дослідження

Щоб показати широту ризиків для комунікацій, у цьому розділі представлено п'ять тематичних досліджень, що охоплюють різні аспекти комунікаційних загроз і сценаріїв реагування на низку кібер- та фізичних інцидентів.

Кожне тематичне дослідження має на меті представити або поглибити основні концепції безпеки та стійкості систем зв'язку, особливо проти загроз з боку терористичних організацій. Хоча окремі тематичні дослідження виконані на високому рівні, в більшості випадків наведені посилання дозволять набагато глибше проаналізувати і розглянути конкретні події. Різні сценарії мали місце в усьому світі, в тому числі в США і Європі, протягом останніх 15 років.

##### Фізичний напад: Вибух центрального офісу, Нешвілл, США

О 6:30 ранку 25 грудня 2020 року біля центрального офісу AT&T у Нешвіллі, штат Теннессі, вибухнув великий саморобний вибуховий пристрій, прикріплений до автомобіля. Будівля залишилася неушкодженою, але фізичні пошкодження нижніх поверхів, а також пожежа та обвалення призвели до того, що будівля була знеструмлена на кілька днів через пошкодження комерційних електромереж об'єкта, вплив вибуху на генератори на місці та проблеми з внутрішніми системами розподілу електроенергії. Розслідування, проведене Федеральним бюро розслідувань (ФБР), дійшло висновку, що нападник діяв самостійно і не був частиною великої організації, і хоча ФБР відзначило, що нападник вірив у низку ексцентричних теорій змови, вони не знайшли ідеологічної мотивації для нападу на цей об'єкт.3 Зрештою, основною мотивацією нападника, схоже, було бажання покінчити з власним життям під час резонансної події, обмеживши при цьому ризик поранення інших людей.

Роботи з відновлення зв'язку розпочалися майже одразу: компанія AT&T перевезла до Нешвіла персонал та обладнання зі своїх груп з відновлення мережі після аварій до Нешвіла, одночасно працюючи над перенаправленням нетермінального трафіку в обхід об'єкта.4 Початкові зусилля з відновлення на місці були ускладнені через труднощі з доступом до будівлі, спричинені низкою факторів, включаючи проблеми безпеки, пов'язані з структурною цілісністю будівлі, та обмеження, пов'язані зі статусом об'єкту як місця злочину, що активно розслідується. Компанія AT&T регулярно інформувала про хід відновлення об'єкту на спеціальній публічній веб-сторінці, а також урядові та галузеві організації за допомогою встановлених протоколів обміну інформацією.5 До ранку 26 грудня компанія AT&T розгорнула портативне мобільне обладнання із супутниковим зв'язком для відновлення зв'язку в регіоні, що в кінцевому підсумку дозволило збільшивши кількість мобільних вишок зв'язку до більш ніж 25 у розпал ліквідації наслідків вибуху. AT&T задіяла великі мобільні генератори для відновлення електропостачання, але через наслідки вибуху компанії довелося пробурити нові отвори для безпечної подачі електроенергії в будівлю. До ранку 27 грудня компанія AT&T відновила електропостачання щонайменше на чотирьох поверхах будівлі. Вранці 28 грудня, всього через три дні після вибуху, AT&T заявила, що відновила більшість послуг.

Хоча зловмисник, можливо, навмисно обрав своє місце розташування через його близькість до об'єкта зв'язку, а можливо, і ні, він навряд чи міг здійснити більш цілеспрямовану атаку на критично важливий вузол зв'язку. Наслідки атаки поширилися на кілька штатів і торкнулися тисяч клієнтів, включаючи бездротові та дротові послуги для споживачів, корпоративних клієнтів та інших операторів зв'язку. Рада з надзвичайних ситуацій штату Теннессі зазначила, що постраждали 66 пунктів зв'язку громадської безпеки - центрів, де приймаються дзвінки на номер "911" для надання першої допомоги - і що це вплинуло на роботу 66 пунктів зв'язку. Оскільки на об'єкті було розміщено інтерфейси міжмережевого зв'язку, численні інші оператори (дротового, кабельного та бездротового зв'язку) мали місцеві та регіональні наслідки, що тривали кілька днів.

Є кілька ключових спостережень і уроків, які можна винести з інциденту в Нешвіллі та реагування на нього:

* + Координація між операторами інфраструктури та службами швидкого реагування має важливе значення, особливо щодо доступу до об'єктів. Там, де це можливо, слід заздалегідь розробити процедури доступу та перевірки повноважень.
  + Враховуючи взаємопов'язаний характер сучасних комунікаційних мереж, координація між операторами має вирішальне значення. У Сполучених Штатах Америки всі основні оператори зв'язку, а також численні торгові асоціації та менші оператори входять до складу Центру обміну та аналізу комунікаційної інформації (Comm-ISAC), який співпрацює з Національним координаційним центром зв'язку Міністерства внутрішньої безпеки США (DHS). Національний координаційний центр і Comm-ISAC негайно почали обмінюватися інформацією про інцидент і 26 грудня провели першу з кількох координаційних телеконференцій. Див. розділ 11 для отримання додаткової інформації про важливу роль таких агенцій, як Comm-ISAC, в обміні інформацією та розвідданими.
  + Фізичне зміцнення інфраструктурних об'єктів. У той час як будівлі через дорогу від центрального офісу були повністю зруйновані, дуже міцно збудований центральний офіс майже не зазнав структурних пошкоджень, що дозволило дуже швидко відновити його після осушення будівлі та перенаправлення електропостачання до ще неушкоджених поверхів та обладнання.
  + Відмовостійкість систем резервного копіювання, в тому числі резервних з'єднань "останньої милі", має важливе значення для критично важливих комунікаційних вимог
  + Можливість швидкого та ефективного перенаправлення, яка часто забезпечується програмно-визначеною мережею, має вирішальне значення для того, щоб локальні збої не впливали на регіональний або національний трафік зв'язку.

##### Фізичний нещасний випадок і напад:

**Перебої з підводними кабелями в Єгипті (2008 і 2013 роки)**

Коли об'єкти критичної інфраструктури простягаються на великі відстані - лінії електропередач, залізничні колії, автомагістралі, трубопроводи або волоконно-оптичні кабелі - їх може бути важко захистити, оскільки зазвичай немає можливості встановити оборонний периметр навколо об'єкта. Хоча цілями можуть бути як наземні, так і підводні волоконно-оптичні кабелі, підводні кабелі мають вищі ризики, оскільки існує менше альтернативних шляхів, їх важче ремонтувати, а їх пропускна здатність, як правило, зосереджена на відносно невеликій кількості шляхів. Одне з критичних місць для підводних кабелів проходить уздовж східної частини Середземного моря до Єгипту і Червоного моря, як показано на рис. 9-2. Хоча випадкові пошкодження підводних кабелів є звичайною справою, два варті уваги інциденти сталися поблизу цього вузького місця у 2008 і 2013 роках.

Розділ 9 Стійкість комунікацій



**Малюнок 9-2. Карта підводних кабелів у східній частині Середземного моря**

(Карта від TeleGeography)

У січні та лютому 2008 року низка, здавалося б, не пов'язаних між собою аварій у східній частині Середземного моря та на Близькому Сході спричинила значний вплив на глобальні інформаційні потоки. Найбільш значна з них сталася 30 січня 2008 року біля узбережжя Александрії (Єгипет), розірвавши дві основні волоконно-оптичні лінії - SEA-ME- WE 4 і FLAG Europe-Asia, які разом забезпечували близько 75% зв'язку між Близьким Сходом і Південною Азією. Ця подія, яку пізніше пояснили тим, що корабель став на якір і пошкодив обидва кабелі, призвела до погіршення інтернет-зв'язку з Єгипту (на 70 відсотків) до Індії (на 60 відсотків), а також до перебоїв в Об'єднаних Арабських Еміратах (ОАЕ), Кувейті та Саудівській Аравії. Наслідки цих перебоїв були посилені кількома додатковими обривами кабелю FALCON поблизу ОАЕ, які сталися як до (23 січня), так і після (1 лютого) інциденту в Александрії. 5 грудня 2008 року сталося ще одне серйозне пошкодження кабелів SEA-ME-WE 4 і FLAG Європа-Азія, але цього разу було розірвано і третій кабель, SEA-ME-WE 3. Оскільки SEA-ME-WEA 3 використовувався для передачі перенаправлених

Якщо під час січневих відключень трафіку, груднева подія мала більший вплив, зачепивши Мальдіви (100% відключення), Індію (82%), Катар, Джибуті та ОАЕ (по 70%), а в Саудівській Аравії, Єгипті та Пакистані спостерігалися близько 50% перебоїв.

У той час у постраждалих країнах і в Інтернеті з'явилося багато теорій змови. Хоча обриви підводних кабелів під впливом цілого ряду факторів трапляються майже 200 разів на рік, поєднання ударів по кабелях, що обслуговують одні й ті ж регіони, одночасно підживлювало нестримні спекуляції, аж поки поблизу місць кількох обривів не були знайдені викинуті корабельні якорі. Хоча прямого зв'язку не було продемонстровано, здається, що зловмисники приділяли пильну увагу подіям 2008 року. У 2013 році кілька кабелів у тому ж районі біля єгипетського узбережжя знову зазнали численних розривів; цього разу, однак, єгипетська берегова охорона затримала трьох водолазів, які намагалися перерізати кабель SEA-ME-WE-4 за кілька сотень метрів від узбережжя Александрії.

У публікації 2017 року, підготовленій за підтримки Офісу директора національної розвідки США і Програми обміну аналітичними даними між державним і приватним секторами Міністерства національної безпеки США, висвітлено низку загроз для підводної кабельної інфраструктури. У звіті оцінюються ризики для підводних кабелів у різних точках вздовж заданого маршруту, охоплюючи наземну "останню милю", прибережні, морські, континентальні і глибоководні ділянки. Особливий інтерес у контексті боротьби з тероризмом викликає оцінка загрози для "вандалів, активістів і терористів", яка була визнана найвищою в наземних і прибережних сегментах. У звіті зокрема зазначається, що "концентрація місць висадки кабелів у дуже обмеженій кількості фізичних точок і відносна легкість пошуку задокументованих кабельних маршрутів і точок закінчення кабелів може полегшити зловмисникам вибір підводної кабельної мережі в якості мішені". У звіті також зазначається, що наземні частини кабельних мереж далекого радіусу дії також піддаються атакам.

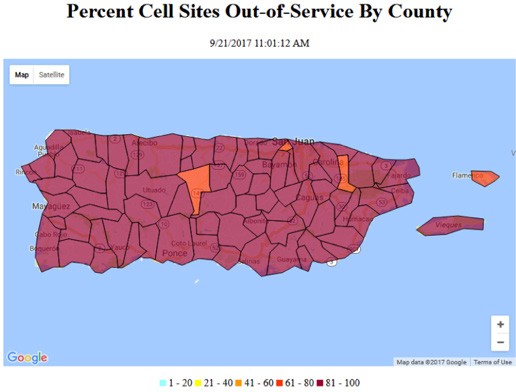
Існує кілька варіантів зменшення ризиків для кабелів зв'язку, особливо від потенційних нападів терористичних угруповань. Нижче наведено деякі ключові уроки та варіанти зменшення ризиків:

* + У тісній координації з приватними операторами кабелів забезпечити фізичне і логічне різноманіття маршрутів для всіх критично важливих комунікаційних шляхів і оперативну підготовку до швидкого перенаправлення трафіку. У випадку підводних кабелів це також повинно включати уникнення, де це можливо, "вузьких місць" і концентрації зайвих кабелів, як, наприклад, поблизу місць висадки в Александрії, Єгипет.
  + Підтримуйте достатній потенціал для ремонту критично важливих кабелів без зайвих затримок.
  + Розгляньте варіанти зміцнення прибережних і наземних підводних кабельних споруд. Приклади включають
    - Обкопайте та закопайте прибережні ділянки, щоб зменшити ризики випадкового вилову риби або пошкодження якоря, а також спроб саботажу з боку водолазів або земснарядів на мілководді.
    - Зміцнити кабельні посадочні станції.
    - Налагодити активну координацію між національними та місцевими правоохоронними органами, береговою охороною, ВМС, телекомунікаційними операторами та операторами посадочних станцій для забезпечення безпеки та реагування на інциденти.
    - Мінімізувати загальнодоступну інформацію, яка містить конкретні місця розташування прибережних кабелів і кабельних наземних станцій.
    - Зміцнити відповідну фізичну інфраструктуру настільки, наскільки це практично можливо, в тому числі забетонувати опори, заварити кришки каналізаційних люків та закріпити інші потенційно вразливі компоненти, такі як електромонтажні шафи, панелі доступу та ліфтові шахти, у приміщеннях спільного користування.

##### Стихійне лихо: ураган у США 2017 року Сезон

Сезон ураганів 2017 року був унікально руйнівним для південного сходу США та Карибських островів. Насправді, руйнування були настільки значними, що Федеральна комісія зв'язку США прийняла рішення Надзвичайна акція, яка полягала у виданні спеціального звіту з детальним описом численних наслідків для інфраструктури зв'язку. Звіт зосередився на збитках від трьох основних штормів: Ураган Харві, що обрушився на Х'юстон, штат Техас, у серпні 2017 року; ураган Ірма, що обрушився на Віргінські острови США, Пуерто-Рико і Флориду на початку вересня 2017 року; і ураган Марія, що зруйнував Віргінські острови США і Пуерто-Рико в середині вересня 2017 року. Оскільки найбільш руйнівні та довготривалі наслідки цих трьох штормів були спричинені ураганом "Марія" в Пуерто-Рико та на Американських Віргінських Островах, це тематичне дослідження зосередиться на наслідках урагану "Марія".

Ураган "Марія" майже повністю зруйнував комунікаційну інфраструктуру як в Американських Віргінських островах, так і в Пуерто-Рико. У найгіршому випадку ураган "Марія" знищив понад 75% мобільного зв'язку в ЗВО США і понад 95% мобільного зв'язку в Пуерто-Рико, де 48 з 78 муніципалітетів (еквівалент округу) були на 100% позбавлені мобільного зв'язку. Рисунок 9-3 ілюструє цю руйнівну втрату мобільного зв'язку в Пуерто-Рико на наступний день після урагану "Марія". Крім того, на відміну від попередніх ураганів, мобільний зв'язок після "Марії" не відновився швидко; фактично, деякі сайти стільникового зв'язку все ще не працювали навіть через шість місяців після урагану. На Американських Віргінських островах основний пункт зв'язку з питань громадської безпеки не працював щонайменше 10 днів. Так само постраждали радіо- і телекомпанії, багато з яких були вимкнені протягом тривалого часу.



**Малюнок 9-3. Стільниковий зв'язок у Пуерто-Рико на наступний день після урагану "Марія**

(Карта Федеральної комісії з питань зв'язку США)

Хоча наслідки стихійного лиха можуть здаватися не пов'язаними з контртерористичним плануванням, є кілька ключових уроків, які можна винести з цих суворих погодних явищ:

* + Стійкість зв'язку тісно пов'язана з наявністю надійного електропостачання. Безумовно, основною причиною збоїв у роботі стільникового зв'язку був брак комерційної електроенергії в поєднанні з відсутністю генераторів, виходом їх з ладу або нестачею пального.
  + Широкомасштабні стихійні лиха певною мірою впливатимуть на комунікаційні мережі, і ці комунікаційні впливи негативно позначаться на ситуаційній обізнаності та управлінні, необхідних для розробки і виконання планів дій з реагування.
  + Збої в роботі комунікацій - наприклад, мобільного зв'язку, можливості викликати першу допомогу або відсутність можливості мовлення - мають значний вплив на стійкість громади. Системне навантаження на інфраструктурні системи, включаючи комунікації, внаслідок стихійних лих робить громади більш вразливими до наслідків наступної атаки терористів, тоді як наслідки такої атаки можуть бути посилені.

##### Кібератака на системи зв'язку: TV5 Monde

8 квітня 2015 року група, що називала себе "КіберХаліфатом", атакувала французьку телевізійну мережу TV5 Monde. Підготовка до цієї витонченої атаки почалася за кілька місяців до того, а первинне проникнення в мережу відбулося ще 23 січня 2015 року. Зловмисники проводили системну розвідку мережі TV5 Monde, щоб зрозуміти, як мережа розробляє, ставить і транслює свій контент. Систематично заглиблюючись у мережу TV5 Monde, зловмисники створили шкідливе програмне забезпечення, яке пошкодило підключене до Інтернету обладнання, що контролювало роботу станції, і навіть поставило під загрозу здатність станції кодувати контент для трансляції. Коли розпочалася основна атака, всі 12 каналів мережі спочатку були виведені з ефіру, Деякі канали не відновлювалися протягом 18 годин. Майже одночасно було зламано веб-сайт та акаунти мережі в соціальних мережах, які використовувалися для розміщення пропаганди на підтримку ісламського халіфату.

Хоча сучасники події спочатку висловлювали тривогу з приводу того, що Ісламський Халіфат раптово виявився більш спроможним і витонченим кіберсупротивником, почали з'являтися ознаки того, що атака могла бути операцією "фальшивого запізнення", проведеною іншим суб'єктом, який намагався перекласти провину за атаку на нього. Комплексна атака використовувала кілька точок проникнення, намагаючись скомпрометувати мережу TV5 Monde, включаючи навіть підключені до Інтернету камери спостереження станції. Компанія FireEye, що спеціалізується на комп'ютерній криміналістиці, остаточно приписала атаку російській групі передових постійних загроз (APT), відомій як Fancy Bear або APT 28, припустивши, що фальшивий фейк був "швидше за все, російською інформаційною операцією", покликаною "скористатися страхами Заходу щодо ісламського екстремізму" і "відвернути увагу Заходу від ролі Росії в українській кризі і до загрози тероризму на Близькому Сході".18 FireEye, разом з урядовими розслідуваннями та іншими фірмами з кібербезпеки, відзначила низку доказів, що вказують на причетність Росії, включаючи блоки Інтернет-протоколу (IP), суміжні з іншими відомими видами діяльності APT 28, компіляції коду, що відповідають операціям у Москві та Санкт-Петербурзі, а також кодову базу, написану за допомогою кириличної клавіатури.

В результаті інциденту зловмисники зняли з ефіру 12 каналів TV5 Monde, завдавши прямих фінансових збитків на суму понад 4,5 мільйона євро. На щастя, зловмисники або не змогли, або вирішили не захоплювати ефір повністю, щоб транслювати контент на свій розсуд. Однак зловмисники захопили пов'язані з TV5 Monde акаунти в соціальних мережах (YouTube, Twitter і Facebook), щоб розпочати пропагандистські кампанії. Деякі спостереження та уроки, винесені з атаки 28 серпня, включають наступне:

* + Важливість багаторівневого захисту. Згідно з численними джерелами, TV5 Monde не мав належної сегментації своєї внутрішньої мережі. Їхні інформаційні та операційні системи були взаємопов'язані, що дозволяло порушенню в бізнес-частині мережі впливати на операційні системи.
  + У кіберподіях важко встановити авторство і навіть за найкращих обставин залишається певний ступінь невизначеності. Крім того, навіть якщо встановлення авторства можливе, публічне визнання авторства може розкрити чутливі джерела і методи, за допомогою яких воно було досягнуто. Ці проблеми з визначенням авторства ускладнюють стримування, оскільки покладання наслідків на зловмисника вимагає певної впевненості в тому, що саме зловмисник понесе витрати, пов'язані з відплатою за скоєне. Див. приклад України в розділі 5 для обговорення труднощів з визначенням авторства і варіантів реагування на кібератаки.
  + Хоча комунікаційні системи часто стають об'єктами кібератак, спрямованих на досягнення інших цілей, комунікації іноді стають безпосередніми мішенями. Оскільки як національні держави, так і недержавні суб'єкти продовжують розглядати інформаційні та дезінформаційні кампанії як засоби для досягнення своїх цілей, припущення, що прямий контроль над засобами комунікації залишатиметься привабливою мішенню.
  + Здатність атакувати мережі мовлення в поєднанні з іншими діями в рамках комплексної атаки може значно ускладнити можливість комунікації з громадськістю, тим самим спричиняючи значно більший вплив, ніж проста кінетична атака сама по собі.

##### Розподілена відмова в обслуговуванні (DDoS): Ботнет Mirai

На початку серпня 2016 року почав поширюватися новий варіант шкідливого програмного забезпечення, відомий як Mirai. Це шкідливе програмне забезпечення, що самовідтворюється, націлене на пристрої Інтернету речей, такі як домашні маршрутизатори, камери спостереження, принтери та мережеві накопичувачі. Після встановлення на новий пристрій шкідливе програмне забезпечення шукало інші пристрої для зараження, випадковим чином скануючи Інтернет у пошуках цілей, а потім намагалося отримати доступ до них, перебираючи 64 загальновживані комбінації логінів і паролів. На той час багато пристроїв Інтернету речей використовували паролі за замовчуванням, які користувачі рідко змінювали, тому шкідливе програмне забезпечення змогло поширитися напрочуд швидко. Компанія Cloudflare, що спеціалізується на кібербезпеці, підрахувала, що протягом перших кількох днів свого існування шкідливе програмне забезпечення подвоювало кількість захоплених пристроїв кожні 76 хвилин. Ці захоплені пристрої (тепер відомі як боти) утворювали своєрідну мережу (ботнет), коли кожен пристрій зв'язувався з командно-контрольними серверами (C2) для отримання інструкцій про те, що робити далі. У випадку з Mirai, сервери C2 могли надати інструкції для запуску DDoS-атак на атакують комп'ютери та мережі фіктивним трафіком, щоб перевантажити здатність серверів відповідати, таким чином роблячи сайт або послугу недоступними для законного використання.

Першими двома жертвами ботнету Mirai стали європейська веб-хостингова компанія OVH 18 вересня 2016 року та сервери, на яких знаходилась онлайн присутність відомого дослідника кібербезпеки Брайана Кребса 21 вересня. На той час це були одні з найбільших DDoS-атак, які коли-небудь спостерігалися. Пізніше того ж місяця творець Mirai розмістив його вихідний код в Інтернеті, що призвело до масового поширення бот-мереж, побудованих за моделлю Mirai, і не минуло багато часу, як ці нові ботнети стали активними. 21 жовтня Mirai був використаний для атаки на Dyn, систему розпізнавання доменних імен (DNS). DNS-розпізнавачі, такі як Dyn, переводять текстові інтернет-адреси в числові IP-адреси, щоб забезпечити маршрутизацію інтернет-трафіку. Оскільки Dyn надавав цю послугу багатьом клієнтам, атака на їхню службу DNS зробила значну частину Інтернету недоступною на короткий час, поки атака не була нейтралізована. У наступні місяці інші групи зловмисників, які використовували Mirai, атакували широке коло жертв по всьому світу. Варіанти Mirai залишаються активними і донині; лише у другому кварталі 2021 року міжнародна комунікаційна компанія Lumen через свій підрозділ з дослідження загроз Black Lotus Labs виявила 349 унікальних інфраструктур Mirai C2, причому кожна "сім'я" Mirai C2 атакувала в середньому понад 15 000 жертв протягом типового місячного терміну життя.

З кількох причин ботнет Mirai є важливим прикладом для розуміння терористичної кіберзагрози системам зв'язку:

* + Опинившись "у вільному доступі", експлойт був швидко взятий на озброєння великою кількістю груп, принаймні деякі з яких продавали DDoS-послуги за винагороду, надаючи цей вид кібератаки в руки будь-якої особи чи групи, готової за це заплатити.
  + Шкідливе програмне забезпечення успішно поширюється в середовищах, де відсутні базові заходи кібербезпеки (наприклад, коли пристрої, підключені до Інтернету, з паролями за замовчуванням або загальними паролями, залишаються незахищеними).
  + Сама атака не була технічно складною. Оригінальний код був написаний студентом старших курсів та двома друзями. Агент ФБР, який розслідував цю справу, сказав: "Ці діти дуже розумні, але вони не зробили нічого високого вони просто мають гарну ідею". Хоча державні кіберсуб'єкти іноді володіють надзвичайно складними можливостями, кіберпростір - це поле бою, де менші гравці можуть створювати, запозичувати або купувати відносно прості засоби, які можуть мати значний вплив на безпеку та стійкість КІ.

### Висновок

Як описано в цьому розділі, системи зв'язку є основним компонентом критично важливої інфраструктури, яка необхідна для функціонування економіки і здатності держави реагувати на кризові ситуації та вести військові дії. На основі нещодавніх інцидентів, що вплинули на системи зв'язку, подібних до тих, що обговорювалися в тематичних дослідженнях, можна виділити кілька важливих заходів, які уряди і галузь можуть вжити для зміцнення безпеки та стійкості сектору зв'язку.

##### Координація та зв'язки з "блакитним небом" Розбудова

Безпека і стійкість сектору зв'язку незмірно підвищуються завдяки активному і міцному державно-приватному партнерству між постачальниками послуг зв'язку, фахівцями з національної безпеки і посадовими особами, відповідальними за громадську безпеку. Ці відносини повинні встановлюватися і розвиватися задовго до катастрофи, що насувається, або фактичної атаки. Рутинна і регулярна взаємодія необхідна для побудови особистого знайомства і встановлення довіри. Ця взаємодія також забезпечує актуальність процесів і процедур координації, включаючи навіть такі базові речі, як наявність контактної інформації, списків розсилки і віртуальних платформ, які є доступними і функціональними. У Сполучених Штатах Національний координаційний центр зв'язку Міністерства внутрішньої безпеки США проводить постійну щотижневу телефонну конференцію з основними федеральними департаментами, регуляторами зв'язку і десятками представників комунікаційних компаній; під час неї обговорюються кібер- і фізичні інциденти, що розвиваються, ставляться запитання і даються відповіді, а також встановлюється спільний лексикон і рівень взаєморозуміння. Партнерства, що розвиваються за допомогою таких механізмів, формують фундамент, на якому найлегше вирішувати цілу низку інших проблем і можливостей, наприклад, таких як

* + Створення базових механізмів координації за допомогою телеконференцій, відеоконференцій, особистих зустрічей, розсилок електронною поштою та онлайн-порталів, які використовуються для обміну інформацією та координації реагування під час стабільних операцій та під час кризових ситуацій.
  + Заздалегідь налагодити процеси звітування про катастрофи, щоб усі ключові зацікавлені сторони розуміли очікувану каденцію звітування і мали доступ до шаблонів звітності та інтерфейсів прикладного програмування для побудови внутрішніх процесів звітування.
  + Створення централізованого координаційного механізму для мінімізації численних звітів та запитів між урядом та промисловістю.
  + Відпрацювання спільно розроблених механізмів перед використанням їх у кризових ситуаціях.
  + Заохочення міжгалузевої координації та співпраці, які можуть бути використані під час реагування на інциденти.

##### Ідентифікація ризиків та відповідне пом'якшення Стратегії

Як і у випадку з усіма заходами з управління ризиками для критичної інфраструктури, сприяння безпеці та стійкості комунікацій є найбільш ефективним, коли власники-оператори комунікаційних мереж залучаються до цього процесу на ранніх етапах. Власники-оператори, озброєні найкращою доступною інформацією про загрози для своєї інфраструктури, мають найкращі можливості для найбільш ефективного інвестування в ініціативи з безпеки і стійкості, спрямовані на усунення цих загроз. Аналогічно, ті, хто залежить від систем зв'язку, отримують вигоду від чіткого аналізу ризиків для цих систем, на які вони покладаються.

Огляд нещодавніх подій, включно з тими, що представлені в наведених тут тематичних дослідженнях, показує кілька сфер, де інвестиції в стійкість були особливо ефективними:

* + Різноманітність фізичних та віртуальних шляхів. Критично важливі комунікації повинні мати різноманітні фізичні та логічні шляхи для забезпечення більшої стійкості. Сучасні комірчасті мережі забезпечують чудову різноманітність маршрутів у магістральних мережах далекого радіусу дії, а програмно-визначені мережі забезпечують гнучкість цих маршрутів, що дозволяє швидко перенаправляти трафік в напрямку від пошкоджених мереж. Однак така динамічна зміна маршрутів можлива лише там, де це дозволяє фізична інфраструктура, і тому є більш складним завданням у менш щільних районах, зокремаРозділ 9 Стійкість комунікацій

на "останній милі", що з'єднує кінцевих користувачів. Ті, хто покладається на зв'язок для виконання критично важливих військових завдань, забезпечення громадської безпеки або бізнес-вимог, повинні тісно співпрацювати з мережевими провайдерами, щоб зрозуміти і врахувати фізичну і логічну різноманітність маршрутів.

* + Базові практики кібербезпеки. Забезпечення базового рівня найкращих практик кібербезпеки - таких як регулярне встановлення патчів, контроль брандмауерів, виявлення вторгнень і багатофакторна автентифікація - допоможе запобігти або принаймні пом'якшити атаки кіберзлочинців і низькорівневих недержавних груп акторів. Зловмисники високого рівня, що фінансуються державою, і все більш кваліфіковані наймані зловмисники можуть зламати навіть найкращі системи кіберзахисту, що робить стратегії пом'якшення наслідків - в тому числі архітектури з нульовою довірою, сегментацію мережі, застосування принципу найменших привілеїв і шифрування даних - однаково важливими. Огляд рекомендованих найкращих практик та інструментів кібербезпеки див. у главі 14.
  + Міжгалузеві зв'язки між комунікаціями, електроенергетикою та інформаційними технологіями. Більшість значних подій, що вплинули на комунікації за останні 20 років, були пов'язані з проблемами в електроенергетиці або інформаційних технологіях. Вкрай важливо, щоб сектор зв'язку регулярно координував і вирішував системні ризики на перетині цих трьох секторів, а державні органи безпеки і планування реагування враховували цю потребу в координації в оперативних планах і планах обміну інформацією.

##### Комунікації Інструменти забезпечення стійкості сектору

Комерційні провайдери зв'язку активно керують мережевими подіями на щоденній основі і є експертами із захисту, обслуговування та відновлення своїх мереж. Однак є ключові сфери, в яких уряд і промисловість можуть співпрацювати задля підвищення стійкості сектору.

На додаток до описаних вище механізмів партнерства, приватний сектор може отримати значну вигоду від регулярного обміну інформацією з урядами про відомі загрози з боку супротивників до того, як інциденти відбудуться. Розуміння ймовірної тактики, методів і процедур супротивника допоможе галузі розробити і впровадити індивідуальні заходи протидії та зниження ризиків. Якщо відомі конкретні тактики, методи і процедури перед атакою або інші кіберіндикатори компрометації, ними слід ділитися з галуззю тому власники та оператори можуть бути в курсі ознак атаки, що наближається. Уряд і промисловість також можуть отримати вигоду від швидкого обміну потенційними заходами захисту, щоб оцінити їх ефективність у своїй галузі або на своєму об'єкті і швидко впроваджувати їх там, де це має сенс. Див. обговорення переваг і кращих практик обміну інформацією в розділі 11.

Досвід показує, що під час інцидентів реагування галузі покращується завдяки тісній координації між відповідними державними та галузевими партнерами. Ключовими елементами такої співпраці є

* + Доступ. Часто після нападу, катастрофи або в періоди підвищеної напруженості просто доставити персонал і транспортні засоби до мережевих об'єктів стає проблемою. Вкрай важливо, щоб провайдери зв'язку та урядовці працювали разом, щоб якнайшвидше забезпечити доступ до зон з обмеженим доступом, координувати розчищення доріг і вивезення завалів, а також розчищати шляхи доступу до віддалених об'єктів.
  + Енергетика. Швидке та/або пріоритетне відновлення електропостачання значно підвищить здатність сектору зв'язку до швидкого відновлення, тому координація щодо пріоритетів відновлення електропостачання та орієнтовного часу відновлення є надзвичайно важливою. Там, де неможливо швидко відновити електропостачання, критично важливим стає доступ до палива (дизельного палива, бензину, а іноді і пропану) для виробництва електроенергії на місці.
  + Безпека. Безпека об'єктів зв'язку, включаючи тимчасові активи, такі як портативні генератори, мобільний мобільний зв'язок, робочі бригади та склади пального, є життєво важливою.
  + Цілісність каналів зв'язку та кабелів. Досвід минулих інцидентів показує, що під час ліквідації наслідків аварій, таких як розбирання завалів, волоконно-оптичні та інші кабелі часто пошкоджуються або знищуються ненавмисно. Тісна координація і чітке інформування громадськості, що закликає до обережності під час роботи у волоконно-оптичних і повітряних кабелях і навколо них, може допомогти зменшити частину цього ризику.
  + Своєчасне оновлення інформації. У міру розвитку ситуації, коли уряд має дієву інформацію - наприклад, розвідувальні дані або визначені захисні заходи - він повинен швидко ділитися цією інформацією з промисловістю, щоб її можна було використати на практиці.

Як сектор життєзабезпечення, зв'язок забезпечує більшість основних функцій сучасного світу, включаючи військове командування і управління, урядові операції, координацію реагування на надзвичайні ситуації, економічну продуктивність і соціальну активність. Саме з цих причин комунікації є привабливою мішенню для терористичних угруповань та інших супротивників. У той час як комунікаційні компанії докладають значних зусиль для побудови безпечних і стійких мереж, уряд і промисловість можуть координувати зусилля для встановлення міцних оперативних зв'язків, виявлення і зменшення критичних ризиків, а також розробки життєздатних планів дій для сценаріїв реагування на катастрофи.

# - 10 -

## Порівняння рамкових політик:

**CISR у США та Європейському Союзі**

Рональд Бірс та Алессандро Лазарі

Понад чверть століття Сполучені Штати і Європейський Союз старанно планують і впроваджують політику і процедури для захисту секторів критичної інфраструктури, які є життєво важливими для процвітання і безпеки більшості їхніх громадян. З огляду на мінливий характер загроз критичній інфраструктурі, останні зусилля США і ЄС зосереджені на посиленні колективної безпеки і стійкості критичної інфраструктури (CISR). Основною метою цих ініціатив CISR є посилення здатності стримувати, запобігати, зменшувати наслідки, реагувати і відновлюватись після широкого спектру вразливостей, небезпек і загроз для критичної інфраструктури. Будь-які перебої в роботі або руйнування цих систем і об'єктів критичної інфраструктури можуть мати руйнівний вплив на окремі країни, трансатлантичну економіку і безпекове середовище, а також на здатність Організації Північноатлантичного договору (НАТО) виконувати свої основні завдання.

Політика і практика США та ЄС у сфері КІСР вже давно визнані двома найбільш передовими системами у світі. Оскільки переважна більшість національних політик і планів у сфері СІСР в усьому світі відображають або певною мірою посилаються на моделі США або ЄС, у цьому розділі описані ключові засади і характеристики кожної з них. Фактично, серед 30 країн-членів НАТО 22 з них - Сполучені Штати і 21 країна, які також є членами ЄС - перебувають під безпосереднім впливом цих концепцій. На них впливають вісім країн-членів та численні країни-партнери.1 У цьому розділі спочатку розглядається система США, а потім ЄС, причому в кожному розділі окреслюються фундаментальні елементи відповідних моделей, причини виникнення цих систем і їх адаптації з часом, а також різні способи їх застосування для зміцнення національної, регіональної і міжнародної безпеки, економічного процвітання, громадського здоров'я і безпеки. Мета цього розділу - допомогти членам і партнерам Альянсу і партнерам краще зрозуміти ці дві концепції і застосувати їхні ключові принципи і положення для посилення СЗБП у своїх країнах.

### US CISR Рамки

Вперше поняття критичної інфраструктури з'явилося в офіційній політиці США в 1996 році, коли президент США Білл Клінтон підписав Указ № 13010, яким було створено національну комісію з оцінки масштабів і характеру вразливостей та загроз об'єктам і системам критичної інфраструктури. Комісія також рекомендувала комплексну національну політику і стратегію її реалізації для захисту об'єктів критичної інфраструктури від фізичних і кіберзагроз і забезпечення їх безперервного функціонування.2 П'ять років потому Патріотичний акт США 2001 року зробив додатковий крок, визначивши критичну інфраструктуру як "системи та активи, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що непрацездатність або руйнування таких систем і активів матиме виснажливий вплив на безпеку, національну економічну безпеку, здоров'я і безпеку населення, або будь-яку комбінацію цих питань".3

Більш ніж десять років потому, у 2013 році, президент США Барак Обама визначив сучасну національну політику США у сфері КІСБ, підписавши Президентську політичну директиву 21 (ППД-21), спрямовану на зміцнення національної єдності зусиль для зміцнення і підтримки безпечної, функціонуючої і стійкої критичної інфраструктури проти всіх небезпек, включаючи фізичні та кіберзагрози.4 Офіційно ППД-21 наголосив на різниці між захистом критичної інфраструктури (ЗКІ) та підвищенням її безпеки та стійкості (ПБСІ).

Критична інфраструктура в США складається з розподілених мереж, численних типів організаційних структур і операційних моделей (включно з багатонаціональною власністю), взаємозалежностей у фізичній і кібернетичній сферах, а також унікальних механізмів, що складаються з повноважень, обов'язків і правил на всіх рівнях уряду і приватного сектору.5 З огляду на таку складну і різноманітну природу критичної інфраструктури, мета політики, викладена в ППД-21, є амбітною і складною для досягнення. Тому ППД-21 визнає необхідність співпраці між державним і приватним секторами, координації між різними відомствами та рівнями влади, а також інтеграції з національною системою готовності в усьому спектрі запобігання, захисту, пом'якшення наслідків, реагування та відновлення.6

Згідно з чинною політикою CISR, встановленою PPD-21, федеральний уряд відповідає за посилення безпеки та стійкості власної критичної інфраструктури, забезпечення безперервності життєво важливих функцій країни та продовження ефективного партнерства з власниками та операторами критичної інфраструктури з метою посилення їхніх зусиль у сфері CISR.7 На додаток до партнерства з власниками та операторами приватного сектору, федеральний уряд співпрацює зі штатами, місцевими, племінними та територіальними утвореннями з метою управління ризиками та посилення безпеки і стійкості критично важливої інфраструктури країни до всіх загроз, які можуть мати виснажливий вплив на національну безпеку, економічну стабільність або громадське здоров'я та безпеку. PPD-21 також вимагає від федерального уряду взаємодіяти з міжнародними партнерами для посилення безпеки та стійкості національної критичної інфраструктури, а також тих об'єктів або активів, розташованих за межами національних кордонів, від яких залежить життєдіяльність країни.

##### Чим керується політика США у сфері CISR ?

ППР-21 окреслює три стратегічні імперативи, які є основою для вдосконалення національних практик і процедур у сфері КІСР. Перший імператив полягає в посиленні функціональних зв'язків між федеральними органами влади з метою забезпечення єдності зусиль на національному рівні. Ключовим елементом цих зусиль є національний план, який визначає ролі та обов'язки галузевих відомств; інших федеральних відомств та відомства, що виконують функції критичної інфраструктури; державні, місцеві, племінні та територіальні утворення; а також власники та оператори об'єктів критичної інфраструктури. Оскільки вразливості, ризики та загрози для критичної інфраструктури у ХХІ столітті змінилися, політика РСБІ також адаптувалася до цих змін, часто у формі інноваційних програм та ініціатив, спрямованих на вирішення конкретних інфраструктурних питань та пріоритетів. PPD-21 окреслює необхідність створення базових можливостей, які відображають цю еволюцію знань і практики, визначення відповідних функцій федеральних програм, а також вжиття заходів для сприяння співпраці та обміну інформацією між федеральними агентствами.8 Як частина цієї оновленої структури, PPD-21 передбачив створення двох національних центрів - для фізичних і кібернетичних аспектів інфраструктури відповідно - при Міністерстві внутрішньої безпеки (DHS), які стануть координаційними центрами інформації та ситуаційної обізнаності для партнерів у сфері критичної інфраструктури. З моменту свого створення у 2018 році ці дві функції виконує Агентство кібербезпеки та безпеки інфраструктури (CISA).

Другим імперативом у цьому контексті є забезпечення ефективного обміну інформацією, в тому числі розвідувальною, між усіма рівнями влади та власниками і операторами об'єктів критичної інфраструктури з метою забезпечення ситуативної обізнаності та багатовекторного обміну інформацією про загрози і вразливості. Для посилення багатовекторного обміну інформацією між урядом і приватним сектором цей імператив підкреслює важливість визначення (1) вимог до форматів і доступності даних та інформації, (2) інтероперабельності систем і (3) резервних систем і альтернативних можливостей на випадок збоїв в роботі основних систем.9

Спираючись на перші два імперативи, третій стратегічний імператив вимагає впровадження функції інтеграції та аналізу критичної інфраструктури, що включає оперативний і стратегічний аналіз інцидентів, загроз і ризиків, що виникають. Інтеграція та аналіз інформації знаходиться в компетенції CISA і включає в себе здатність зіставляти, оцінювати та інтегрувати інформацію щодо вразливостей та наслідків з потоками загроз та інформацією про небезпеки. Хоча ця функція не повторює аналіз, що проводиться в більш широкому національному розвідувальному співтоваристві, вона

(1) допомагає визначити пріоритетність активів та управляти ризиками для критичної інфраструктури,

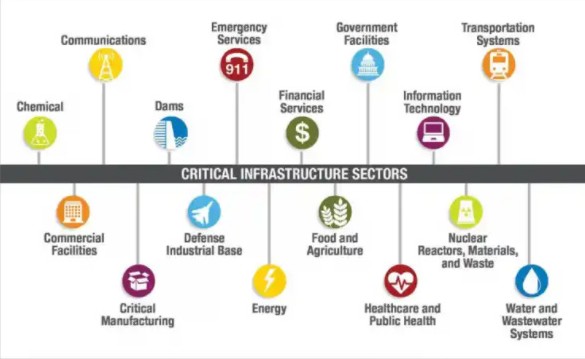
(2) передбачає каскадний вплив через взаємозалежності, (3) рекомендує заходи CISR до, під час і після події або інциденту, і (4) підтримує зусилля з управління інцидентами та відновлення критично важливої інфраструктури.

Ця функція залежить від зацікавлених сторін - федеральних департаментів і відомств, а також аналітичних структур на всіх інших рівнях влади і в приватному секторі - які надають відповідну, своєчасну і належну інформацію CISA, щоб вона могла підтримувати і поширювати ситуаційну обізнаність майже в режимі реального часу, надаючи практичну інформацію про неминучі загрози, значні тенденції та інциденти, які можуть вплинути на критично важливу інфраструктуру.11

Враховуючи ці три стратегічні імперативи та ширший стратегічний напрямок, викладений у ППД-21, Національний план захисту інфраструктури (НПЗІ) 2013 року відповідає на чіткий заклик ППД-21 щодо оновлення національного плану. NIPP 2013 представляє бачення та місію політики CISR, за яку CISA несе головну відповідальність серед федеральних агентств. Згідно з NIPP 2013, фізична та кібернетична критична інфраструктура повинна "залишатися безпечною та стійкою, вразливості мають бути зменшені, наслідки мінімізовані, загрози виявлені та знешкоджені, а реагування та відновлення - прискорені". У свою чергу, це бачення визначає основний підхід до зміцнення CISR "шляхом управління фізичними і кібернетичними ризиками за допомогою спільних і інтегрованих зусиль спільноти критично важливої інфраструктури".

Важливим першим кроком є визначення секторів інфраструктури, які є одночасно критично важливими для підтримки безперервного надання послуг або функціонування і вразливими до певних видів загроз або небезпек. Уряд США визначив чотири сектори - транспортні системи, системи водопостачання та водовідведення, енергетика та зв'язок - як сектори життєзабезпечення, оскільки більшість інших секторів залежать від цих функцій та послуг. Пояснення щодо секторів життєзабезпечення див. у розділі 1.14 Через таку залежність і взаємозалежність між елементами інфраструктури втрата однієї функції життєзабезпечення, як правило, має негайний вплив на роботу кількох секторів. Більш детально про характер залежностей, взаємозалежностей і каскадних або ескалаційних ефектів див. у розділі 12. Визначення та офіційне визнання секторів життєзабезпечення, а також виявлення існуючих міжсекторальних взаємозалежностей полегшує співпрацю та обмін інформацією, а також сприяє безперервності операцій і послуг.

Загалом, політика США у сфері КІСР наразі визнає 16 секторів критично важливою інфраструктурою. На додаток до чотирьох секторів життєзабезпечення, ще 12 секторів включають: хімічну промисловість, комерційні об'єкти, дамби, оборонну промисловість, аварійні служби, енергетику, фінансові послуги, харчову промисловість і сільське господарство, урядові установи, охорону здоров'я, інформаційні технології, критично важливі виробництва, ядерні реактори, матеріали та відходи (див. рис. 10-1).16 Хоча кількість визначених секторів критичної інфраструктури наразі становить 16, ця кількість може змінюватися з огляду на вразливість окремих секторів і характер взаємозалежності між ними. Наприклад, у 2017 році уряд США виділив виборчу інфраструктуру як підсектор сектору державних установ через важливість вільних і чесних демократичних виборів як основи американського способу життя.



**Рисунок 10-1. 16 секторів критичної інфраструктури, визнаних політикою США**

(Джерело: діаграма DHS)

Коли йдеться про захист цих критично важливих секторів інфраструктури та підвищення їхньої стійкості, важливо розуміти природу загроз і небезпек, які можуть вплинути на їхню діяльність. Деякі небезпеки та загрози є специфічними для географічних регіонів, інші впливають на всю країну, а деякі можуть мати навіть глобальний вплив. Використовуючи підхід, що враховує всі небезпеки, політика США у сфері РСБІ починається з оцінки спектру загроз і небезпек для критичної інфраструктури, аналізу ймовірності їх виникнення та потенційних наслідків, а потім спрямовує зусилля на зосередження уваги на тих, що становлять найбільший ризик, і підготовку до них. Хоча цей перелік не є вичерпним, уряд розглядає наступні небезпеки та загрози при визначенні відповідних заходів

Політика та практика CISR. Детальніше про фізичні, кібернетичні та гібридні загрози див. у розділах 2-4.

* + Кліматологічні, гідрологічні, метеорологічні та геофізичні події, такі як посуха, лісові пожежі, повені, тропічні циклони, сильні зимові бурі, землетруси, цунамі або виверження вулканів
  + Пандемії
  + Промислові аварії, такі як руйнування конструкцій та розливи хімічних речовин
  + Незаплановані перебої через старіння інфраструктури або несправності
  + Кримінальні інциденти та фізичні або терористичні напади
  + Кіберінциденти, включаючи атаки на відмову в обслуговуванні, шкідливе програмне забезпечення та фішинг
  + Атаки, що використовують вразливості ланцюгів постачання для спричинення збою в роботі системи
  + Іноземні операції з поширення дезінформації, підриву демократичних процесів або інвестицій, які надають іноземним державам неправомірний вплив

##### Впровадження раціональної системи управління ризиками

Важливим першим кроком у розробці політики КІСБ є розуміння природи ризиків для критичної інфраструктури та розробка відповідних заходів для їх зменшення або реагування на них. NIPP 2013 визначає ризик як потенційну можливість небажаного результату в результаті інциденту, події або явища, що визначається ймовірністю його виникнення - з огляду на характер загроз і вразливостей - і наслідків, які можуть настати після цього.18 Управління ризиками - це процес виявлення, аналізу та інформування про ризики, а потім прийняття, уникнення, передачі або контролю за ними на прийнятних рівнях і з прийнятними витратами.19 Управління ризиками посилює позицію США у сфері СЗПБ у кількох важливих аспектах. По-перше, воно привертає увагу до тих загроз і небезпек, які з найбільшою ймовірністю можуть спричинити значні небажані наслідки для конкретної інфраструктури або сектора. По-друге, воно інформує про дії і спрямовує застосування ресурсів для запобігання або пом'якшення наслідків цих загроз і небезпек.

По-третє, управління ризиками дозволяє зацікавленим сторонам визначати пріоритети дій, спрямованих на забезпечення безперервності основних функцій і послуг, а також на підтримку посилених зусиль з реагування та відновлення після інцидентів. Нарешті, управління ризиками полегшує прийняття рішень і визначення пріоритетів серед усіх зацікавлених сторін.

Чинна система управління ризиками критичної інфраструктури США, описана в NIPP 2013, складається з наступних основних принципів.

* + Для ефективного розподілу ресурсів необхідно скоординовано виявляти ризики та управляти ними в рамках спільноти критичної інфраструктури.
  + Партнерства можуть покращити розуміння еволюції ризиків для кібер- та фізичних систем і активів, а також надати дані та перспективи від різних зацікавлених сторін.
  + Розуміння та подолання ризиків, пов'язаних із міжгалузевими залежностями та взаємозалежностями, має важливе значення для посилення загальної позиції CISR.
  + Здобуття знань та зменшення інфраструктурних ризиків вимагає обміну інформацією на всіх рівнях спільноти критичної інфраструктури.
  + Партнерський підхід, що передбачає залучення державних і приватних зацікавлених сторін, визнає унікальні перспективи і порівняльні переваги різноманітної спільноти об'єктів критичної інфраструктури.
  + Регіональні, державні та місцеві партнерства мають вирішальне значення для вироблення спільних поглядів на існуючі прогалини та дії, необхідні для покращення ситуації.
  + Критична інфраструктура виходить за межі національних кордонів і тому потребує двосторонньої, регіональної та міжнародної співпраці, розбудови потенціалу, взаємодопомоги та інших угод про співпрацю, таких як Канадсько-американський план дій щодо критичної інфраструктури.
  + На етапі проектування об'єктів або систем критичної інфраструктури слід розглянути та передбачити заходи з підвищення безпеки та стійкості.

##### Новий підхід:

**Управління міжгалузевими ризиками для критичної інфраструктури**

Ефективне управління ризиками залежить від здатності зацікавлених сторін у сфері критичної інфраструктури взаємодіяти з різними секторами, щоб сприяти спільному розумінню ризиків та інтегрувати широкий спектр заходів для управління ними. У квітні 2019 року CISA опублікувала список з 55 національних критично важливих функцій, які є операціями і послугами державного і приватного секторів, настільки важливими для Сполучених Штатів, що їх порушення, корупція або дисфункція матимуть виснажливий вплив на фізичну та економічну безпеку, а також громадське здоров'я і безпеку.21 Визначення цих критично важливих функцій знаменує собою перехід від попередньої системи управління ризиками, яка зосереджувалася переважно на управлінні ризиками на рівні організації, до підходу на рівні підприємства, який натомість зосереджується на критично важливих кінцевих результатах.

Національна система критичних функцій охоплює ризики та пов'язані з ними залежності, які мають міжгалузевий характер і можуть мати каскадний вплив як всередині секторів, так і між ними. Використання цього функціонального підходу до ризиків дозволяє спільноті критичної інфраструктури посилити позиції CISR у більш стратегічний спосіб, включаючи більш точне визначення цілей і пріоритетів для активів і систем на основі розуміння критично важливих функцій і ключових залежностей і взаємозалежностей.

CISA розподіляє ці функції на чотири сфери: (1) технологічні зв'язки, що забезпечують життєво важливі комунікації, (2) методи розподілу для переміщення товарів, людей та комунальних послуг, (3) процеси управління, пов'язані з національною та громадською безпекою, і (4) ланцюги постачання та послуги, що забезпечують безпеку економіки, такі як водопостачання або житло. Функціональна структура дозволяє CISA краще ідентифікувати ризики, які в іншому випадку могли б залишитися поза увагою, включаючи ризики для ланцюгів постачання, основні проблеми кібербезпеки, такі як атаки з метою крадіжки інтелектуальної власності або маніпулювання системами промислового контролю, а також необхідність міжгалузевої взаємодії для вирішення складних проблем, таких як вразливості, пов'язані з системами визначення місцезнаходження, навігації та синхронізації часу.

##### Хто відповідає за зусилля CISR ?

У США CISR є колективною відповідальністю, яку поділяють власники та оператори критичної інфраструктури, урядові установи та неурядові організації (включаючи галузеві асоціації).

Оскільки компанії приватного сектору володіють і експлуатують більшість об'єктів критично важливої інфраструктури, державно-приватне партнерство має важливе значення для ефективних зусиль у сфері РСБІ. Хоча цей розділ не є вичерпним, він представляє деякі з найважливіших елементів колективної відповідальності за зусилля у сфері РСБІ та державно-приватного партнерства.

Починаючи з урядового рівня, галузеві агентства - це федеральні органи, які відповідають за один або кілька секторів критичної інфраструктури. Наприклад, Міністерство охорони здоров'я та соціальних служб відповідає за охорону здоров'я та сектор громадського здоров'я, а Агентство з охорони навколишнього середовища - за водопостачання та водовідведення. Уряди на рівні штатів, місцевому, племінному і територіальному рівнях відіграють ключову роль у захисті громадської безпеки і добробуту, наданні основних послуг, плануванні та реалізації заходів, що забезпечують безпеку і стійкість критично важливої інфраструктури в межах їхніх юрисдикцій.

З неурядової точки зору, кілька спільнот відіграють ключову роль у підтримці зусиль CISR.26 Внесок академічної спільноти включає дослідження і розробки, тестування і оцінку технологічних досягнень CISR, а також участь в аналізі та управлінні ризиками. Консультативні ради, такі як Національна консультативна рада з питань інфраструктури, надають рекомендації, поради та експертизу державним установам щодо низки ініціатив і політик у сфері CISR.

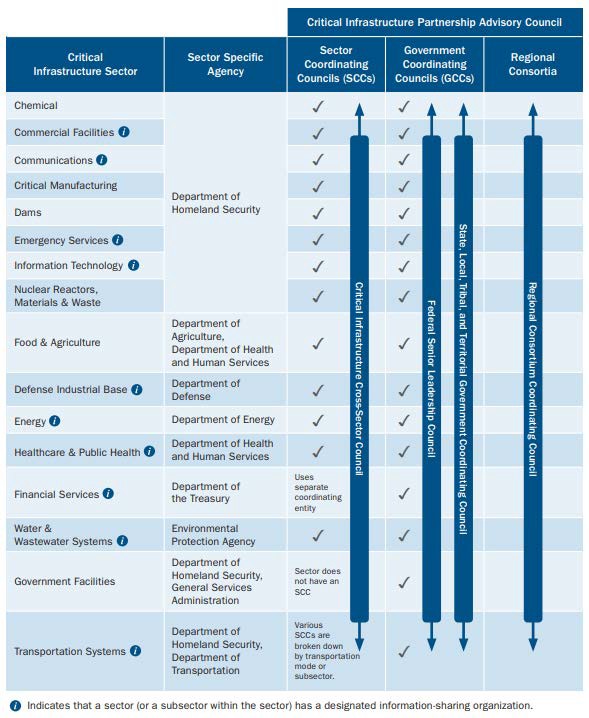
Нарешті, власники та оператори об'єктів критичної інфраструктури з державного та приватного секторів мають важливе значення для сильної позиції CISR. Компанії приватного сектору володіють і експлуатують приблизно 85% фізичної та кіберінфраструктури, тоді як федеральні, державні або місцеві органи влади управляють рештою 15%.27 Оскільки приватні компанії володіють і керують більшістю об'єктів критичної інфраструктури, вони мають унікальну можливість управляти ризиками для своїх систем і активів та розробляти ефективні стратегії для підвищення їхньої безпеки і стійкості.

Мабуть, найсильнішим елементом колективної відповідальності за практику CISR у США є мережа партнерств, починаючи з низкою рад державно-приватного партнерства.28 По-перше, галузеві координаційні ради - це самоврядні групи власників і операторів приватного сектору та представників галузевих асоціацій з 16 секторів критичної інфраструктури. Враховуючи їхній колективний досвід та управління повсякденною діяльністю більшості об'єктів критичної інфраструктури, ці ради надають уряду ключові ідеї та рекомендації щодо планування та реалізації заходів з РСБІ в конкретних секторах.

По-друге, урядові координаційні ради - це галузеві групи, до складу яких входять представники всіх рівнів влади, що слугують державним аналогом рад приватного сектору. Окрім того, що галузеві координаційні ради можуть робити самостійно, ці урядові ради забезпечують координацію між юрисдикціями та між різними державними установами.

По-третє, міжгалузеві ради, які зазвичай складаються з голів або заступників голів кожної з галузевих рад, є майданчиком для вирішення питань і взаємозалежностей, що стосуються кількох секторів критичної інфраструктури, та обміну передовим досвідом. Нарешті, Регіональна координаційна рада консорціуму є національним форумом, який забезпечує структуру та основу для міжсекторальної координації та зусиль CISR на регіональному рівні. Враховуючи важливість державно-приватного партнерства, Консультативна рада з питань партнерства у сфері критичної інфраструктури (CIPAC) забезпечує структуру для сприяння взаємодії між цими різними радами та їхніми різними членами. CIPAC безпосередньо підтримує NIPP 2013 і PPD-21, забезпечуючи форум, на якому державні установи та власники і оператори об'єктів критичної інфраструктури можуть зустрічатися для планування, підтримки і координації зусиль у сфері CISR. Малюнок 10-2 на наступній сторінці ілюструє взаємозв'язок між цими різними радами, федеральними агентствами та 16 секторами критичної інфраструктури.

Хоча програми CISR можуть бути добровільними, регуляторними або їх комбінацією, добровільні програми є найпоширенішими в США, оскільки вони зазвичай найкраще працюють для просування інноваційних концепцій, особливо коли величезна різноманітність у секторі чи галузі обмежує можливість застосування загальних стандартів.30 Регуляторні програми, як правило, є оптимальним вибором для встановлення єдиного стандарту в секторі чи галузі, просування певних галузевих практик або забезпечення того, щоб організації не страждали від несприятливого конкурентного середовища через дотримання вимог. Наприклад, хімічний сектор сприяє підвищенню готовності через добровільні рамки між промисловістю та урядом і частково підпадає під дію регуляторних програм для забезпечення відповідності стандартам.



**Малюнок 10-2. Партнерства: Секторальна та міжсекторальна координація**

(Діаграма DHS)

Ролі та обов'язки зацікавлених сторін у CISR широко варіюються і залежать від кількох важливих факторів, таких як

* + Незалежно від того, чи перебуває об'єкт критичної інфраструктури у державній або приватній власності
  + Нормативно-правові акти, що регулюють діяльність у секторі критичної інфраструктури
  + Галузеві загрози та небезпеки
  + Чи пріоритетними для сектору або регіону є дії щодо захисту інфраструктури, зменшення наслідків або швидкого реагування та відновлення після несприятливих подій

Галузеві асоціації часто відіграють ключову роль у наданні рекомендацій, тоді як в інших секторах можуть існувати нормативні акти, які вимагають від власників та операторів певних дій. У деяких секторах існують державні або національні стандарти проектування для захисту об'єктів та активів від пошкоджень, спричинених такими подіями, як пожежі, пожежі та землетруси. Страхові компанії також можуть встановлювати вимоги безпеки для своїх страхувальників у деяких секторах. Залежно від етапу діяльності у сфері CISR - підготовка до інциденту чи події, запобігання йому, реагування на нього або відновлення після нього - зацікавлені сторони мають різні ролі та обов'язки. Наприклад, хоча служби швидкого реагування, власники та оператори об'єктів критичної інфраструктури, а також регіональні та федеральні ресурси можуть керувати зусиллями з реагування після інциденту, відповідальність за відновлення в добровільній системі покладається на власників та операторів, які найкраще знають інфраструктуру.

Цей короткий розділ демонструє велику цінність взаємодії між приватним сектором і всіма рівнями влади, а також ключову роль рад у зміцненні взаєморозуміння та довіри, сприянні обміну інформацією та практичним обміном. Зокрема, організації, які сприяють плануванню, визначенню пріоритетності ресурсів, проведенню навчань і тренінгів, сприяють підвищенню національної готовності, створенню більш безпечної і стійкої інфраструктури та більш своєчасному реагуванню, що в кінцевому підсумку є бажаними результатами політики CISR.

##### Ефективна CISR: побудована на співпраці та інформації Обмін інформацією

Як зазначено в NIPP 2013, безпека - це процес зменшення ризику для критичної інфраструктури від вторгнень, атак або наслідків природних чи техногенних катастроф шляхом застосування фізичних засобів або оборонних заходів. Аналогічно, стійкість - це здатність готуватися до мінливих умов і адаптуватися до них, в тому числі здатність протистояти і швидко відновлюватися після збоїв, навмисних атак, аварій або природних загроз чи інцидентів. Для того, щоб дійсно зробити критичну інфраструктуру більш безпечною і стійкою, потрібен міцний фундамент співпраці та обміну інформацією.

Ефективна співпраця вимагає кількох життєво важливих елементів: (1) структури і процеси, що дозволяють учасникам вільно спілкуватися без розголошення службової інформації або надання несправедливих переваг, (2) довірливе середовище, в якому зацікавлені сторони обмінюються інформацією, необхідною для зміцнення безпеки і стійкості, і (3) справедливе представництво і залучення відповідних зацікавлених сторін на всіх рівнях влади, промисловості, управління в надзвичайних ситуаціях і безпеки. Аналогічно, для успішного обміну інформацією повинні бути створені механізми або канали для регулярного зв'язку із зацікавленими сторонами в умовах безхмарного неба і на різних етапах інциденту. Обмін інформацією може відбуватися в різних формах, включаючи навчальні заходи, брифінги, оповіщення електронною поштою, конференц-зв'язок, зустрічі в безпечних місцях для обговорення секретних матеріалів про конкретні загрози або небезпеки, а також документи і форуми, які заохочують до обміну набутим досвідом.

CIPAC є основною структурою для сприяння добровільній співпраці та обміну інформацією всередині та між секторами критичної інфраструктури через державно-приватні партнерства та ради, про які йшлося вище. Однак, окрім CIPAC, існує кілька інших програм або майданчиків, які сприяють співпраці та обміну інформацією. У цьому розділі буде представлено дві з них. По-перше, центри обміну інформацією та аналізу дозволяють обмінюватися інформацією між урядом і приватним сектором, використовуючи секторальну модель, що означає, що організації, які належать до певного сектору критичної інфраструктури (або певного сегменту в секторі), об'єднуються для обміну інформацією.34 Для організацій, які не належать до чітко визначеного сектору або мають унікальні інформаційні потреби, більш життєздатним варіантом може бути приєднання до однієї з низки організацій, що займаються обміном інформацією та її аналізом. Зосереджені на зборі, аналізі та поширенні інформації про кіберзагрози серед своїх членів, ці організації пропонують більш гнучкий підхід до самоорганізованого обміну інформацією між певними спільнотами за інтересами, наприклад, юридичні чи бухгалтерські фірми, які підтримують клієнтів у кількох критично важливих секторах інфраструктури.

З огляду на колективний досвід, накопичений з середини 1990-х років, спільнота критичної інфраструктури винесла важливі уроки щодо обміну інформацією, які з часом були інкорпоровані в політику і практику США у сфері РСЗІ. Деякі з цих ключових уроків є наступними (1) залучення відповідних зацікавлених сторін CISR при захисті інформації про власників і операторів,

(2) обмінюватися інформацією про загрози, щоб власники та оператори могли вжити відповідних заходів, (3) заохочувати і практикувати взаємний і багатовекторний обмін інформацією, і (4) застосовувати методи безпечного і більш широкого розповсюдження інформації про загрози, особливо серед компаній приватного сектору, які не мають відповідних допусків до секретної інформації.36 Оскільки цей перелік найкращих практик співпраці та обміну інформацією в США не є вичерпним, корисно ознайомитися з більш ретельним аналізом і обговоренням принципів, рамок і найкращих практик обміну інформацією та розвідданими, викладених у главі 11.

##### Рухаючись вперед: Підтримка успіху CISR у довгостроковій перспективі

Як показав майже 30-річний досвід Сполучених Штатів, створення та реалізація ефективної національної політики у сфері КІСР є одним з найскладніших завдань, які може вирішити країна. Навіть маючи сформовану, сильну політику, культуру і практику КІСР, Сполучені Штати залежать від продовження міцного державно-приватного партнерства, передачі інституційних знань та інвестицій у людський капітал, щоб підтримувати і розвивати цю позицію в майбутньому.

Тренінги, навчання та навчання мають фундаментальне значення для довгострокового успіху національної системи КІСР і повинні охоплювати державних службовців, власників та операторів інфраструктури, служби швидкого реагування, а також широку громадськість, де це доречно. Навчання може зосереджуватися на загальних концепціях, передовому досвіді або конкретних темах і повинно бути доступним у різних формах для забезпечення максимально широкого охоплення, включаючи такі засоби, як курси під керівництвом інструктора, онлайн-курси для самостійного навчання, а також письмові інструкції та робочі посібники. Наприклад, DHS наразі пропонує низку навчальних тем для використання державними установами та організаціями приватного сектору, включаючи найкращі галузеві практики, боротьбу з внутрішніми загрозами або сценаріями "активного стрільця", ризики в ланцюгах поставок, управління та залежність від третіх сторін, промислові системи управління та операційні технології, а також управління інцидентами та реагування на них.

Аналогічно, навчання можуть посилити тренування і освіту, надаючи сценарії для застосування знань і навичок в оперативних умовах, моделюючи реальні загрози і відповідні варіанти реагування, а також зміцнюючи довіру і взаєморозуміння у відносинах між організаціями-учасницями і всередині них. Використання різноманітних моделей - в тому числі тренінгів і семінарів, настільних навчань, репетицій ключових планів, функціональних навчань і повномасштабних навчань - допоможе Сполученим Штатам (або будь-якій іншій країні) підтримувати і розвивати культуру постійного вдосконалення своїх сил і засобів CISR, щоб країна була готова до нинішніх і наступних поколінь загроз для своєї критичної інфраструктури.

Щоб підтримувати успіх у впроваджених програмах CISR, організації повинні просувати програму і періодично проводити її аналіз та оцінку. Коли йдеться про просування програми ВІКІ, незалежно від рівня, на якому вона існує, американський підхід підкреслює важливість інформаційно-пропагандистської роботи та обізнаності. Хоча програми CISR залучають різні зацікавлені сторони - в тому числі компанії приватного сектору, місцеві органи влади та громадян - у різний спосіб, забезпечення розуміння ними ризиків, наявність достатньої інформації та можливість впевнено приймати рішення щодо пом'якшення ризиків та управління ними є ключовими елементами для забезпечення успіху.38 Використання соціальних мереж, онлайн-навчання, публічні ЗМІ та презентації на конференціях - це лише кілька способів охопити широке коло зацікавлених сторін. Корисним прикладом є кампанія DHS "Якщо ти щось бачиш, скажи щось" (If You See Something, Say Something®). Ця кампанія успішно охопила не лише персонал, безпосередньо задіяний в операціях на об'єктах критичної інфраструктури, а й цілі громади, підвищивши їхню обізнаність про ситуацію. Детальний опис цієї ініціативи див. у главі 11.

Аналогічно, періодична оцінка існуючих програм РІСБ є важливою для забезпечення їх адаптації до нових загроз і застосування відповідних заходів для посилення безпеки та стійкості. Оскільки в програмах CISR можуть брати участь представники різних секторів, кількох рівнів влади, а також власники і оператори різних об'єктів або систем, їх також може бути складно ефективно оцінити. Система CISR США визнає і намагається збалансувати два конкуруючі імперативи для оцінки програм. По-перше, програми CISR повинні мати прості вимірювання та проводити їх послідовно впродовж тривалого часу, документувати та порівнювати фактичні результати діяльності в різних секторах і регіонах, а також виявляти недоліки або прогалини в діяльності та вживати заходів для їх усунення. По-друге, вони повинні мати адаптовані показники ефективності, які можуть працювати в будь-якій ситуації звітності. Таким чином, поєднання показників ефективності, спільних для кожного сектору, разом із нюансованими показниками на рівні підсекторів, може допомогти задовольнити ці потреби.

Разом ці кроки з навчання та підготовки кадрів, просування програми серед широких верств населення та розробка відповідних рамок для аналізу та оцінки ефективності сприяють тому, що програми CISR можуть бути успішними в майбутньому, коли з'являться нові загрози, ризики та вразливості. Хоча американська система CISR підтримує ці кроки, вони не є унікальними для американської ситуації. У багатьох аспектах система СІСР ЄС стикається зі схожими викликами, що й у США, і вживає схожих заходів для їх подолання. У той час як політика США у сфері СІСР спирається на координацію між різними рівнями влади і юрисдикціями та міцні партнерські відносини між державним і приватним секторами, ЄС повинен координувати зусилля у сфері СІСР між 27 країнами-членами, кожна з яких має власне поєднання об'єктів критичної інфраструктури, державно-приватних партнерств і питань національного суверенітету. У наступному розділі ми розглянемо політику і практику CISR в ЄС, яка впливає не лише на країни-члени, але й на інші європейські країни, які не є членами ЄС, але розташовані поруч або в межах його кордонів.

### Політика ЄС у сфері CISR Рамки

Серія терористичних атак на початку двадцять першого століття послужила основною мотивацією для розробки політики посилення колективної колективної позиції у сфері СІСР в Європі. У 2004 році ЄС запровадив свої перші спільні заходи у сфері КІСР після вибухів на залізниці в Мадриді, коли терористичні атаки 11 вересня були ще свіжими в пам'яті Заходу і лише за рік до атак на лондонський метрополітен. Детальний аналіз конкретних прикладів мадридського і лондонського терактів на залізниці див. у розділі 7. Ці теракти переконали ЄС, як на інституційному рівні, так і на рівні держав-членів, у важливості встановлення спільних правил, механізмів та інструментів для сприяння кращому врядуванню, управлінню та захисту національної та європейської критичної інфраструктури (NCI та ECI, відповідно).

Мета ЄС - не втручатися в питання національної безпеки, які залишаються виключною відповідальністю кожної країни-члена. Натомість політика ЄС у сфері СЗІБ сприяє зміцненню безпеки та стійкості критично важливих об’єктів.

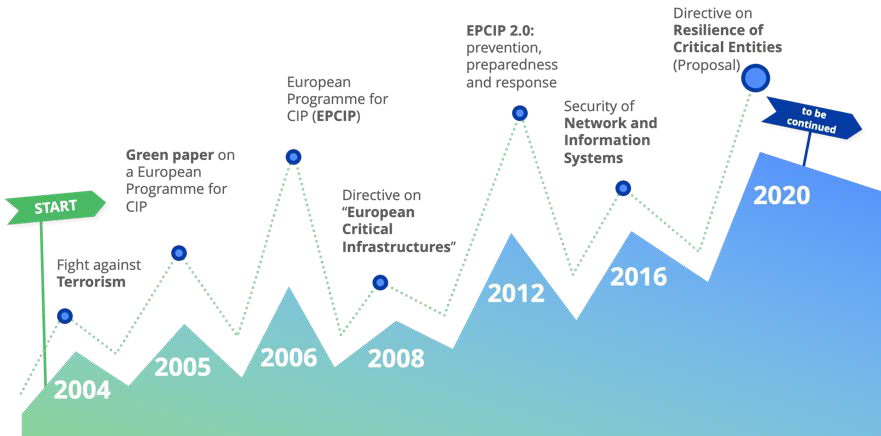
У рамках програми, яка гармонізує зусилля країн-членів ЄС та забезпечує більш зрілу позицію ЄС у сфері РІСБ в цілому, було прийнято рішення про створення спільної інфраструктури. У 2004 році рівень зрілості окремих політик і практик країн-членів ЄС у сфері CISR був дуже нерівномірним. Невелика кількість країн, таких як Франція, Німеччина та Велика Британія, на той час вже мали національну законодавчу базу, в той час як переважна більшість країн-членів покладалася на базовий набір правил або дуже зародкові підходи. Незважаючи на те, що більшість країн мали різні елементи програм CISR у своєму національному законодавстві, вони були дуже фрагментарними і не мали довгострокових цілей, що відповідали б унікальній природі європейської критичної інфраструктури. Наприклад, національні програми CISR не враховували заходи щодо запобігання транскордонним зовнішнім ефектам та ефекту доміно, які є одними з рушійних сил нинішнього підходу ЄС.

Враховуючи ці умови, ЄС заснував Європейську програму захисту критичної інфраструктури (EPCIP) у 2006 році, і з того часу ця програма слугує основою для планування, виконання і консолідації більшості європейських заходів з РСБІ. У відповідь на це інституції ЄС, зокрема Європейська комісія, відіграли ключову роль у створенні умов для загального покращення спроможностей CISR по всій Європі, сприяючи застосуванню підходу, що базується на оцінці ризиків. Використання оцінки і управління ризиками як основи для зусиль у сфері СІСР стало настільки вкоріненим, що ця ментальність впливає навіть на найновіші директиви і регламенти, що стосуються кібербезпеки, такі як регламент ЄС 2019 року, який оновив мандат Агентства ЄС з мережевої та інформаційної безпеки (ENISA) з метою протидії новим ризикам і загрозам у кіберпросторі.

EPCIP підвищила безпеку і стійкість критичної інфраструктури як у державному, так і в приватному секторах, переконавши країни-учасниці створити або оновити свої національні рамки і поліпшити співпрацю з операторами приватного сектору та зацікавленими сторонами критичної інфраструктури в сусідніх державах. Хоча програма EPCIP була успішною, реалізація цілей плану зайняла більше часу, ніж передбачалося спочатку. Одним із прикладів, який ілюструє цей амбітний графік, є зобов'язання ЄС переглянути Директиву 114/08/ЄС, яка закликала держави-члени завершити оцінку з метою визначення та призначення об'єктів або секторів, що є критично важливими для об'єктів, що відносяться до критичної інфраструктури - через чотири роки після набуття нею чинності. Запланований на 2012 рік перегляд так і не відбувся, оскільки деякі країни-члени ЄС лише нещодавно імплементували директиву в своє національне законодавство і все ще потребували завершення оперативної фази ідентифікації, визначення та захисту критичної інфраструктури. Директива 114/08/ЄС залишається чинною, хоча, ймовірно, буде скасована до 2023 року і замінена директивою про стійкість критично важливих об'єктів, яка була введена в дію наприкінці 2020 року.

Гармонізація численних національних підходів до ідентифікації, позначення та захисту як НСІ, так і ВКІ виявилася досить складним завданням. Ця складність пов'язана не лише з різними рівнями готовності та спроможності країн-членів ЄС у сфері кібербезпеки, але й з тим, що кожна з 27 країн-членів сприймає цілі безпеки, визначені ЄС, через призму власної культури, моделей управління, історії, економіки та існуючих пріоритетів. На інституційному рівні ЄС керується принципом субсидіарності, який гарантує, що держави-члени зберігають здатність приймати рішення і діяти в тих сферах, в яких ЄС не має виключної компетенції. Ці обставини глибоко вплинули на те, як кожна країна реагує на спільний порядок денний безпеки, викладений в СЄПБО. Таким чином, прагнення до сильної європейської позиції у сфері СЗПБ створює унікальні виклики у порівнянні зі Сполученими Штатами, зважаючи на суттєву різницю в їхніх моделях управління.

На сьогоднішній день інституції ЄС, національні уряди країн-членів, власники та оператори критичної інфраструктури, наукові кола та дослідницькі центри спільно працюють над підвищенням базового рівня безпеки та стійкості в Європі. Повільний і стабільний прогрес, якого ЄС та його держави-члени досягли в підвищенні обізнаності та розробці більш зрілих політик і практик у сфері КІСІ, відображає менталітет постійного вдосконалення, який спонукав ЄС прийняти низку додаткових заходів і галузевих політик, що виходять за рамки EPCIP. Якщо розглядати ці досягнення в комплексі, вони дають обнадійливу картину прогресу від програми CISR, яка спочатку була зосереджена на захисті та характеризується ізольованими національними підходами до структури, яка надає пріоритет стійкості та стає все більш гармонізованою, скоординованою та всеосяжною серед країн-членів ЄС. На Рисунку 10-3 нижче показано розвиток політики ЄС у сфері СІСР з 2004 року.



**Рисунок 10-3. Етапи розвитку політики ЄС у сфері СІСР (2004-20 рр.)**

У наступних розділах буде надано макрорівневий опис етапів та етапів, зображених на рис. 10-3, які характеризують еволюцію політичної бази ЄС у сфері ШІСР протягом останніх двох десятиліть. У розділі буде зосереджено увагу на основних етапах і не обговорюватимуться галузеві заходи, такі як політика, директиви та регламенти в таких ключових сферах, як безпека портів або цивільна авіація.

##### 2004: Ембріональна стадія, мотивована боротьбою з тероризмом

Терористичні атаки в Мадриді, що відбулися в 2004 році, стали іскрою, яка запалила спільну програму ЄС із захисту критичної інфраструктури (ЗКІ). Ці трагічні події виявили крихкість повсякденного життя європейського суспільства, в тому числі стратегічних активів і критичної інфраструктури, які забезпечують його процвітання і надають життєво важливі послуги щодня. Вони також створили контекст і мотивацію для ЄС на інституційному рівні для реалізації низки ініціатив, які зрештою лягли в основу цілей EPCIP. Кілька важливих повідомлень Європейської Ради та Комісії ЄС протягом 2004 року ілюструють цю нову траєкторію.

З точки зору Ради, два життєво важливі документи відображають суть політики СІП на початковому етапі її становлення і розвитку. По-перше, висновок головуючої країни за підсумками засідання Європейської Ради в Брюсселі 17-18 липня доручив Раді та Комісії "рішуче переслідувати мету побудови спільного простору свободи, безпеки та правосуддя" на найближчі роки і розробити пропозиції щодо нової програми, яка б сприяла досягненню цієї стратегічної мети. Водночас Рада також доручила Комісії співпрацювати з Радою у підготовці загальної стратегії з метою посилення захисту критичної інфраструктури та повної інтеграції боротьби з тероризмом у політику зовнішніх відносин ЄС. Друга важлива подія відбулася через чотири місяці, коли Рада опублікувала оновлений План дій ЄС з боротьби з тероризмом. Основні моменти цього плану наведені нижче.

* + Посилити міжнародні зусилля і волю до боротьби з тероризмом.
  + Зменшити доступ терористів до фінансових та інших економічних ресурсів.
  + Максимізувати спроможність органів ЄС та держав-членів виявляти, розслідувати та переслідувати терористів, запобігати терористичним атакам та долати наслідки терористичних атак.
  + Безпека міжнародних перевезень та забезпечення ефективних систем прикордонного контролю.
  + Усунути фактори, що сприяють підтримці та вербуванню терористів.
  + Спрямувати дії в рамках зовнішніх відносин ЄС на пріоритетні треті країни, які потребують посилення своєї прихильності та спроможності боротися з тероризмом.

Аналогічно, Європейська Комісія опублікувала чотири спеціальні повідомлення до Ради та Європейського Парламенту 20 жовтня 2004 року. Разом ці повідомлення продемонстрували прагнення Комісії вийти за рамки індивідуальних, національних підходів і перейти до більш структурованої, широкої і колективної структури ЄС, яка могла б сприяти своєчасному, адекватному і більш скоординованому реагуванню на всі терористичні сценарії. Разом ці повідомлення представили кілька пріоритетних тем, таких як наявність спільних систем оповіщення для швидкого та ефективного зв'язку з громадянами, а також заходи для покращення обміну інформацією, посилення прозорості та можливості відстежувати фінансові операції терористів.

Можливо, найважливіше з цих повідомлень, "*Захист критичної інфраструктури в боротьбі з тероризмом"*, уточнило визначення критичної інфраструктури, визначило конкретні сектори як критичну інфраструктуру, а також окреслило фундаментальні концепції та вимоги, які стали основою для EPCIP. У цьому повідомленні критична інфраструктура визначається як "фізичні та інформаційно-технологічні об'єкти, мережі, послуги та активи, які, в разі їх порушення або знищення, матимуть серйозний вплив на здоров'я, безпеку, економічний добробут громадян або ефективне функціонування урядів" в різних державах-членах ЄС.48 У повідомленні також визначено дев'ять секторів критичної інфраструктури:

(1) енергетичні установки та мережі, (2) комунікації та інформаційні технології, (3) фінанси, (4) охорона здоров'я, (5) продукти харчування, (6) вода, (7) транспорт, виробництво, зберігання та транспортування небезпечних вантажів, а також

1. основні державні послуги та функції.

Хоча цей початковий перелік критично важливих об'єктів інфраструктури є досить повним, Комісія вирішила, що він потребує подальшого доопрацювання та визначення. Комісія, зокрема, доручила державам-членам визначити, які об'єкти критичної інфраструктури є національними (NCI), а інституціям ЄС - до кінця 2005 року визначити, які з них є європейськими (ECI). Визначення національних та європейських критичних інфраструктур було першим важливим кроком, оскільки це дозволило ЄС - відповідно до принципу субсидіарності та визнання тісного взаємозв'язку і взаємозалежності цих послуг і мереж - зосередити свої зусилля на тих секторах, які найбільше впливають на функціонування критичної інфраструктури в державах-членах ЄС. Для керівництва Інституціям ЄС та державам-членам при призначенні НЦІ та ЄЦІ Комісія рекомендувала враховувати три фактори, викладені нижче.50

* + Масштаб. Географічна територія - міжнародна, національна або місцева, наприклад, - на яку вплинула втрата або недоступність критично важливої інфраструктури.
  + Масштаб. Ступінь впливу або втрати критичної інфраструктури можна оцінити як відсутність, мінімальний, помірний або значний. Корисними критеріями для оцінки потенційних масштабів є вплив на населення, економіку, навколишнє середовище, інші сектори або об'єкти критичної інфраструктури, а також здатність уряду функціонувати належним чином.
  + Вплив часу. В який момент втрата критичної інфраструктури може мати серйозні наслідки: негайно, через кілька днів, тижнів або довше.

Нарешті, ця важлива комунікація обґрунтувала необхідність створення загальноєвропейської програми CIP, що складається зі спільної структури, але з чіткими обов'язками для країн-членів та ЄС відповідно. Посилаючись на неможливість захисту всіх можливих інфраструктур, які держави-члени можуть визнати критично важливими, Комісія стверджувала, що на інституційному рівні ЄС повинен надавати пріоритет захисту інфраструктур, які мають транскордонний вплив, залишаючи всі інші під юрисдикцією держав-членів. Цей акцент на транснаціональних мережах і транскордонних зв'язках був в основі EPCIP з самого початку, і він залишається одним з основних елементів і керівних принципів системи CISR ЄС. З цього приводу Комісія також окреслила три показники, за якими вона буде вимірювати успіх майбутнього ЄІКЗІ: (1) визначення державами-членами критично важливих об'єктів інфраструктури відповідно до пріоритетів ЄІКЗІ та їх інвентаризація, (2) співпраця бізнесу в межах секторів та з урядом з метою обміну інформацією та зменшення ймовірності серйозних інцидентів, що порушують роботу критичної інфраструктури, та (3) спільний підхід ЄС до вирішення питань безпеки критичної інфраструктури через державно-приватне співробітництво. Ці три критерії становлять початкові основи, на яких інституції ЄС і держави-члени заснували EPCIP і стали основою для їхніх інтенсивних дискусій про те, як розвивати програму.

##### 2005: Від боротьби з тероризмом до підходу, орієнтованого на всі загрози

У хронології подій 2005 рік є ключовим, оскільки саме тоді ЄС прийняв підхід, що враховує всі загрози, як основу для СПКІК та його зусиль із захисту критичної інфраструктури від широкого спектру загроз, які можуть порушити роботу або знищити об'єкти та активи. Питання сильної, колективної позиції у сфері КІСІ стало більш помітним у європейському політичному порядку денному, оскільки з'явилися побоювання, що негативні наслідки, спричинені порушенням, виходом з ладу або руйнуванням критично важливої інфраструктури в одній країні-члені, можуть поширитися і на інші. В той час як ключові ініціативи 2004 року запровадили мандат на підготовку стратегії захисту критичної інфраструктури і, зрештою, створення EPCIP, негайні дії Комісії були спрямовані на збір критичної маси зацікавлених сторін, що беруть участь у життєвому циклі критичної інфраструктури. У 2005 році Комісія організувала два семінари, під час яких держави-члени обмінялися інформацією про стан і прогрес своїх програм захисту критичної інфраструктури, а також обмінялися інформацією з представниками приватного сектору про те, як краще визначити відповідні компетенції та сфери інтересів.

В результаті дискусій на цих двох семінарах Комісія опублікувала *Зелену книгу про Європейську програму захисту критичної інфраструктури*, яка містила аналіз численних варіантів політики у відповідь на запит Ради ЄС 2004 року про створення ЄПЗКІ. Як зазначалося на початкових етапах 2004 року, основним завданням СПЗКІ було б досягнення належного рівня захисту всіх об'єктів критичної інфраструктури з пріоритетною увагою до тих об'єктів, порушення роботи яких може призвести до серйозних наслідків у багатьох країнах-членах ЄС. Мабуть, найважливіше, що в документі стверджувалося, що оптимальним способом зміцнення критичної інфраструктури в ЄС є створення спільної структури EPCIP і сприяння обміну найкращими практиками і способами контролю за дотриманням вимог.53

У Зеленій книзі Комісія також включила два важливих елементи майбутнього EPCIP: потенційне визначення КІК та постійний акцент на важливості оцінки транскордонних наслідків. По-перше, в документі збережено визначення критичної інфраструктури як ресурсів, послуг, об'єктів, мереж і активів, порушення або знищення яких матиме серйозний вплив на здоров'я, безпеку, економічний або соціальний добробут.

Що стосується кваліфікаційних областей, які повинні бути визначені як європейська критична інфраструктура, Комісія представила два варіанти для розгляду при визначенні ЄКІ: ті, які в разі порушення або руйнування (1) матимуть серйозний вплив на дві або більше держав-членів або (2) будуть залучені до трьох або більше держав-членів.54 Акцент на транскордонному впливі є основним рушієм майбутньої політики ЄС, оскільки він є частиною визначення та вимогою для визначення та призначення ІКЦ.

Враховуючи транскордонний і взаємозалежний характер критичної інфраструктури в ЄС, Комісія запропонувала, щоб спільна структура EPCIP - хоча вона в першу чергу зосереджена на ЄКІ - також стала основою для того, як держави-члени ідентифікують, призначають і захищають свої НЦІ. Комісія рекомендувала такий підхід "згори донизу" з точки зору надання власникам і операторам критичної інфраструктури більш спрощеної та ефективної структури, а також в інтересах окремих держав-членів і ЄС в цілому. Хоча Комісія запропонувала державам-членам створити національні організації з питань захисту критичної інфраструктури, які могли б застосовувати додаткові, більш жорсткі заходи, ніж ті, що викладені в EPCIP, основне питання полягало в застосуванні принципу субсидіарності. Хоча держави-члени загалом підтримали колективний підхід ЄС, вони також мали сильне бажання зберегти контроль над тими критично важливими об'єктами інфраструктури в межах своїх національних кордонів, які будуть визначені як ЄКІ.

Хоча політичні рекомендації Зеленої книги поклали початок цій суперечці щодо управління певними об'єктами критичної інфраструктури на рівні ЄС і національного контролю над іншими, пізніше *Директива Ради* ЄС *2008* року внесла більше ясності в це питання. З цього питання Директива Ради підтвердила суверенітет держав-членів у визначенні того, які об'єкти критичної інфраструктури, розташовані в межах їхніх національних кордонів, можуть бути визначені як ЄКІ, а також уточнила роль Комісії у підтримці держав-членів у цьому процесі.56 Аналогічно, багато інших елементів і передових практик, представлених у Зеленій книзі, пізніше лягли в основу EPCIP у 2006 році і стали основою для керівних принципів, викладених у *Директиві Ради 2008 року,* яка сьогодні є основним елементом EPCIP.

##### 2006: ЄС офіційно створює EPCIP

Після консультацій і дискусій, ініційованих Зеленою книгою, у 2006 році було опубліковано *Повідомлення Комісії про Європейську програму захисту критичної інфраструктури (*EPCIP), яка офіційно створила структуру для захисту критичної інфраструктури в ЄС, окреслила принципи, процедури та інструменти для її реалізації, а також пообіцяла ухвалити директиву Ради ЄС, яка забезпечить досягнення спільних цілей захисту. Хоча тероризм визнано пріоритетною загрозою для критичної інфраструктури, в основу EPCIP було покладено підхід, що враховує всі загрози. Як основа для захисту критичної інфраструктури на всій території ЄС, EPCIP складається з кількох важливих елементів, які мають спрямовувати майбутні зусилля. У наведеному нижче переліку містяться ключові концепції, викладені в EPCIP:

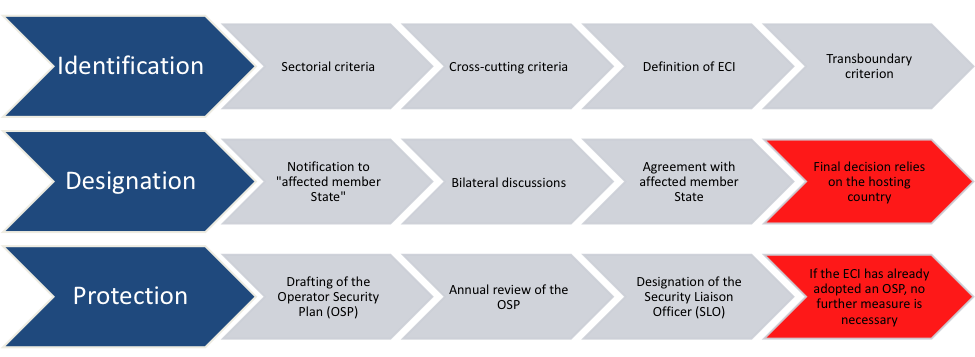
* + Процедура ідентифікації та призначення ОВК
  + Загальний підхід до оцінки та посилення захисту ІВК
  + Підтримка держав-членів у визначенні, призначенні та захисті своїх НСІ
  + Планування на випадок надзвичайних ситуацій для мінімізації наслідків збоїв в роботі ECI або NCI
  + Зовнішній вимір для оцінки впливу ВІП за межами кордонів ЄС
  + Фінансові заходи для забезпечення ініціатив та зусиль, пов'язаних з CIP
  + Кілька заходів для подальшої розробки та впровадження EPCIP

Серед заходів, спрямованих на реалізацію КПКЗІ, було кілька способів обміну передовим досвідом, обміну інформацією та покращення діалогу між відповідними зацікавленими сторонами у сфері КІП. Ці заходи включали створення експертних груп на рівні ЄС, процеси обміну інформацією про КІП з метою зміцнення довіри та захисту конфіденційної інформації, процес виявлення та аналізу взаємозалежностей на основі географії та секторів, а також інформаційну мережу попередження про загрози для критичної інфраструктури (CIWIN). Рамкова програма також включає План дій EPCIP заснований на трьох основних напрямках роботи: (1) забезпечення стратегічної платформи для загальної координації та співпраці між інституціями ЄС та державами-членами через контактну групу ЄС з питань КЗІ, (2) посилення захисту КІК шляхом зменшення їхньої вразливості та (3) підтримка держав-членів у всіх зусиллях, пов'язаних з КІК. Одним з найсильніших елементів плану дій було створення контактної групи з питань КІК ЄС. Ця група, до складу якої увійшли по одному представнику КЗІ від кожної держави-члена, відповідальному за координацію національних питань КЗІ, стала форумом під головуванням Комісії ЄС, на якому держави-члени могли обговорювати питання і приймати рішення один з одним, а також з Радою і Комісією.

Нарешті, EPCIP досягла прогресу у спірному питанні щодо НЦІ, роз'яснивши, що відповідальність за НЦІ лежить на державах-членах та власниках і операторах НЦІ, і що Комісія надаватиме підтримку державам-членам на їхнє прохання. EPCIP закликав кожну державу-члена розробити національну програму захисту НЦІ, засновану на процесі та підході, що застосовуються до ECI, для захисту НЦІ, розташованих на її відповідній національній території. Згідно з EPCIP, національні програми повинні бути спрямовані на: (1) ідентифікація та призначення НЦІ на основі географічного масштабу збитків і тяжкості наслідків, що виникають внаслідок порушення або руйнування цих інфраструктур, (2) визначення географічної та галузевої взаємозалежності, (3) налагодження діалогу з власниками та операторами, відповідальними за захист НЦІ, та (4) розробка планів дій на випадок надзвичайних ситуацій у разі потреби.61 Певною мірою елементи цих національних програм захисту все ще перебувають на стадії розробки, оскільки, згідно з практикою постійного вдосконалення, ЄС прагне консолідувати колективні результати, а потім встановлювати нові цілі та порогові значення для досягнення успіху, якщо це дозволяє загальна зрілість системи захисту.

##### 2008: Ідентифікація, позначення та захист ECI

2008 рік став наступною важливою віхою в політиці ЄС у сфері захисту прав інтелектуальної власності. У цьому році Директива Ради ЄС встановила процедуру ідентифікації та визначення КІК та окреслила загальний підхід до оцінки того, як покращити захист цих КІК. Для більшої ясності, Директива Ради визначила ЄКІ як інфраструктуру, розташовану в певній державі-члені, порушення або руйнування якої матиме значний вплив щонайменше на дві держави-члени з точки зору декількох наскрізних критеріїв, таких як ті, що призводять до від міжгалузевих залежностей від інших секторів або систем інфраструктури. Рисунок 10-4 ілюструє поетапну процедуру ідентифікації та позначення ЕКІ, а також загальний підхід до їх захисту.



**Малюнок 10-4. Процес ідентифікації, призначення та захисту ІВК**

Як і передбачалося, Рада вирішила використати енергетичний і транспортний сектори для імплементації директиви, оскільки ці два сектори пов'язані з найбільш суттєвими зв'язками, взаємозалежностями і транскордонними ефектами - ключовими концепціями, що склалися в ході еволюції політики ЄС у сфері РЕЧВ, починаючи з 2004 року. Що стосується галузевих критеріїв для визначення ЄКІ, то в таблиці 10-1 описано, що директива зосереджується на енергетичному і транспортному секторах та їхніх відповідних підгалузях.

**Таблиця 10-1. Сектори та підсектори ІКЦ**

|  |  |  |
| --- | --- | --- |
| **Сектор** | **Підсектор** | |
| Енергія | Електрика | Інфраструктура та об'єкти для виробництва та передачі електроенергії (постачання електроенергії) |
|  | Олія | Видобуток, переробка, підготовка, зберігання та транспортування нафти трубопроводами |
|  | Газ | Видобуток, переробка, очищення, зберігання та транспортування газу трубопроводами, включаючи LNG-термінали |

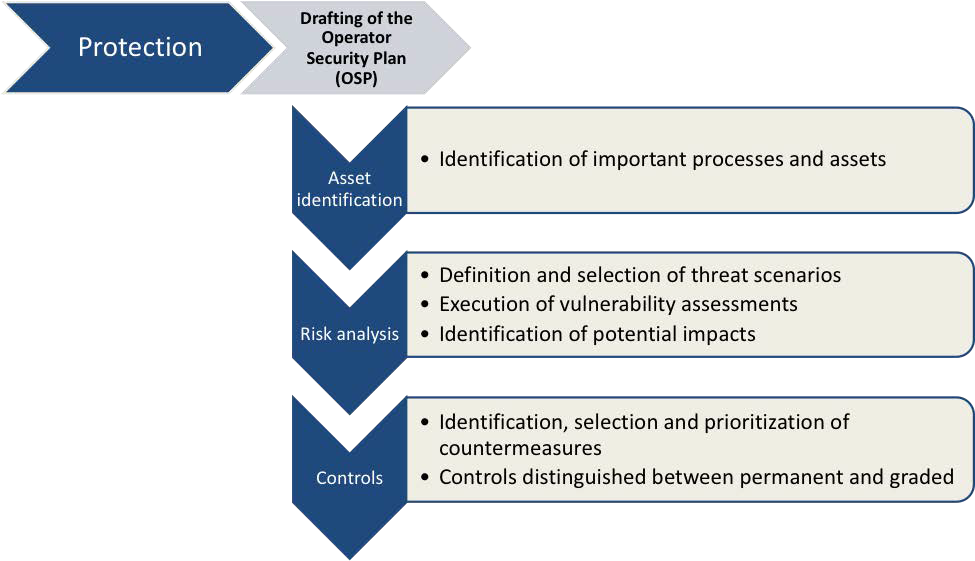
При застосуванні галузевих критеріїв для визначення потенційних ЄКІ Директива передбачає, що держави-члени повинні розглянути альтернативи - ті інфраструктури або послуги, які можуть функціонувати як запасні варіанти (наприклад, альтернативні порти або LNG-термінали) - якщо запропоновані ЄКІ недоступні. Відсутність чітко визначеного критерію для відповідних альтернатив фактично обмежила кількість визначених ЄКІ і слугувала обхідним шляхом для уникнення призначення.

Після секторальних критеріїв, описаних вище, наступним кроком у визначенні ІКЦ є застосування декількох наскрізних критеріїв. Ці критерії включають

(1) жертви - потенційна кількість загиблих або поранених, (2) економічні наслідки, що оцінюються за значущістю потенційних економічних збитків та/або погіршення якості продукції або послуг, включаючи вплив на навколишнє середовище, та (3) вплив на громадськість з точки зору впливу на суспільну довіру, фізичні страждання та порушення повсякденного життя, включаючи втрату основних послуг.64 Нарешті, останні кроки процесу ідентифікації вимагають від держав-членів застосування визначень критичної інфраструктури та ІКІ, а також транскордонного критерію для визначення того, які об'єкти інфраструктури, у разі їх порушення або руйнування, матимуть значний вплив щонайменше на дві держави-члени.

Формальний процес призначення ЄКІ є більш політичним за своєю природою, ніж технічним, оскільки він передбачає співпрацю країн-членів ЄС з державою-членом, на території якої знаходиться ЄКІ, яка приймає остаточне рішення. Така процедура на початковому етапі застосування директиви призвела до того, що до кількох невдалих спроб призначити ОВК. Ці невдачі були зумовлені кількома факторами, зокрема: (1) недостатньою транскордонною співпрацею між державами-членами у сфері КІП, (2) небажанням деяких держав-членів чинити додатковий тиск на власників об'єктів критичної інфраструктури, які вже беруть участь у проектах національної безпеки, та (3) вимогою до призначених ОВК підготувати план безпеки оператора (ПБО) та призначити відповідального за зв'язки з питань безпеки.

Серед цих причин, необхідність належного управління безпекою через ОПБ та призначеного офіцера зв'язку з питань безпеки є важливими елементами процесу захисту КІК. Заснований на ризик-орієнтованому підході, що ґрунтується на базових міжнародних стандартах управління ризиками, OSP складається з трьох ключових етапів: (1) визначення життєво важливих процесів та активів критичної інфраструктури, які забезпечують її функціональність, (2) проведення аналізу ризиків на основі загроз, вразливостей та можливих наслідків, та (3) розробка, визначення пріоритетів та застосування заходів контролю для зменшення ризиків та посилення загального захисту. На Рисунку 10-5 наведено огляд мети та ключових етапів OSP.



**Малюнок 10-5. Підхід до розробки плану безпеки оператора**

##### 2013: EPCIP 2.0 - Новий підхід

З моменту започаткування перших колективних зусиль у сфері КІП підхід ЄС був спрямований на постійний прогрес, спрямований на поступове вдосконалення рамок з плином часу і виокремлення відповідних пріоритетних сфер для ЄС, країн-членів, а також власників і операторів критичної інфраструктури. Хоча перші кроки європейського шляху були спрямовані на боротьбу з тероризмом і попри те, що головними пріоритетами були безпека та захист, відповідні зацікавлені сторони з часом усвідомили важливість таких тем, як комплексний підхід до захисту від усіх загроз, стійкість та кібербезпека. Коли в 2004 році ЄС розпочав реалізацію колективних зусиль у сфері CIP, країни-члени не мали спільної концепції або підходу, а їхні спроможності у сфері CIP були на дуже різних рівнях. Беручи до уваги ці реалії, ЄС скоригував свої зусилля, щоб уникнути перевантаження країн-членів, які оновлювали свої відповідні рамки, стратегії, політику і процедури у сфері КІП - іноді з нуля.

До 2013 року інституції та держави-члени ЄС визнали, що вони спільно досягли прийнятного рівня зрілості критично важливої інфраструктури і повинні розглянути можливість запровадження нових загальноєвропейських політик і цілей для посилення CIP. У цьому дусі постійного вдосконалення серія дискусій на рівні ЄС призвела до того, що ЄС підтримав початкові елементи нової концепції: стійкість критично важливої інфраструктури. Сприйняття стійкості як офіційної концепції вперше з'являється в *Робочому документі персоналу Європейської Комісії (SWD) 318,* який зосереджувався на новому підході і більш практичній імплементації EPCIP. *SWD 318* починався з передумови, що забезпечення високого рівня захисту інфраструктури ЄС і підвищення її стійкості до всіх небезпек і загроз може мінімізувати наслідки втрати послуг по всій Європі.

На додаток до тематичних областей, які раніше розглядалися в рамках EPCIP, *SWD 318 закликав* держави-члени розглянути та інтегрувати запобігання, готовність та реагування у свої національні підходи. Ці три сфери сформували стовпи, на яких Комісія бажає будувати майбутні ініціативи після консолідації досягнень в рамках EPCIP. Ці початкові елементи шляху до підходу, заснованого на стійкості, забезпечили новий спосіб для держав-членів ЄС інтерпретувати та впроваджувати рамки ЄС для критичної інфраструктури. Таким чином, *SWD 318* фактично ознаменував перехід ЄС від захисту критичної інфраструктури (ЗКІ) до безпеки і стійкості (БСІ), оскільки він закликав країни-члени розширити свої зусилля, не обмежуючись лише запобіганням атакам, а й вжити необхідних заходів для підготовки до таких атак і розвитку спроможності реагувати на них і відновлюватися після них якомога швидше і безперешкодно.

##### 

##### 2016: Директива про мережу та інформацію Безпека

Відповідно до свого менталітету безперервного вдосконалення, ЄС зробив великий крок уперед до покращення кібербезпеки критичної інфраструктури у 2016 році, коли Європейський парламент і Рада опублікували свою директиву про мережеву та інформаційну безпеку (NIS). До 2016 року держави-члени вже приділяли увагу питанням кібербезпеки та вживали заходів для зменшення ризиків у кіберсфері на національному рівні. Зрештою, Директива Ради 2008 року передбачала необхідність включення інших секторів, окрім енергетики і транспорту, зокрема, називаючи сектор інформаційно-комунікаційних технологій як одну з таких сфер, що становлять новий інтерес. Подібно до Директиви Ради 2008 року про ЄКІ, головною метою Директиви 2016 року про НІС була гармонізація етапів ідентифікації та призначення, включаючи шлях до досягнення кращої безпеки мережевих та інформаційних систем і забезпечення механізмів для сприяння кваліфікованому та ефективному співробітництву між державами-членами. Директива NIS, однак, внесла кардинальні зміни в розуміння і вдосконалення CISR, оскільки вона запропонувала підхід, зосереджений на основних послугах, а не на критично важливих інфраструктурах. Обґрунтуванням такого рішення було розмежування основ фізичної безпеки (критичної інфраструктури) і кібербезпеки (основних послуг), а також чіткий сигнал про необхідність зосередитися на захисті послуг, які покладаються на мережеві та інформаційні системи.

Як і в Директиві ECI, етап визначення мережевих та інформаційних систем частково ґрунтується на секторальному підході. Якщо Директива ECI охоплювала лише енергетичний і транспортний сектори, то Директива NIS розширила сферу свого впливу, включивши до неї сім секторів: енергетику, транспорт, водопостачання, банківську справу, інфраструктуру фінансових ринків, охорону здоров'я та цифрову інфраструктуру. Розширення кола секторів, включених до Директиви ННД, свідчить про те, наскільки зросла прихильність держав-членів до зусиль у сфері CISR з моменту опублікування Радою Директиви ECI у 2008 році.

Директива NIS спрямована на підвищення загального рівня безпеки мережевих та інформаційних систем в ЄС. На практиці це означає, що мережеві та інформаційні системи можуть протистояти будь-яким діям, які "ставлять під загрозу доступність, автентичність, цілісність або конфіденційність" даних, що зберігаються, передаються або обробляються, а також будь-яких послуг, які ці системи можуть пропонувати або надавати.

Для досягнення цієї мети Директива ННД була спрямована на ці життєво важливі сфери:

1. готовність держав-членів за допомогою таких засобів, як розробка національної стратегії НІБ або створення груп реагування на інциденти комп'ютерної безпеки (CSIRT),
2. посилення співпраці між країнами-членами через Групу співробітництва,

(3) покращення культури безпеки ННД в ЄС, (4) вжиття заходів безпеки для зменшення ризиків для систем і (5) розробка механізму повідомлення національних органів влади про інциденти, пов'язані з безпекою ННД.

З огляду на те, що Директива NIS зосереджена на основних послугах, вона пропонує процедуру визначення того, які суб'єкти відповідають цим кваліфікаційним вимогам. Суб'єктами, які можуть бути визнані операторами основних послуг, є ті, які (1) працюють в одному з семи секторів, зазначених вище, (2) надають послуги, необхідні для забезпечення життєдіяльності суспільства та/або економіки, (3) залежать від мережевих та інформаційних систем для надання цих послуг, і (4) можуть зіткнутися зі значним руйнівним впливом на їхню здатність надавати ці послуги в разі інциденту в сфері безпеки НМД. Для визначення терміну "*значний руйнівний вплив"* директива визначає кілька міжгалузевих факторів, які слід враховувати, наприклад, кількість користувачів, які покладаються на послугу, ступінь залежності інших секторів від послуги, вплив, який інциденти можуть мати на економіку, суспільство або громадську безпеку, а також географічну територію, яка може постраждати від інциденту. Додатковими факторами є частка суб'єкта господарювання на ринку послуг, що надаються, та його важливість для підтримання достатнього рівня послуг, беручи до уваги альтернативні засоби.

Окрім опису процесу ідентифікації та призначення операторів основних послуг, Директива про НСД також встановлює низку вимог щодо безпеки. По-перше, оператори основних послуг повинні вживати належних і пропорційних заходів для управління ризиками, що загрожують їхній безпеці НСД. Далі, оператори повинні вживати заходів для запобігання та мінімізації наслідків інцидентів, що впливають на безпеку НСД, і прагнути забезпечити безперервність надання цих важливих послуг. Нарешті, вони повинні повідомляти компетентний національний орган або CSIRT про інциденти, які серйозно впливають на безперервність їхніх послуг, і надавати інформацію, яка дозволить цим органам визначити будь-які транскордонні впливи, що могли виникнути в результаті. Під час підготовки остаточного тексту Директиви НІС зацікавлені сторони інтенсивно обговорювали вимогу щодо повідомлення про інциденти оскільки вона фактично створила новий вид соціального контракту між операторами та урядами країн-членів. Такий механізм сповіщення не може досягти свого повного потенціалу без співпраці операторів і відповідних заходів реагування, які вживаються урядами для мінімізації наслідків інциденту. Уряди можуть покращити запобігання, готовність і загальну безпеку лише тоді, коли вони мають своєчасний доступ до життєво важливої інформації про інциденти.

Таким чином, Директива про ННД пропонує безпрецедентні зусилля, особливо у створенні Групи співробітництва і мережі CSIRT. Група співробітництва, до складу якої входять представники держав-членів, Комісії, ENISA та інших зацікавлених сторін, слугує для обміну інформацією про безпеку ННД і передовим досвідом, обговорення рівнів спроможності і готовності, а також для надання стратегічних рекомендацій мережі CSIRT.73 Аналогічно, мережа CSIRT, що складається з CSIRT держав-членів і групи реагування на комп'ютерні надзвичайні ситуації ЄС, з Комісією в ролі спостерігача і ENISA в ролі секретаріату, існує для поглиблення довіри між державами-членами і сприяння ефективному оперативному співробітництву в галузі безпеки ННД. Разом ці дві структури вживають ключових заходів для вирішення стратегічних і тактичних питань кібербезпеки, забезпечуючи при цьому швидкий і ефективний обмін інформацією в межах ЄС, а також між державним і приватним секторами.

Оприлюднення Директиви про НІС є першим повним циклом зусиль ЄС, спрямованих на забезпечення фізичної безпеки критично важливих об'єктів інфраструктури та кібербезпеки основних послуг, які вони надають. З 2016 року зобов'язання держав-членів у цих сферах постійно зростають. Прагнення ЄС провести оцінку впливу та громадські консультації щодо Директиви про НІС, незважаючи на її відносно коротке існування, є одним із прикладів, який демонструє цю прихильність. Наступний розділ буде присвячений темі постійного вдосконалення політики і практики ЄС у сфері СІСР.

##### 2020: Пропозиція щодо Директиви про стійкість критично важливих суб'єктів

16 грудня 2020 року має бути включено до знакових дат в історії CISR ЄС, оскільки цього дня Комісія опублікувала дві пропозиції щодо нових директив, пов'язаних з CISR. З виходом цих документів двома пропозиціями ЄС розпочав новий цикл, спрямований на радикальне покращення безпеки у фізичній та кіберсфері критичної інфраструктури та основних послуг, які вони надають. По-перше, Комісія подала до Європейського парламенту і Ради пропозицію скасувати оригінальну Директиву про НІС і прийняти оновлену версію - так звану НІС 2.0 - яка передбачає подальші вдосконалення, особливо в частині сприяння співпраці.76 По-друге, пропозиція щодо директиви про стійкість критично важливих об'єктів передбачає зміщення акценту на фізичну безпеку, яка все ще регулюється Директивою 2008 р., а тому вважається застарілою і надто обмеженою за обсягом, оскільки охоплює лише енергетичний і транспортний сектори.77 Цією подвійною пропозицією Комісія прагнула гармонізувати свої зусилля у сферах фізичної та кібербезпеки, а також у процесах ідентифікації та призначення основних послуг і критично важливих установ, які раніше регулювалися двома різними директивами.

Ця гармонізація також є важливим кроком вперед у вдосконаленні обсягу і характеру політичної бази ЄС у сфері кібербезпеки, з новим акцентом на посиленні безпеки і стійкості, але все ще заснованим на міжсекторальній і транскордонній взаємозалежності. Пропонуючи директиву про стійкість, Комісія мала намір запропонувати рамки, що охоплюють усі загрози, щоб підвищити здатність критично важливих організацій "запобігати, протистояти, поглинати і відновлюватися після руйнівних інцидентів, незалежно від того, чи вони спричинені стихійними лихами, аваріями, тероризмом, внутрішніми загрозами або надзвичайними ситуаціями у сфері охорони здоров'я", як, наприклад, пандемія COVID-19, яка кинула виклик ЄС і решті світу з початку 2020 року. Пропозиція щодо директиви про стійкість розширить галузеву сферу застосування до 10 секторів: енергетика, транспорт, банківська справа, інфраструктура фінансового ринку, охорона здоров'я, питна вода, водовідведення, цифрова інфраструктура, державне управління та космос.

З метою посилення колективної позиції ЄС у сфері кібербезпеки, пропозиція включає конкретні заходи для покращення організації та нагляду на рівні ЄС, а також вимоги до держав-членів та операторів критично важливих об'єктів з метою мінімізації вразливостей та забезпечення безперебійного надання послуг. Зокрема, пропозиція передбачає вимагатиме від держав-членів мати стратегію забезпечення стійкості критично важливих установ, проводити національну оцінку ризиків та визначати критичні установи на основі цієї оцінки ризиків. Пропозиція щодо забезпечення стійкості також зобов'язуватиме критично важливі установи проводити власні оцінки ризиків, вживати відповідних технічних та організаційних заходів для підвищення стійкості та повідомляти про будь-які інциденти, що можуть призвести до порушення роботи, відповідним національним органам влади. На рівні ЄС пропозиція передбачає створення механізмів нагляду, включаючи консультативні місії, організовані Комісією, за критично важливими підприємствами, що надають послуги щонайменше третині країн-членів ЄС або в них. Комісія запропонує різні форми підтримки державам-членам і критично важливим підприємствам, такі як огляд ризиків на рівні ЄС, найкращі практики, методології, транскордонні навчальні заходи та вправи для оцінки стійкості критично важливих підприємств. Нарешті, пропозиція передбачає створення Групи з питань стійкості критично важливих об'єктів, що складатиметься з експертів, для сприяння регулярному транскордонному співробітництву з метою імплементації директиви.

Майбутнє політичної бази ЄС у сфері кібербезпеки перебуває на вирішальному етапі, оскільки Європейський парламент і Рада, ймовірно, видадуть ці дві директиви до 2023 року після обговорення, переговорів і оновлення формулювань, викладених у пропозиціях. Початкові ознаки вказують на те, що в процесі переговорів буде збережено більшість положень, передбачених у пропозиціях, оскільки ЄС явно потребує прийняття цих нових заходів для вирішення поточних і майбутніх викликів, пов'язаних із критичною інфраструктурою, основними послугами та критично важливими суб'єктами.

##### Майбутнє ЄС: Постійне вдосконалення та адаптація до нових загроз

Із запровадженням NIS 2.0 та директив щодо стійкості критично важливих об'єктів у 2020 році - і їх очікуваним прийняттям та імплементацією в найближчому майбутньому - ЄС створить інноваційну, всеосяжну та інклюзивну структуру, яка підготує країни-члени до викликів, що постануть перед їхньою критично важливою інфраструктурою в найближчі роки. Вся робота, спрямована на підвищення безпеки і стійкості до фізичних і кіберзагроз, також прокладе шлях до того, щоб допомогти ЄС і його країнам-членам підготуватися до гібридних загроз і реагувати на них, які становлять значний, складний і тривожний виклик для ЄС. Огляд кожного з цих типів загроз див. у розділах 2-4.

Починаючи з 2016 року, ЄС дедалі активніше намагається зрозуміти природу гібридних загроз і вжити заходів для кращої підготовки до них та протидії їм. Зокрема, Комісія опублікувала дві відповідні пропозиції: (1) *Спільну рамкову програму з протидії гібридним загрозам* у 2016 році та (2) *Спільне повідомлення* 2018 року *про підвищення стійкості та зміцнення Спроможності протистояти гібридним загрозам*. Нещодавно, в листопаді 2020 року, Об'єднаний дослідницький центр Європейської комісії спільно з Європейським центром передового досвіду з протидії гібридним загрозам опублікував концептуальні рамки, які описують компоненти гібридних загроз з точки зору суб'єктів загроз, їхніх цілей і інструментів, а також сфер, які вони намагаються скомпрометувати, і чітких етапів дій, спрямованих на ці сфери. Ця концептуальна основа гібридних загроз є ще одним стовпом нещодавніх нововведень, включених до системи CISR ЄС, і вже дозволяє країнам-членам робити перші кроки для протидії загрозам, що постійно змінюються.

Хронологія подій, описаних у цьому розділі про ЄС, дає загальне уявлення про еволюцію та поточний стан європейської політики і практики у сфері КІСР. Відповідно до свого менталітету постійного вдосконалення, ЄС з 2004 року зосередився на адаптації до нових загроз, впроваджуючи поступові зміни і надаючи державам-членам достатньо часу для прийняття і впровадження кожного вдосконалення на своїх національних рівнях. Підхід ЄС забезпечив безпечне середовище, в якому кожна зацікавлена сторона у сфері критичної інфраструктури має можливість обговорювати найважливіші питання, обмінюватися інформацією, знайомитися з зусиллями інших країн у сфері КІСБ та в інших секторах, отримувати доступ до різних передових практик і, за необхідності, звертатися за двосторонньою або багатосторонньою підтримкою. Таким чином, адаптивна і всеосяжна система CISR ЄС ставить ЄС і його держави-члени в сильну позицію для стримування, запобігання, зменшення наслідків, реагування і відновлення після широкого спектру загроз для критично важливих інфраструктур і об'єктів у найближчі роки.

# - 11 -

## Обмін інформацією та розвідданими

Кріс Андерсон та Реймонд Мей

Обмін інформацією та розвідданими має важливе значення для успіху будь-яких зусиль з безпеки і стійкості критичної інфраструктури (CISR) в рамках Організації Північноатлантичного договору, оскільки жодна організація не володіє всією інформацією, необхідною для повного розуміння:

* + Загрози - включаючи наміри, можливості, тактику, методи і процедури (ТТП) - з боку національних держав і недержавних суб'єктів, таких як терористи і злочинці
  + Вразливість інфраструктурних систем до цих загроз
  + Далекосяжні первинні та каскадні наслідки деградації або втрати критично важливої інфраструктури, включаючи залежності та взаємозалежності між інфраструктурними об'єктами та секторами
  + Найефективніші стратегії захисту від постійно еволюціонуючих ПТЗ противника

З огляду на складність і мінливість інформації, необхідної для просування CISR, надзвичайно важливо, щоб ключові зацікавлені сторони інфраструктури намагалися обмінюватися інформацією для повного розуміння комплексних інфраструктурних ризиків, щоб вони могли визначити найбільш ефективні та дієві засоби для пом'якшення цих небезпек. Цей процес передбачає розбудову довіри, спільні та практичні методи комунікації, а також структурований, багатовимірний обмін інформацією.

### Обмін інформацією Фундаментальні Концепції

Ефективні програми обміну інформацією мають бути адаптовані до правового, культурного та соціального середовища, в якому вони працюють. Не існує універсального підходу до обміну інформацією, але успішні програми повинні враховувати наступні основні концепції обміну інформацією: партнерство з доданою вартістю, важливість довірчих відносин, багатовекторний обмін інформацією та своєчасне надання інформації тим, хто може на неї вплинути. У цьому розділі ми більш детально розглянемо кожну з цих основних концепцій, а на завершення обговоримо фактори, які можуть перешкоджати або заважати обміну інформацією, і які успішні програми обміну інформацією повинні брати до уваги і намагатися подолати.

##### Додана вартість Партнерства

Мабуть, найбільш важливою концепцією у створенні та підтримці програми обміну інформацією є те, що вона надає інформацію, яка має цінність для всіх учасників. Для того, щоб зробити необхідні інвестиції в персонал і процеси, а також для того, щоб члени групи обміну інформацією були готові ділитися потенційно конфіденційною інформацією, вони повинні бути зацікавлені в продовженні участі, як правило, гарантуючи, що всі учасники отримають користь від обміну інформацією. Незбалансовані механізми обміну інформацією можуть призвести до втрати учасників, які не бачать цінності в інвестиціях, якщо вони не отримують корисної інформації. Це не означає, що взаємна вигода завжди збалансована в короткостроковій чи навіть довгостроковій перспективі, але без чіткої причини для всіх учасників продовжувати участь у програмі, вона з часом занепадає.

У найбільш ефективній формі партнерства з доданою вартістю всі учасники розробляють і обмінюються інформацією в межах своєї основної галузі знань, отримуючи при цьому вигоду від досвіду інших. Уряди досягають успіху в зборі і підтримці великих масивів статистичної або геопросторової інформації. Військові, правоохоронні і розвідувальні організації часто мають найкраще (або єдине) уявлення про наміри і планування супротивника, в той час як оператори інфраструктури мають глибоке розуміння вразливостей і взаємозалежностей, що лежать в основі системних ризиків для складних систем і процесів, які вони розробляють і експлуатують.

***Розвідка, інформація та дані***

Хоча збір розвідданих та аналіз інформації виходять за рамки цієї глави, є два ключових поняття, важливих для системи обміну інформацією. Першим фактором є оцінка достовірності інформації, що підлягає обміну. Особливо при створенні розвідувальних продуктів про потенційних супротивників, інформацію може бути важко отримати, а супротивник може намагатися навмисно ввести в оману такі зусилля. Другий фактор - це ступінь, до якого необроблені дані повинні бути проаналізовані і контекстуалізовані в інформацію і розвідувальні дані для прийняття рішень і дій.

Ці концепції мають важливе значення для обміну інформацією в критично важливих аспектах. Надійні мережі обміну інформацією можуть значно полегшити як оцінку достовірності, так і контекстуальний аналіз необроблених даних. Але, мабуть, найголовніше - точне інформування про достовірність і ступінь аналізу в спільному продукті має важливе значення для побудови і підтримки довіри одержувачів; можуть бути вагомі причини ділитися інформацією, яка не викликає довіри, або необробленою інформацією, але вона завжди повинна бути передана саме так, як вона є.

##### Важливість довірчих відносин

Незалежно від того, чи йдеться про розмову віч-на-віч, чи про велику, керовану процесами організацію, готовність ділитися інформацією пов'язана з рівнем довіри між учасниками. Інформація, яка має цінність, майже завжди за своєю природою є чутливою для власника цієї інформації. Обмін інформацією може поставити під загрозу джерела та методи, за допомогою яких вона була розроблена, виявити сильні або слабкі сторони критично важливого об'єкта або процесу, або дозволити зловживати інформацією для створення або підриву конкурентних переваг. Щоб подолати ці чутливі моменти, учасники обміну інформацією повинні вірити, що одержувачі будуть використовувати інформацію за призначенням і захистять її від подальшого розголошення або неправомірного використання.

Мабуть, найпершим кроком у розбудові довіри є завчасне налагодження відносин. Кола обміну інформацією повинні бути створені в стабільних умовах, щоб учасники та організації могли познайомитися один з одним, встановити групові норми, розробити, відшліфувати та вкорінити основні процеси. Налагодження цих відносин на ранньому етапі дає час для визначення та залучення всіх необхідних учасників у кожній групі з обміну інформацією. Після визначення учасників можна розробити механізми для обміну контактною інформацією, щоб можна було обмінюватися інформацією електронною поштою, на онлайн-форумах і під час групових зустрічей (особистих або віртуальних), залежно від складу учасників і типу інформації, якою обмінюються. Регулярна взаємодія також гарантує, що учасники вивчають професійний жаргон один одного і сприяють швидкому обміну інформацією про місію в більш пізніх ситуаціях, коли час може мати вирішальне значення. Нарешті, така взаємодія дозволяє встановити процеси, шаблони і правила обміну інформацією, які є критично важливими для швидкого, ефективного і безпечного обміну інформацією.

##### Багатовекторний Поширення

Для повної реалізації двох попередніх концепцій режим обміну інформацією повинен дозволяти і навіть заохочувати різноспрямований обмін інформацією. Хоча в будь-якій схемі обміну інформацією можуть бути випадки, коли необхідний односторонній обмін інформацією - наприклад, уряди можуть зберігати військову, розвідувальну або правоохоронну інформацію, яка не є суспільним надбанням, але є життєво важливою для власників і операторів інфраструктури - програми, які є ефективними в довгостроковій перспективі, включають двосторонній обмін інформацією. Обмін інформацією не може обмежуватися лише тим, що уряд "підштовхує" промисловість або програми, які покладаються виключно на промисловість у наданні інформації - наприклад, про вразливості інфраструктури або підозрілу діяльність, пов'язану з їхніми об'єктами або системами, - державним партнерам, не отримуючи натомість цінної інформації.

Багатовекторний обмін виходить навіть далі, ніж просто двосторонній обмін між урядом і промисловістю. На базовому рівні уряд повинен визначити, як він обмінюється інформацією всередині себе (відомство до відомства), а також між різними юрисдикціями, від національного до регіонального та місцевого рівнів. Аналогічно, промисловість повинна вивчити наявні методи обміну інформацією про безпеку між різними компаніями і між організаціями всередині цих компаній. Такий багатовекторний обмін часто відбувається неформально в колах кібербезпеки, коли фахівці з інформаційної безпеки використовують свої особисті мережі, а також на місцевому рівні серед фахівців з фізичної безпеки. Однак, якими б важливими не були ці методи, на них не слід покладатися як на заміну більш повторюваним, формальним і стійким процесам. Комерційні постачальники інформації про загрози і ризики, особливо в кіберпросторі, відіграють все більш важливу роль у забезпеченні достатньої поінформованості операторів критичної інфраструктури про загрози, що змінюються.

Для того, щоб повністю уможливити багатовекторний обмін, учасники повинні визначити і дотримуватися норм щодо того, як спільна інформація може бути використана, перепакована, об'єднана з іншими елементами і поширена без порушення будь-яких обмежень на обмін з боку первісного постачальника інформації.

##### Своєчасна інформація для тих, хто може Діяти

Незалежно від того, чи призначена вона для охоронця на воротах об'єкта перед потенційною терористичною атакою, адміністратора брандмауера, відповідального за блокування потенційно небезпечного інтернет-трафіку, або для служби швидкого реагування, яка може відстежити підозрілу особу, що веде можливе спостереження за об'єктами критичної інфраструктури, інформація, особливо оперативна антитерористична інформація, часто є надзвичайно важливою в умовах дефіциту часу. Враховуючи цей часовий тиск, вкрай важливо постійно розвивати та вдосконалювати процеси, щоб прискорити отримання інформації та надати дієву інформацію тим, хто буде її використовувати.

Прискорення надходження інформації вимагає ретельного аналізу кожного кроку в процесі розвідки та обміну інформацією. Загальна схема оцінки комплексного процесу розвідки включає постановку завдань, збір, обробку, використання і поширення інформації. Хоча перші чотири етапи цього процесу також можуть запропонувати значні шанси скоротити час, необхідний для отримання інформації одержувачами, ця глава в першу чергу зосереджена на поширенні інформації. У процесі розповсюдження інформації організації повинні розробити процедури, які підштовхують владу до того, щоб оприлюднювати інформацію на якомога нижчому рівні. Для інформації, яка є дуже чутливою до часу, на цьому етапі може знадобитися надання повноважень на розкриття інформації цілодобовому оперативному центру, який працює 24 години на добу, сім днів на тиждень. Інформація, якою обмінюються на постійній основі, повинна мати заздалегідь встановлені шаблони і формати, відомі заздалегідь, щоб ті, хто надсилає інформацію, і ті, хто її отримує, могли робити це якнайшвидше і найефективніше. В рамках обміну інформацією з питань кібербезпеки ці шаблони повинні також включати машинозчитувані формати. Нарешті, учасники обміну інформацією повинні розробити спільний синтаксис і лексику, щоб полегшити швидке спілкування і взаєморозуміння.

Хоча швидка передача інформації є важливою, це лише частина рішення. Організація, яка отримує інформацію, повинна розробити процедури для подальшої передачі інформації тим членам групи, які будуть її використовувати (якщо первісні одержувачі не є тими, хто буде діяти на основі цієї інформації). Водночас, організації-передавачі повинні бути обережними, щоб не засекретити або іншим чином не обмежити можливості подальшого обміну та поширення інформації. Наприклад, передача засекреченої інформації або інформації з обмеженим доступом єдиній контактній особі в компанії може мати обмежену цінність, якщо ця інформація не зможе потрапити до тих, хто в кінцевому підсумку буде вживати заходів. При обміні інформацією з приватним сектором це часто означає, що критична інформація повинна мати найнижчий можливий рівень засекреченості або, як мінімум, "лінію розриву", яка передає найсуттєвіші елементи інформації з найменшими обмеженнями. Основи "блакитного неба зазначені вище, підвищують як швидкість обміну інформацією, так і стандартизовані процедури, які забезпечують передачу інформації в зручному для використання форматі потрібним людям на об'єкті критичної інфраструктури, які можуть її використати.

##### Обмін інформацією Стримуючі фактори

Будь-яке всебічне обговорення обміну інформацією повинно також враховувати фактори, які стримують або перешкоджають обміну інформацією. Важливо розуміти ці природні стримуючі фактори і створювати програми і політику - в тому числі законодавчі або нормативні акти, де це необхідно - які мінімізують їхній вплив на середовище обміну інформацією.

Приватний сектор має кілька потенційних перешкод для обміну інформацією. Загалом, промисловість може не бажати добровільно ділитися інформацією з тим самим урядом, який відповідає за регулювання галузі, через побоювання, що обмін інформацією може призвести до примусових дій або заохочення до додаткового регулювання. Антимонопольне законодавство або законодавство у сфері конкуренції може перешкоджати обміну певною інформацією з колегами та конкурентами або навіть зустрічам з групою конкурентів у тому ж секторі. Промисловість може мати побоювання щодо добровільного розкриття інформації, яка потім стає публічною і може створити або посилити ризик відповідальності через оприлюднення непублічної інформації, яка згодом буде використана в судовому процесі проти компанії, що її оприлюднила. У деяких випадках законодавство або окремі положення контракту можуть вимагати, щоб певна інформація залишалася конфіденційною, зокрема, інформація про власну мережу клієнта або інформація, пов'язана зі станом здоров'я. Промисловість може неохоче ділитися інформацією про ризики, які сприймаються іншими компаніями, наприклад, про проблеми безпеки ланцюга постачання, через відповідальність за наклеп. Для компаній, акції яких котируються на біржі, законодавство про цінні папери може обмежувати публічне розкриття суттєвої інформації про діяльність або ризики компанії. Нарешті, галузь може бути занепокоєна тим, що комерційна інформація потрапить до рук конкурентів, тим самим зашкодивши позиції компанії на ринку.

Урядові партнери також мають перешкоди в обміні інформацією. Інформація, якою володіють спецслужби про національні державні або терористичні загрози, часто є суворо засекреченою або іншим чином суворо контролюється, а покарання за розголошення такої інформації є суворим, оскільки вона може викрити джерела і методи, які використовувалися для збору інформації. Федеральні та місцеві правоохоронні органи також занепокоєні тим, що компрометація джерел та інформації, яка може бути важливою для поточних розслідувань, призводить до небажання ділитися своєчасною інформацією та створює розрив між правоохоронними органами та приватним сектором. Щоб виправити ці недоліки, слід зосередити зусилля на побудові довірчих відносин і налагодженні такі механізми, як "лінії розриву", для обміну інформацією та розвідувальними даними без шкоди для поточних розслідувань, ефективності правоохоронних органів і традицій розвідувального співтовариства. Уряди часто мають обмеження щодо визначення особи чи компанії як загрози без належної правової процедури. Додаткові перешкоди для обміну інформацією між урядами можуть бути дуже різними:

(1) державні органи можуть бути обмежені законом або нормативними актами в обміні певними видами інформації; (2) органи можуть неохоче ділитися інформацією, яка може негативно відобразитися на їхній діяльності або можливостях; і

(3) потенційні політичні наслідки або наслідки для зв'язків з громадськістю можуть змусити деякі державні установи вагатися, чи ділитися потенційно суперечливою інформацією.

### Обмін інформацією Підкатегорії

Хоча ці основоположні концепції застосовуються майже універсально, існують деякі специфічні міркування, коли йдеться про певні типи обміну інформацією. У цьому розділі ми окремо розглянемо більш вузько визначені підтипи обміну інформацією, оскільки вони можуть мати певні переваги для учасників або можуть підходити для конкретних типів програм обміну інформацією.

##### Кібербезпека

Захист від кіберзагроз є одним з найяскравіших прикладів корисного багатовекторного обміну інформацією. У промисловості багато компаній вже обмінюються інформацією з іншими компаніями в тому ж секторі і навіть між секторами. Мережеві захисники спілкуються з колегами з інших компаній, щоб поділитися спостереженнями про нові загрози і пов'язані з ними ТТП. Приватні компанії збирають критично важливу інформацію про нові вразливості та способи захисту від кібератак, що тривають, і часто відкрито діляться цією інформацією, намагаючись довести свою добросовісність і зміцнити своє місце на ринку послуг із запобігання та пом'якшення наслідків кіберзагроз.

Ключовим елементом обміну кіберінформацією є ідентифікація цифрових підписів зловмисних дій та інші способи виявлення зловмисників. Оскільки кіберзагрози рухаються буквально зі швидкістю світла, обмін цими даними між машинами є важливим для концепції отримання своєчасної інформації тими, хто може діяти. Інформація про поширені або нещодавно виявлені вразливості часто має вирішальне значення, особливо якщо вона супроводжується способами усунення або пом'якшення вразливості. Коли щойно виявлене шкідливе програмне забезпечення спостерігається в природних умовах, оператори критичної інфраструктури також отримують вигоду від обміну інформацією про коригувальні заходи реагування, які є ефективними проти конкретного кіберсупротивника або набору втручань, і є важливими учасниками цього процесу.

Нарешті, надійні режими обміну інформацією забезпечать готовність і здатність компаній приватного сектору, особливо в секторах зв'язку та інформаційних технологій, ділитися з урядом своєю ситуативною обізнаністю про кіберсередовище таким чином, щоб усі сторони могли швидко спостерігати, ідентифікувати, співвідносити і протидіяти діям супротивника. Компанії з секторів інформаційних технологій і зв'язку часто мають найкраще уявлення про кібернетичну екосистему з широкого кола питань.

##### Фізична Безпека

Організації, відповідальні за захист від терористичних атак та інших фізичних загроз, також виграють від активного обміну інформацією. У міру того, як ТТП супротивника розвиваються, захисникам інфраструктури життєво важливо вивчати ці нові загрози, а потім розробляти найбільш ефективні способи їхнього пом'якшення. Подібні типи об'єктів часто виграють від обміну найкращими практиками щодо захисних заходів і бенчмаркінгу - своєрідного порівняння, яке може допомогти визначити, де стан фізичної безпеки об'єкта не такий сильний, як у його аналогів. Забезпечення базового рівня захисту допомагає об'єктам не стати найлегшою або найслабшою мішенню. Оскільки багато операторів об'єктів критичної інфраструктури постійно спостерігають за територіями навколо своїх об'єктів, їх пильне спостереження та звітування можуть допомогти виявити підозрілу діяльність або планування атаки перед її початком. Повідомлення про підозрілу діяльність (наприклад, фотографування захисних споруд по периметру або прольоти безпілотних літальних апаратів) може свідчити про постійне спостереження або планування. Регулярний обмін інформацією може допомогти виявити групу противника, яка діє в регіоні і веде спостереження за кількома об'єктами з метою вибору цілі. Військові, правоохоронні або розвідувальні служби можуть мати найкращу інформацію про ТТП потенційних супротивників завдяки спостереженню за полем бою, груповому проникненню або перехопленню інформації про діяльність з планування. Обмін цією інформацією з власниками і операторами критичної інфраструктури дозволить їм зрозуміти потенційні наслідки нових методів нападу і розробити відповідні контрзаходи.

##### Аналіз ризиків та їх мінімізація

Партнерство між урядом і промисловістю має важливе значення для розуміння ризиків для критично важливої інфраструктури та обґрунтування державних і приватних інвестицій, спрямованих на зменшення цих ризиків. Без галузевих знань державним планувальникам може бути надзвичайно складно зрозуміти вразливість надскладних інфраструктурних об'єктів або наслідки різноманітних атак на них, як у фізичній, так і в кіберпросторі. Ще складніше отримати повне уявлення про міжгалузеві залежності та взаємозалежності - критичні зв'язки, які можуть збільшити або зменшити ризики. Огляд природи взаємозалежностей та використання системного підходу для підвищення стійкості див. у главі 12. Належний обмін інформацією може зробити значний внесок у взаємне розуміння спільних вразливостей, що може слугувати для визначення сфер для дій галузі, урядових досліджень і розробок або інших заходів з пом'якшення наслідків. Нещодавні події привернули увагу до ризиків у ланцюгах постачання як фізичного обладнання, так і критично важливого програмного забезпечення. Спільний аналіз і набори даних, проведений урядом і промисловістю, можуть допомогти виявити потенційні ризики як у фізичних, так і в кібер-ланцюгах постачання, пов'язані зі складними міжгалузевими відносинами, фізичними або віртуальними "вузькими місцями" і концентрацією критично важливих промислових джерел в одного постачальника, країні або регіоні.

### Режими обміну інформацією та програми

У цьому розділі описано низку існуючих режимів обміну інформацією, які наразі діють у США та Європі. Багато з цих програм покликані максимізувати переваги або усунути перешкоди, описані раніше в цьому розділі. Хоча деякі з цих програм перекривають сфери відповідальності - оскільки обмін інформацією може сильно залежати від побудови відносин - може бути корисно мати ряд програм, які забезпечують "глибокий захист" і допомагають забезпечити широке розповсюдження важливої інформації.

У Сполучених Штатах Америки Міністерство внутрішньої безпеки (МНБ) відповідає за координацію зусиль у сфері СІСР.1 Працюючи з іншими федеральними відомствами, МНБ реалізує низку програм та ініціатив, спрямованих на побудову міцного державно-приватного добровільного партнерства, заснованого на обміні інформацією. У цьому розділі буде коротко представлено чотири типи таких програм, першою з яких є Консультативна рада з питань партнерства у сфері критичної інфраструктури (CIPAC). CIPAC - це правова база, яка забезпечує взаємодію між урядом і власниками та операторами об'єктів критичної інфраструктури, дає змогу представникам галузі розробляти консенсусні рекомендації та ділитися ними з федеральним урядом, а також сприяє обговоренню питань безпеки та стійкості між урядом і галуззю в непублічних заходах.2 У країнах, де антимонопольні обмеження або вимоги до розкриття інформації обмежують можливості уряду проводити непублічні зустрічі з приватними компаніями індивідуально або в групі, така структура, як CIPAC, може сприяти відвертим дискусіям між урядом і промисловістю, необхідним для вирішення проблем безпеки та стійкості.

Другою програмою обміну інформацією є Програма захисту інформації про об'єкти критичної інфраструктури (PCII). Однією з головних перешкод в обміні інформацією між урядом і промисловістю є загальне небажання приватних компаній надавати уряду інформацію, яка згодом може бути використана проти них у регуляторних діях або притягненні до відповідальності. Щоб подолати цю перешкоду, Сполучені Штати прийняли законодавчу базу PCII. Програма PCII захищає інформацію, добровільно надану промисловістю, від використання в регуляторних цілях та розголошення відповідно до деяких урядових зобов'язань щодо розкриття інформації громадськості в рамках закону "Про свободу інформації".3

З огляду на те, що інформація, якою володіють уряди щодо загроз критичній інфраструктурі, може бути засекреченою, важливо розробити способи обміну цією інформацією з промисловістю, щоб допомогти запобігти атакам або пом'якшити їхні потенційні наслідки. Як зазначалося вище, найважливішою стратегією для подолання цього виклику є розробка процесів для створення продуктів, якими можна ділитися на незасекреченому рівні. Цей крок особливо важливий для будь-яких рекомендованих захисних заходів, щоб цими заходами можна було вільно обмінюватися всередині та між компаніями приватного сектору. На додаток до використання продуктів "лінії розриву", DHS також прийняла Програму допуску приватного сектору, яка надає обмежену кількість допусків персоналу приватного сектору, який відповідає за захист об'єктів критичної інфраструктури, щоб питання засекречення не перешкоджали уряду ділитися життєво важливою інформацією, коли це необхідно. Оскільки деяка інформація просто не може бути розсекречена, деяким членам Альянсу і країнам-партнерам може бути корисно впроваджувати програми, подібні до цієї.

У той час як попередні програми стосуються обміну як кібер-, так і фізичною інформацією, четвертий тип програм - обмін інформацією з питань кібербезпеки - має деякі унікальні характеристики, які вимагають спеціалізованих підходів до обміну інформацією. Усвідомлення цієї потреби спонукало DHS розробити Програму обміну та співпраці в галузі кібербезпеки, яка дозволяє своєчасно обмінюватися несекретною інформацією про загрози та вразливості за допомогою надійних державно-приватних партнерств. Для обміну інформацією з кібербезпеки важливо визначити спільну мову і синтаксис, особливо якщо обмін інформацією має відбуватися від машини до машини - від комп'ютера до комп'ютера - і від машини до комп'ютера. критично важливою здатністю, враховуючи швидкість, з якою поширюються нові кіберзагрози. Однією з таких систем є Автоматизований обмін індикаторами, який полегшує обмін машинозчитуваними індикаторами кіберзагроз і рекомендованими захисними заходами. Ця можливість обміну використовує відкриті стандарти, такі як Структурований вираз інформації про загрози для індикаторів кіберзагроз і інформації про захисні заходи, а також Довірений автоматизований обмін інформацією про індикатори для міжмашинної комунікації.6

Аналогічно, Федеральне бюро розслідувань США (ФБР) координує кілька додаткових програм обміну інформацією, в тому числі три приклади, розглянуті тут. Перша програма - це концепція Об'єднаної цільової групи з боротьби з тероризмом (JTTF). Коли нью-йоркський відділ ФБР створив першу JTTF у 1980 році, ця група, до складу якої входили співробітники нью-йоркської поліції і ФБР, дозволила обмінюватися життєво важливою інформацією про пограбування банків, здійснені терористичною групою в Нью-Йорку. Враховуючи успіх у вирішенні проблеми обміну інформацією та розвідувальними даними на підтримку цих розслідувань, концепція JTTF виявилась придатною і для подальшого використання.

У 1998 році ФБР створило спеціальну оперативну групу (JTTF), щоб розпочати підготовку до зимових Олімпійських ігор 2002 року в Солт-Лейк-Сіті, штат Юта. У 1998-2002 роках ця робоча група зосередила своє розслідування на праворадикальному антисемітському угрупованні, відомому під назвою "Сини арійської культури", яке здійснювало злочинну діяльність на території Солт-Лейк-Сіті. Розслідування JTTF показало, що банда розробляла плани нападу на Олімпійські ігри, але протягом чотирьох років JTTF ефективно ліквідувала цю групу і зірвала її плани нападу на Олімпіаду. В рамках роботи JTTF понад 100 лідерів громадської безпеки отримали допуск до державної таємниці, що дозволило їм законно обмінюватися секретною інформацією та розвідувальними даними. Ці зусилля виявилися дуже ефективними у протидії терористичним загрозам під час Олімпіади і створенні ефективних і об'єднаних зусиль з громадської безпеки на підтримку цієї великої події. Мабуть, найбільш значні зусилля ЦГБТ були докладені після терористичних атак 11 вересня, коли до складу ЦГБТ увійшли понад 100 різних груп і 5 000 місцевих, державних і федеральних офіцерів.

Слід зазначити, що після 11 вересня коло членів ЦГБТ розширилося, і тепер до неї можуть входити організації громадської безпеки в межах певної юрисдикції. Критично важливим компонентом успіху кожної окремої ЦГСБ була доведена готовність обмінюватися розвідданими та інформацією між відомствами-учасниками. Члени ЦГСБ проходять ретельну перевірку на благонадійність перед тим, як їм дозволять приєднатися до ЦГСБ. Незважаючи на те, що перевірка біографічних даних і допусків, необхідних для кожного члена ЦГСБ, є дороговартісною і трудомісткою, вона дозволяє проводити скоординовані міжвідомчі розслідування і обмінюватися життєво важливою конфіденційною інформацією та розвідувальними даними. ЦГСБ є надзвичайно ефективним правоохоронним механізмом для обміну інформацією та секретними розвідувальними даними і зробили значний внесок в успішну боротьбу з тероризмом в США після 11 вересня.

Другою важливою програмою обміну інформацією під егідою ФБР є географічно сфокусована мережа обміну інформацією про критичну інфраструктуру, відома як InfraGard. Ця мережа є інструментом державно-приватної співпраці, спрямованої на прискорення своєчасного обміну інформацією та сприяння взаємному навчанню з питань захисту критично важливої інфраструктури. Однією з ключових переваг програми є зв'язок місцевих відділень InfraGard з місцевими відділеннями ФБР. Такий географічний зв'язок дає змогу будувати відносини за принципом "відкритого неба" і налагоджувати стосунки, засновані на взаємній довірі. Під час стабільних операцій InfraGard зосереджується на навчанні та обміні інформацією за допомогою вебінарів, брифінгів щодо несекретних загроз та обміну документами через захищений онлайн-портал. InfraGard має близько 80 відділень у більшості великих міст США і залучає до співпраці керівників, часто на рівні об'єктів, які перебувають на "передовій" захисту інфраструктури.

Третьою програмою обміну інформацією, якою керує ФБР, є Рада Альянсу внутрішньої безпеки (DSAC). На відміну від InfraGard, яка зосереджена на побудові довірчих відносин з операторами на місцевому рівні, DSAC забезпечує механізм на рівні виконавчої влади для покращення комунікації та сприяння своєчасному і ефективному обміну інформацією з питань безпеки та розвідки між федеральним урядом і приватним сектором.7 Для досягнення цієї мети DSAC об'єднує вище державне керівництво ФБР і Міністерства внутрішньої безпеки, а також керівників приватного сектору. DSAC був створений у 2005 році за зразком Консультативної ради з питань безпеки за кордоном Державного департаменту США, яка співпрацює з приватним сектором, допомагаючи американським приватним компаніям, що працюють за кордоном, бути обізнаними про загрози міжнародним операціям.

Ряд програм в Європейському Союзі зосереджені на обміні інформацією про безпеку та стійкість критичної інфраструктури як для кібер-, так і для фізичної інфраструктури. Одну з останніх програм Європейська Комісія започаткувала 23 червня 2021 року, оголосивши про створення Об'єднаного кіберпідрозділу (JCU), покликаного сприяти співпраці між кіберспільнотами в інституціях, агентствах, органах та органах влади країн-членів ЄС. Зокрема, JCU має на меті посилити співпрацю та обмін інформацією між різними організаціями, що займаються питаннями стійкості, правоохоронними органами, обороною, дипломатією та приватним сектором - разом з користувачами та постачальниками рішень та послуг у сфері кібербезпеки - у відповідь на збільшення кількості серйозних кіберінцидентів, що впливають на громадян та бізнес по всьому ЄС. Для досягнення своїх цілей - сприяння скоординованому реагуванню ЄС, покращення ситуаційної обізнаності та гарантування спільної готовності - ЄКГ розвиватиме спроможності впродовж чотирьох запланованих етапів розвитку і, як очікується, стане повністю функціональною до середини 2023 року.8

Однією з програм обміну інформацією, спільною для США та Європи, є Центр обміну та аналізу інформації (ISAC), який є організацією, що спеціалізується на обміні інформацією про загрози та вразливості в секторі критичної інфраструктури. Агентство ЄС з кібербезпеки є прихильником створення ISAC в Європі, а його посібник "Моделі співпраці" містить вичерпний опис діяльності ISAC в Європі, включаючи моделі для конкретних країн і секторів, а також міжнародні моделі ISAC. У Сполучених Штатах багато секторів і підсекторів інфраструктури самоорганізувалися в ISAC, які відповідають потребам компаній-членів. Деякі ISAC надають послуги на платній основі, тоді як інші тісно координують та використовують урядові операційні центри для обміну інформацією. Деякі ISAC, як, наприклад, комунікаційний ISAC США, мають широку сферу діяльності і охоплюють цілий сектор, тоді як інші є вузькоспеціалізованими, як, наприклад, ISAC з питань переробки та збуту природного газу. ISAC також можуть координувати обмін інформацією від ISAC до ISAC, що дозволяє здійснювати міжгалузевий обмін інформацією для підвищення безпеки та стійкості інфраструктури.

Програми обміну інформацією в жодному разі не обмежуються тими, що спрямовуються згори донизу державними установами. Багато з найефективніших механізмів органічно розвиваються для задоволення потреб учасників, пов'язаних спільною географією або схожими умовами роботи. Хоча програми федерального уряду, описані вище, можуть бути важливими для загального успіху обміну інформацією, багато програм розвивалися без підтримки керівництва, а іноді навіть участь федерального уряду. Різноманітні місцеві, державні, національні та міжнародні групи розширюють можливості обміну інформацією для своїх членів, надаючи їм оперативну підтримку або просто визначаючи шаблони, стандарти та процеси, які полегшують обмін інформацією.

Наприклад, FIRST - міжнародне партнерство, спрямоване на об'єднання команд реагування на кіберінциденти і безпеки - задокументувало простий "протокол світлофора", який визначає, яким чином певний звіт або частина інформації може бути надалі поширена або обмежена.10 Ця система забезпечує певний рівень безпеки для тих, хто ділиться інформацією, а також чіткість для одержувачів щодо того, чи можна ділитися інформацією і з ким. У Сполучених Штатах Америки державні та місцеві центри злиття сприяють обміну інформацією між правоохоронними органами на федеральному рівні, на рівні штатів, на місцевому рівні та в приватному секторі в межах певного штату чи регіону. Національні та міжнародні професійні асоціації, такі як Інститут інженерів з електротехніки та електроніки і Американське товариство інженерів-будівельників, допомагають обмінюватися інформацією про безпеку і стійкість відповідних інфраструктур. Нарешті, галузеві групи часто об'єднуються для обміну інформацією на ключові теми, що становлять інтерес для стійкості критично важливої інфраструктури, як, наприклад, Міжнародний посібник з безпеки ботнетів і Інтернету речей Ради з безпеки цифрової економіки або Американська асоціація водогосподарських підприємств, яка ділиться інформацією, життєво важливою для безпеки водного сектору.11

### Тематичні дослідження: Обмін інформацією в акції

У цьому розділі коротко описано кілька реальних прикладів обміну інформацією. Кожен приклад висвітлює одну або декілька концепцій та програм, описаних у попередньому розділі.

##### Робоча група з кібер-здоров'я: Державно-приватна інформація Спільне використання

Робоча група з кібер-здоров'я (CHWG) була створена у 2015 році Вашингтонським відділенням ФБР, Національним альянсом членів InfraGard, відділенням InfraGard у столичному регіоні та Виконавчим партнерством з інтегрованого співробітництва, неприбутковою організацією 501(c)(3) у Шарлотті, Північна Кароліна. Використовуючи просту технологію Listserv, CHWG забезпечує двосторонній обмін інформацією в режимі реального часу для кібер-практиків у сфері охорони здоров'я та громадського здоров'я. Учасники обмінюються найкращими практиками, нові загрози та тенденції, а також індикатори компрометації. З моменту заснування групи кількість її членів зросла з приблизно 200 на початку до більш ніж 1 300 осіб.

Учасники - це члени InfraGard, які працюють на перетині секторів інформаційної безпеки та охорони здоров'я, які використовують список розсилки та онлайн-портал для обміну інформацією про ризики, відповідність вимогам, нові загрози та найкращі практики в галузі кібербезпеки. Оскільки InfraGard - це державно-приватна програма співпраці, до складу CHWG входять представники як приватного, так і державного секторів. Керівний комітет CHWG, що складається з учасників приватного сектору, які представляють різні підгалузі сектору охорони здоров'я, забезпечує базове управління групою і визначає місію, сферу діяльності та параметри членства в ній. Місія CHWG полягає в тому, щоб розвивати, підтримувати та сприяти створенню спільноти професіоналів у сфері кібербезпеки, які працюють у секторі охорони здоров'я, а також тих, хто має відповідні обов'язки (наприклад, кібербезпека фізичних об'єктів), і тих, хто може обмінюватися інформацією в режимі реального часу про ризики, управління, загрози, індикатори, тенденції та передовий досвід. Членство в CHWG, як встановлено керівним комітетом, відкрите для всіх осіб, які відповідають наступним критеріям:

* + Є чинним членом InfraGard або має заяву на розгляді в місцевому осередку InfraGard.
  + Працює у сфері кібербезпеки в організації в секторі охорони здоров'я або займається кібербезпекою на фізичному об'єкті.
  + Принаймні частково відповідає за питання кіберзагроз, ризиків, управління або комплаєнсу.
  + Може отримати доступ до інформації про загрози та/або найкращих практик кібербезпеки та потенційно ділитися нею.
  + Не має ролі, яка в першу чергу зосереджена на розвитку бізнесу або продажу продуктів і послуг, і не буде використовувати групу для маркетингу або просування продуктів і послуг.

За даними Вашингтонського відділення ФБР, CHWG допомагає ФБР у виконанні його місії, прогнозуючи випадки, посилюючи поточні розслідування, виявляючи нових жертв кібервторгнень і беручи участь у створенні кількох розвідувальних продуктів. Наприклад, під час нещодавньої кібератаки на великого постачальника медичних послуг CHWG виявила атаку до того, як цілодобовий центр спостереження за кіберопераціями ФБР і члени групи з різних штатів обмінялися суттєвою інформацією та визначили інші мережі обміну інформацією, які мали відповідну інформацію, включаючи індикатори компромісу. Після успіху CHWG були створені додаткові робочі групи за тією ж моделлю для сектору комерційних об'єктів (кібербезпека), фінансового сектору (кібербезпека) та сектору центрів обробки даних (фізична безпека).

### Якщо ти щось бачиш, скажи Щось®

Якщо ти щось бачиш, скажи щось® - це національна антитерористична інформаційно-просвітницька програма США, ліцензована Міністерством національної безпеки і оборони (МНБ). У партнерстві з Загальнонаціональною ініціативою з повідомлення про підозрілу діяльність Міністерства юстиції США, МНБ офіційно розпочала цю кампанію в липні 2010 року з метою підвищення обізнаності про ознаки тероризму та злочинів, пов'язаних з тероризмом, а також навчання правоохоронців на державному та місцевому рівнях розпізнавати ці типи поведінки та ознаки.12 Загальнонаціональна ініціатива з повідомлення про підозрілу діяльність розробила стандартний процес документування та аналізу спостережень, які генерує кампанія, і регулярно передає ці звіти відповідним об'єднаним групам під керівництвом ФБР для проведення розслідувань і державним об'єднаним центрам для проведення аналізу.

Від початку кампанія "Якщо ти щось бачиш, скажи щось" була поширена на штати, округи, міста та транспортні підприємства (такі як аеропорти та громадський транспорт, великі розважальні заклади та спортивні заходи, коледжі та університети, приватний бізнес та засоби масової інформації). Партнери програми просувають кампанію як частину свого ширшого плану з охорони та безпеки, використовуючи внутрішню рекламу для співробітників (наприклад, у місцях загального користування, кімнатах відпочинку, туалетах та електронною поштою), а також у місцях, доступних для громадськості. Організації, які приєднуються до кампанії, мають доступ до соціальної реклами, освітніх матеріалів, вивісок, а також відповідного і стійкого контенту в соціальних мережах.

Завдяки цій кампанії було зірвано кілька терористичних планів і врятовано кілька життів.13 Одним із прикладів є справа Александра Чікколо з Адамса, штат Массачусетс. Син капітана бостонської поліції, Чікколо носив ім'я Алі Аль-Амрікі і захоплювався "Ісламською державою". (Даеш) терористичного угрупування. За наводкою батька Чікколо ФБР розпочало розслідування, під час якого було записано, як Чікколо обговорює плани участі в терористичній діяльності, натхненній Ісламською державою (ДАІШ), що передбачала наповнення скороварок чорним порошком, цвяхами та кульковими підшипниками. Після спецоперації в липні 2015 року Чікколо був заарештований і згодом визнав себе винним за кількома звинуваченнями, зокрема у спробі надати матеріальну підтримку іноземній терористичній організації. У вересні 2018 року він був засуджений до 20 років позбавлення волі і довічного звільнення під наглядом.

##### Атака на Капітолій США: Обмін інформацією Провал?

6 січня 2021 року учасники заворушень атакували будівлю Капітолію США, намагаючись зірвати спільне засідання Конгресу, під час якого члени Конгресу мали підрахувати голоси виборців на виборах президента та віце-президента США, а потім оголосити офіційні результати виборів 2020 року. Нападники увірвалися до будівлі Капітолію, вандалізували та викрадали майно, обшукували офіси, нападали на представників правоохоронних органів, а також загрожували безпеці та життю обраних лідерів США. Співробітники поліції Капітолію разом з федеральними, штатними та місцевими правоохоронцями відновили контроль над будівлею, а голова Сенату, віце-президент Майк Пенс оголосив Джозефа Р. Байдена-молодшого і Камалу Гарріс обраними президентом і віце-президентом Сполучених Штатів рано вранці 7 січня. На жаль, семеро людей, у тому числі троє правоохоронців, загинули.

Сенат США розслідував збої в системі безпеки, планування та реагування, а також критичні поломки в різних федеральних відомствах, зокрема в ФБР, Міністерстві національної безпеки і оборони та Міністерстві оборони. Сенатське розслідування задокументувало низку недоліків, які створили передумови для проникнення в Капітолій. Цікаво, що у звіті особливо підкреслено два збої в обміні інформацією як такі, що мали велике значення для загальної нездатності захистити Капітолій.

По-перше, у звіті Сенату йдеться про те, що федеральна розвідувальна спільнота на чолі з ФБР і Міністерством національної безпеки не змогла попередити про потенційне насильство, спрямоване проти Капітолію 6 січня, на основі оцінки загроз. У доповіді документує, як правоохоронні органи, зокрема Поліція Капітолію США, покладаються на розвідувальне співтовариство в оцінці та інформуванні про загрози національній безпеці. У той час як ФБР і МНБ поширювали численні письмові документи з детальним описом потенціалу зростання насильницько-екстремістської активності та нападів на співробітників правоохоронних органів, урядові установи та працівників інших законних протестів протягом 2020 року, жодних подібних звітів щодо загроз 6 січня не було оприлюднено. Хоча онлайн-заклики до насильства біля Капітолію були виявлені та оцінені відомствами, посадовці ФБР та Міністерства внутрішньої безпеки заявили, що виявлена активність, можливо, була захищеною конституцією свободою слова, а не реальними, достовірними погрозами насильства. У своїх свідченнях посадовці ФБР і МНБ визнали необхідність покращити обробку та поширення інформації про загрози з соціальних мереж і онлайн-дошок оголошень. Цей перший звіт Сенату показує, як стримуючі фактори - в даному випадку поєднання нечітких правових норм і побоювання політичної непередбачуваності - можуть обмежити готовність урядових установ ділитися інформацією.

По-друге, у звіті Сенату зазначається, що розвідувальні підрозділи УСПП, які відповідають за підготовку власного розвідувального аналізу, не передавали повного обсягу інформації про загрози, якою вони володіють.16 У звіті задокументовано, що, незважаючи на відсутність розвідданих ФБР і МЗС та інформації про загрози, провідний розвідувальний компонент USCP - Відділ розвідки і міжвідомчої координації (IICD) - знав про потенціал насильства в дні і тижні, що передували 6 січня, на основі численних джерел інформації про великі натовпи людей, які, як очікувалося, зберуться у Вашингтоні 6 січня, і про конкретні загрози насильства, зосереджені на спільному засіданні Конгресу і комплексі споруд на території Капітолію. Незважаючи на те, що у розпорядженні СВРК була необхідна внутрішня інформація, він не зміг повною мірою включити її у внутрішню оцінку подій 6 січня та спільної сесії. Як наслідок, офіцери УБКП та інші партнери з правоохоронних органів не мали цієї критично важливої інформації про загрози насильства. Цей показник демонструє, наскільки шкідливою може бути ситуація, коли життєво важлива інформація не надається тим, хто потребує її для вжиття захисних заходів для зменшення ризиків і загроз, а також для захисту критично важливої інфраструктури.

Крім того, у звіті Сенату стверджується, що підготовка USCP до спільної сесії постраждала через децентралізовану природу її розвідувальних компонентів і відсутність обміну інформацією між цими елементами.

5 січня співробітник окремого підрозділу УСКТ, що займається розвідкою, отримав інформацію від місцевого відділення ФБР у Норфолку про обговорення в Інтернеті насильства, спрямованого проти Конгресу, в тому числі про те, що протестувальники приходять до Конгресу "підготовленими до війни". Цей звіт, який був схожий на іншу інформацію, отриману IICD, і міг би слугувати підтвердженням, не був поширений серед керівництва IICD або USCP до 6 січня.

Це невдалий приклад важливості багатовекторного обміну інформацією; якби різні компоненти в рамках однієї структури були більш ефективними в латеральному обміні інформацією, результат подій 6 січня міг би бути зовсім іншим.

##### Національна антитерористична консультативна система

Після терористичних атак на Сполучені Штати 11 вересня уряд визначив потребу в стандартному способі обміну інформацією про терористичні загрози з населенням США. Перша з цих програм, Консультативна система національної безпеки (HSAS), була створена 12 березня 2002 року.18 Ця програма була задумана як простий засіб інформування про рівні загроз і, як така, передбачала п'ять базових рівнів загроз, позначених різними кольорами (див. рис. 11-1). На додаток до рівнів загроз, HSAS також надавала рекомендовані захисні заходи для федеральних агентств, але, що важливо, не для органів влади штатів і місцевих органів влади, приватного сектору або широкої громадськості. Проста, заздалегідь встановлена система кольорового кодування використовувала один з ключових принципів обміну інформацією, який полягає у встановленні шаблонів і визначень заздалегідь, щоб полегшити швидкий обмін складною інформацією.

Незважаючи на добрі наміри, HSAS стала жертвою кількох пасток, характерних для програм обміну інформацією. Однією з головних проблем HSAS було те, що її попередження були розпливчастими і для більшості користувачів не містили конкретних дієвих захисних заходів. Як обговорювалося раніше, програми обміну інформацією функціонують найкраще, коли вони розміщують своєчасну, дієву інформацію в руках тих, хто здатен впроваджувати захисні заходи. Хоча інформація про зміни в HSAS поширювалася через низку механізмів, жоден з них не був повністю задовільним, і багато користувачів повідомляли наглядовим комітетам Конгресу, що основним джерелом повідомлень про зміни в HSAS для них були ЗМІ з відкритим вихідним кодом. Підвищення рівнів HSAS часто призводило до значних витрат для федеральних агентств, державних і місцевих служб реагування, а також приватного сектору, оскільки вони впроваджували більш жорсткі заходи захисту. Тому особи, відповідальні за визначення рівнів HSAS, неохоче підвищували їх, але водночас вони не хотіли знижувати рівень загрози, щоб потім бути здивованими терористичною атакою, яку важко виявити, і бути звинуваченими в тому, що вони втратили пильність у найневідповідніший момент. В результаті рівні загрози HSAS змінювалися не дуже часто; "під охороною" і "низький" рівні ніколи не використовувалися, а найвищий рівень (суворий) застосовувався лише протягом трьох днів, але тільки спеціально для вхідних рейсів з Великої Британії одразу після теракту в цій країні.



**Малюнок 11-1. Дорадча система національної безпеки**

У січні 2011 року МНБ скасувало HSAS і замінило її новою системою - Національною системою консультування з питань тероризму (NTAS). У новій системі було скасовано кольорове кодування рівнів на користь двох специфічних продуктів: підвищених сигналів тривоги, які попереджали про реальні загрози, і неминучих сигналів тривоги, які попереджали про близьку реальну загрозу, що передбачала необхідність негайних захисних дій. Обидва типи оповіщень мали високий поріг для запобігання надмірному використанню системи, що могло б призвести до того, що одержувачі не сприймали б оповіщення серйозно. Однак такий підхід мав і зворотний бік, оскільки він унеможливлював обмін інформацією нижчого рівня, яка не відповідала цим високим порогам, але все одно могла бути корисною для захисту проти загроз. Щоб заповнити цю прогалину, пізніше МНБ додало нову категорію рекомендацій, відому як бюлетені, для обміну інформацією про "терористичні тенденції, події і потенційні загрози в тих ситуаціях, коли можуть бути виправдані додаткові запобіжні заходи, але коли обставини не вказують на загрозу Сполученим Штатам з достатньою мірою достовірності або конкретності і достовірності", щоб виправдати оголошення оповіщення. Хоча NTAS запропонувала деякі суттєві покращення, вона не повністю подолала розпливчастість, відсутність конкретних захисних заходів і стимулів до їх застосування, які заважали її попередниці.

### Національні заходи зі спеціальної безпеки

**та Рейтинг оцінки спеціальних подій**

Оскільки великі події, такі як інавгурації президентів, Олімпійські ігри, чемпіонати світу та Суперкубок, привертають мільйони глядачів і привертають увагу всього світу або збирають в одному місці найважливіших лідерів, вони вимагають особливих заходів безпеки для належного захисту від терористичних атак. Насправді, деякі з цих заходів у минулому були об'єктами терористичних змов і нападів. Готуючись до таких подій, країни, що їх проводять, можуть визначати такі події як такі, що мають значення для національної безпеки, і надавати спеціальне національне фінансування, повноваження і ресурси, включно з обміном інформацією, для допомоги у плануванні та виконанні оперативних вимог. У Сполучених Штатах федеральний уряд може визначати певні заходи як національні заходи особливого рівня безпеки (коли на них будуть присутні президент, глави іноземних держав або інші високопосадовці під захистом Секретної служби) або присвоювати їм особливий рейтинг активності (коли велике скупчення людей або символічні заходи можуть підвищити загрозу і наслідки терористичної атаки).

Як зазначалося раніше, довіра є критично важливим елементом, який необхідно розвивати для того, щоб установи та організації були вмотивовані ділитися інформацією та розвідувальними даними. Визначення цих важливих подій забезпечує ресурси і концентрацію уваги, необхідні для того, щоб дозволити відомствам взаємодіяти, ділитися юрисдикційним плануванням і оперативними обов'язками, а також розвивати довірчі відносини за допомогою інтегрованих, скоординованих зусиль у сфері безпеки і боротьби з тероризмом.

CISR є ключем до успіху цих великих заходів, оскільки безпека учасників та успішне проведення заходу завжди залежать від основних послуг, такі як надійне електропостачання, зв'язок, транспорт і водопостачання. Розбудова довіри та координація операцій між різними секторами критичної інфраструктури вимагає тісної співпраці з приватним сектором, правоохоронними органами та службами безпеки. Залучення власників та операторів об'єктів критичної інфраструктури до планування та оперативної координації є нелегкою справою, але такі зусилля створюють основу для довіри між усіма учасниками, сприяють обміну інформацією та розвідданими і, зрештою, допомагають убезпечити об'єкти критичної інфраструктури і, як наслідок, саму подію.

### Резюме та дії для розгляду

Програми обміну інформацією завжди будуть представляти операційні та політичні виклики, оскільки багато їх елементів містять внутрішню напругу і тому повинні бути постійно збалансовані. Занадто багато інформації може призвести до інформаційної втоми, але занадто мало - до того, що критичні знання не потраплять туди, де їх можна буде використати. Аналогічно, інформація, якою обмінюються, повинна знаходити золоту середину між (1) надто вичерпним звітуванням, яке приховує критичні моменти в несуттєвих даних, і (2) поверхневим звітуванням, якому бракує достатньої деталізації, щоб викликати довіру і дозволити швидко і правильно приймати рішення.

Як зазначено в цьому розділі та детально розглянуто в тематичних дослідженнях, нижче наведено кілька ключових моментів для побудови ефективних програм обміну інформацією.

* Побудуйте довірливі відносини з правильними партнерами. Важливість довірливих відносин для ефективного обміну оперативною інформацією неможливо переоцінити. Таку довіру часто можна розвивати за допомогою регулярних контактів в умовах "чистого неба" або стабільної обстановки. У цьому контексті важливо ретельно ідентифікувати, відбирати і розвивати критично важливих членів спільноти з обміну інформацією, а саме тих, хто володіє критично важливою інформацією, і тих, хто може вжити заходів на основі інформації, якою потрібно ділитися.
* Встановіть норми спільного використання в громаді. Норми спільноти включають (1) керівні принципи або правила використання та подальшого обміну інформацією, отриманою через мережу;

1. спільну лексику та термінологію, включно з пороговими значеннями та критеріями щодо того, коли і як обмінюватися інформацією; та
2. шаблони і формати для продуктів обміну інформацією. Ці шаблони можуть бути настільки специфічними, як машинозчитувані формати повідомлень з кібербезпеки, такі як STIX/TAXII, або зручні для читання людиною формати звітів, які включають критично важливу інформацію там, де одержувачі очікують її побачити.

* Оцініть стимули та перешкоди для обміну інформацією та розробіть програми, щоб максимізувати переваги та мінімізувати недоліки для всіх учасників. Недостатньо просто заохочувати обмін інформацією та очікувати, що це станеться раптово і природно. Створення ефективної програми вимагає розуміння різних поглядів на стимули та перешкоди, яких дотримуються різні зацікавлені сторони, а потім розробки конкретних програм, які б збільшували переваги та обмежували недоліки.
* Подумайте про середовище, в якому відбуватиметься обмін інформацією. Механізми обміну інформацією часто передбачають компроміси, зокрема, між безпекою та простотою використання. Залежно від потреб громади, обмін інформацією може відбуватися лише особисто; через багатофакторну автентифікацію на онлайн-форумах; через електронну пошту, телефонні дзвінки та текстові повідомлення; або ж за допомогою відкритих джерел новин та засобів масової інформації.
* Постійно переоцінюйте ефективність. Жодна програма обміну інформацією не може ідеально відповідати потребам своєї громади, і навіть якщо це так, потреби громади з часом змінюються. Регулярна переоцінка дає можливість гарантувати, що процеси обміну інформацією відбуваються якнайшвидше і що інформація дійсно потрапляє до тих, хто може її використати найбільше.

Задля ефективного захисту критично важливої інфраструктури НАТО від усього спектра загроз, в тому числі і тероризму, особи, які приймають рішення у військових, правоохоронних органах і спільнотах власників і операторів, повинні співпрацювати і обмінюватись різними фрагментами пазла, якими кожен з них володіє. Лише завдяки довірливим відносинам обміну інформацією в усталеному, безпечному середовищі можна отримати повну картину ризиків. Цей процес дозволить приймати рішення щодо захисних заходів і інвестицій в стійкість з урахуванням ризиків, що сприятиме підвищенню безпеки критично важливої інфраструктури.

# - 12 -

## Моделювання та аналіз взаємозалежності критичної інфраструктури:

**Вдосконалення стратегій управління стійкістю**

Дуейн Вернер

Країни-члени Організації Північноатлантичного договору та країни-партнери стикаються зі значними труднощами у формулюванні та впровадженні ефективних стратегій для подолання ризиків, пов'язаних з природними, техногенними (в тому числі терористичними) та соціально-технологічними загрозами. Екстремальні погодні явища можуть завдати величезної шкоди кільком секторам інфраструктури в результаті одного шторму.1 Руйнівні наслідки є наслідком неефективного управління та відсутності інвестицій в інфраструктуру, що забезпечує життєдіяльність громади.2 Мабуть, найбільш нагальна з цих проблем - зміна клімату - створює значні загрози для прибережних громад, а також зміну екологічних умов у всьому світі, таких як температура і кількість опадів, для яких сучасний дизайн і продуктивність інфраструктури не передбачені.

Вернер

були адаптовані.3 Складність оцінки цих ризиків та управління потенційним руйнівним впливом цих подій на критичну інфраструктуру зростає, якщо врахувати взаємозалежність, яка існує між об'єктами та системами інфраструктури. Об'єкти критичної інфраструктури функціонують у взаємодії один з одним. Тому катастрофічні події можуть каскадом поширюватися на ці взаємопов'язані системи і перешкоджати здатності операторів критичної інфраструктури продовжувати свою діяльність.

Політичні рекомендації з різних дисциплін, від принципів національної безпеки до стандартів безперервності бізнесу, вказують на важливість врахування взаємозалежностей для посилення безпеки та стійкості систем критичної інфраструктури.4 Однак більшість цих документів не дають вичерпного визначення методологій для розуміння складних взаємодій між об'єктами критичної інфраструктури і підтримки стратегій управління стійкістю. В останні роки дослідження і розробки в галузі моделювання взаємозалежностей критичної інфраструктури набули значного розвитку. Ці підходи, як правило, використовують методи системної інженерії та інженерії безпеки. Однак застосування цих методів до систем критичної інфраструктури є складним завданням через труднощі, пов'язані з отриманням усіх даних, необхідних для запуску комбінованих імітаційних моделей декількох інфраструктурних систем.

Для вирішення цих проблем системний підхід, орієнтований на надання системних послуг, може допомогти встановити відповідний обсяг аналізу взаємозалежності та визначити пріоритетність конкретних активів та/або підсистем, щодо яких необхідно зібрати інформацію, пов'язану зі стійкістю. Використовуючи цей підхід, аналіз враховує контекст високого рівня - соціально-економічну вразливість, наприклад, певного регіону, характеристики об'єктів критичної інфраструктури, що забезпечують регіон ресурсами, а також можливості як об'єктів критичної інфраструктури, так і регіональне управління надзвичайними ситуаціями. Завдяки конкретному реагуванню на вимоги зацікавлених сторін і створенню середовища для співпраці, гнучка система аналізу може забезпечити розробку комплексної та інтерактивної оцінки стійкості взаємозалежностей критично важливої інфраструктури. Ця система також може слугувати для інтеграції різних галузей знань - таких як інженерія, соціальні науки, безперервність бізнесу та управління в надзвичайних ситуаціях - у поєднанні підходів "зверху-вниз" (на рівні системи) і "знизу-вгору" (на рівні об'єктів).

У цій главі досліджується потенціал цього рамкового підходу до аналізу в наступних п'яти розділах. У першому розділі обговорюється важливість врахування взаємозалежностей для підвищення безпеки та стійкості систем критичної інфраструктури. Наступний розділ містить загальний огляд основних характеристик і вимірів взаємозалежностей критичної інфраструктури. У третьому розділі узагальнено загальні підходи до моделювання та оцінки критичної інфраструктури. У наступному розділі пропонується гнучка система аналізу критичної інфраструктури, яка може бути використана для розробки стратегій управління відмовостійкістю. В останньому розділі визначаються елементи для практичного застосування врахування взаємозалежностей критично важливої інфраструктури для управління системами критично важливої інфраструктури. Члени і партнери НАТО можуть використовувати запропоновані рамки аналізу і додаткові міркування щодо практичного застосування його результатів для зменшення ризиків, що загрожують критичній інфраструктурі, і сприяння підвищенню стійкості за допомогою міжсекторальної співпраці.

### Ризик, стійкість та взаємозалежності

Аналітики часто визначають ризик і стійкість як важливі аспекти забезпечення безперервної безпечної експлуатації інфраструктури в економічно ефективний спосіб. Хоча в науці існують певні розбіжності щодо визначення цього поняття, *ризик, як* правило, є поєднанням величини наслідків - наприклад, збитків після події збоїв - і ймовірності або вірогідності настання цих наслідків. Стенлі Каплан і Б. Джон Гаррік вперше визначили три ключові питання, які можуть стати основою для оцінки ризиків. Які проблеми можуть виникнути в системі? Яка ймовірність того, що ці проблеми можуть виникнути? Якими будуть наслідки цих подій? *Управління ризиками* - це назва для широкого спектру методологій для експлуатації та обслуговування системи таким чином, щоб забезпечити прийнятний рівень ризику для всіх зацікавлених сторін, включаючи власників системи, операторів та регуляторні органи. Огляд стратегій оцінки та управління ризиками див. у главі 13. Ефективна оцінка та управління ризиками вимагає виявлення потенційних несприятливих подій, які можуть мати наслідки для системи та її користувачів.

На відміну від ризику, *стійкість* не має універсального визначення в науковій літературі. Визначення стійкості варіюється залежно від теми - наприклад, економічна стійкість, стійкість критичної інфраструктури та соціальна стійкість - і від об'єкта аналізу, такого як громада, інфраструктурна система та інфраструктурний актив. Відмінності у визначенні стійкості впливають на те, як особи, що приймають рішення, вимірюють та оцінюють стійкість.11 У своєму ґрунтовному огляді літератури, присвяченому визначенням стійкості, Л. Карлсон та ін. виділили дві основні наукові школи, основна відмінність між якими полягає в тому, чи вважатимуться дії, вжиті до настання несприятливої події, такими, що підвищують стійкість. Майже вся література визначає стійкість, частково або повністю, як здатність поглинати порушення та адаптуватися або швидко відновлюватися після змін, спричинених порушенням, щоб відновити функціональність.13 У деяких літературних джерелах стійкість також визначається як здатність планувати, пом'якшувати та протистояти загрозам, щоб зменшити загальну вразливість, а отже, ймовірність того, що загроза або небезпека спричинить збій у роботі. Розглядаючи підгрупу цих заходів, що вживаються до події, які здійснюються за припущення, що несприятлива подія відбудеться, Карлсон та ін. визначили стійкість як "здатність об'єкта - активу, організації, громади, регіону - передбачати, протистояти, поглинати, реагувати, адаптуватися і відновлюватися після збурення".

Ризик і стійкість - поняття тісно пов'язані між собою; дії, спрямовані на зниження ризику системи, ймовірно, підвищать стійкість системи, і навпаки.

Оцінка та інформування про заходи зі зниження ризиків та підвищення стійкості вимагає визначення потенційних природних і техногенних загроз, а також оцінки вразливості системи, заходів зі зниження ризиків і можливостей реагування та відновлення після збоїв у роботі.

Ці кроки також обов'язково передбачають ширші характеристики громади та регіону, які обслуговує інфраструктура. Інфраструктурні системи прямо чи опосередковано забезпечують населення товарами та послугами, яких воно потребує. У своїй фундаментальній праці про індивідуальні потреби А. Г. Маслоу розглядав людські потреби як піраміду, кожен з нижчих рівнів якої слугує основою для розвитку вищого порядку.17 На найбільш фундаментальних рівнях ієрархія Маслоу описує фізіологічні потреби та потреби в безпеці (такі як вода, їжа, житло та безпека). Ці потреби мають бути задоволені для того, щоб люди відчували приналежність, повагу та самореалізацію в процесі психологічного розвитку.

Паралельний конструкт, який застосовує ієрархію Маслоу до суспільного розвитку, може допомогти визначити питання, які є найбільш важливими для осіб, що приймають рішення на рівні громад та регіонів, при формулюванні стратегій стійкості.19 У цій структурі різні інфраструктурні системи (зокрема, водна інфраструктура, сільськогосподарська інфраструктура та служби екстреної допомоги) забезпечують ці основні суспільні потреби. У свою чергу, ці інфраструктурні системи потребують послуг і товарів, що надаються іншими інфраструктурними системами. Наприклад, інфраструктура водопідготовки, яка переробляє сиру воду на безпечну питну воду, потребує хімічних речовин (таких як хлор і фтор), що надаються хімічною інфраструктурою. Таким чином, хімічна інфраструктура, що виробляє хімікати для очищення води, опосередковано підтримує потреби людей. Якість інфраструктурних систем та товарів і послуг, які вони надають, може мати значний вплив на якість життя і силу суспільства.

### Таксономії та концепції взаємозалежності критичної інфраструктури

Визначення того, що є критичною інфраструктурою, є відносно узгодженими в усьому світі. У Таблиці 12-1 наведено приклади визначень критичної інфраструктури, що використовуються на Заході.

**Таблиця 12-1. Визначення критичної інфраструктури**

|  |  |
| --- | --- |
| **Країна** | **Визначення** |
| **Австралія** | Фізичні об'єкти, ланцюги постачання, інформаційні технології та комунікаційні мережі, які в разі руйнування, деградації або недоступності протягом тривалого періоду суттєво вплинуть на соціальний або економічний добробут нації, або вплинуть на здатність Австралії здійснювати національну оборону та забезпечувати національну безпеку.22 |
| **Канада** | Процеси, системи, об'єкти, технології, мережі, активи та послуги, що мають важливе значення для здоров'я, безпеки, захисту чи економічного добробуту канадців та ефективного функціонування уряду.23 |
| **Європейський Союз** | Об'єкт або система, що має важливе значення для підтримки життєво важливих суспільних функцій. Пошкодження критичної інфраструктури, її руйнування або порушення роботи внаслідок стихійних лих, тероризму, злочинної діяльності або зловмисної поведінки може мати значний негативний вплив на безпеку ЄС та добробут його громадян.24 |
| **Сполучене Королівство** | Об'єкти, системи, сайти, інформація, люди, мережі та процеси, необхідні для функціонування країни, від яких залежить повсякденне життя.25 |
| **Сполучені Штати** | Інфраструктура настільки життєво важлива, що її непрацездатність або руйнування матиме виснажливий вплив на оборону та національну безпеку.26 |

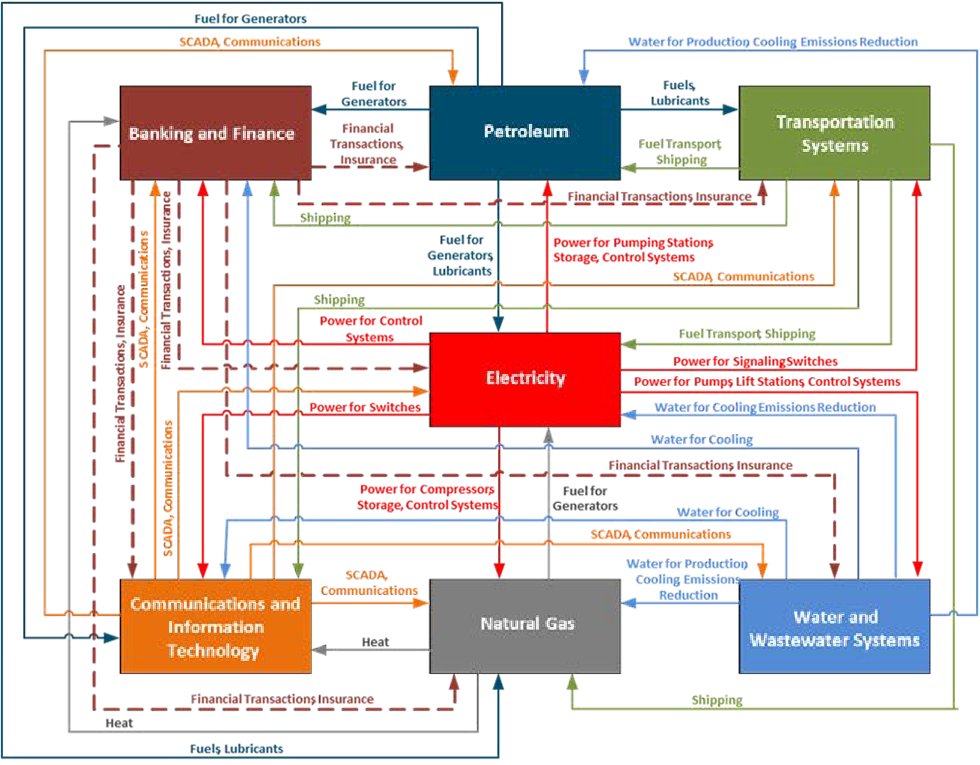
Навіть якби всі ці визначення визнавали критичну інфраструктуру основним компонентом, що підтримує добробут суспільства, вони не відображали б консенсусу щодо того, які сектори складають критичну інфраструктуру. Розділ 1 присвячений обговоренню секторів, які зазвичай визначаються як критичні інфраструктура. У Таблиці 12-2 наведено приклади різних способів, у які західні країни організовують і класифікують сектори як критичну інфраструктуру.

**Таблиця 12-2. Таксономія секторів критичної інфраструктури**

|  |  |
| --- | --- |
| **Країна** | **Сектори** |
| **Австралія** | 7 секторів: енергетика, водопостачання, зв'язок, транспорт, харчовий ланцюг, охорона здоров'я, банківська справа та фінанси27 |
| **Канада** | 10 секторів: охорона здоров'я, харчова промисловість, фінанси, водопостачання, інформаційно-комунікаційні технології, безпека, енергетика та комунальні послуги, виробництво, уряд та транспорт28 |
| **Європейський Союз** | 2 сектори: енергетика (тобто електроенергія, нафта і газ) і транспорт (автомобільний, залізничний, повітряний, внутрішні водні шляхи, а також океанське і каботажне судноплавство і порти)29 |
| **Сполучене Королівство** | 13 секторів: хімічна, цивільна ядерна промисловість, зв'язок, оборона, аварійні служби, енергетика, фінанси, харчова промисловість, уряд, охорона здоров'я, космос, транспорт та водопостачання30 |
| **Сполучені Штати** | 16 секторів: хімічна промисловість, комерційні об'єкти, зв'язок, критичне виробництво, греблі, оборонна промислова база, аварійні служби, енергетика, фінансові послуги, харчова промисловість та сільське господарство, державні об'єкти, охорона здоров'я та громадське здоров'я, інформаційні технології, транспортні системи, системи водопостачання та водовідведення, а також ядерні реактори, матеріали та відходи31 |

Усі ці таксономії включають принаймні сектори життєзабезпечення - енергетику, водопостачання, зв'язок і транспорт, - які задовольняють фізіологічні потреби, визначені Маслоу. Різноманітність характеристик секторів критичної інфраструктури свідчить про складність цих систем та їхній тісний взаємозв'язок.

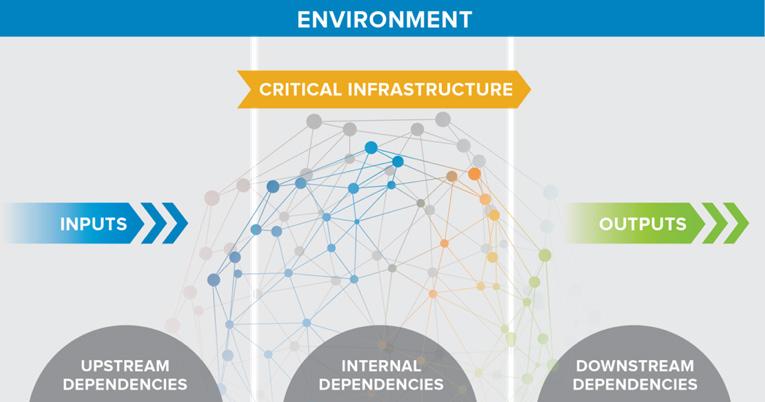
Активи критичної інфраструктури являють собою систему систем, в якій ресурси - а саме товари або послуги, що постачаються однією мережею, є сировиною, що підтримує роботу інших мереж. На Рисунку 12-1 наведено приклад взаємозалежності між системами життєзабезпечення на високому рівні.



**Малюнок 12-1. Взаємозалежності між системами життєзабезпечення**

(Діаграма Аргонської національної лабораторії)

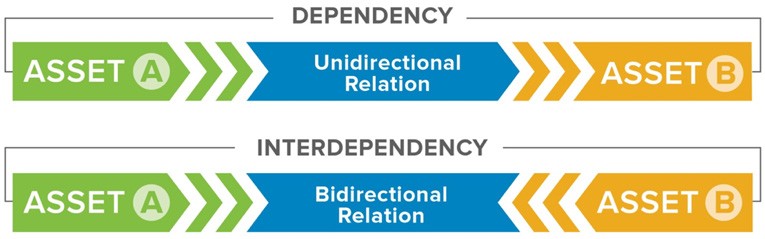
Як показано на рис. 12-1, взаємозалежності характеризуються обміном ресурсами, які є як вхідними, так і вихідними для різних об'єктів інфраструктури. Тому розуміння взаємозалежностей, що існують всередині та між системами критичної інфраструктури, передбачає визначення відносної важливості категорій залежностей у висхідному, внутрішньому та низхідному напрямках. Рисунок 12-2 ілюструє взаємодію між критичною інфраструктурою та її оточенням.



**Рисунок 12-2. Критична інфраструктура та її оточення**

(Діаграма Аргонської національної лабораторії)

Функціонування системи критичної інфраструктури потребує товарів та послуг, що надаються іншими інфраструктурними системами. *Залежність* можна визначити як односпрямований зв'язок між двома об'єктами інфраструктури, в якому послуга або товар, що надається першим об'єктом другому, є необхідним для функціонування останнього. *Взаємозалежність* можна охарактеризувати як поєднання двох залежностей; це двосторонній зв'язок між двома активами. На практиці розуміння взаємозалежності вимагає розуміння двох залежностей між двома активами, що складають взаємозалежність. Рисунок 12-3 ілюструє поняття залежності та взаємозалежності.



**Рисунок 12-3. Залежність та взаємозалежність між активами**

(Діаграма Аргонської національної лабораторії)

Типи залежностей і взаємозалежностей можуть мати різну природу і специфічні характеристики. Кілька авторів розробили таксономії інфраструктурних взаємозалежностей. Однак класифікація, розроблена С. М. Рінальді, Я. П. Перенбумом і Т. К. Келлі, є найбільш повною і найбільш широко використовуваною для аналізу критичної інфраструктури. Ця таксономія визначає чотири класи залежностей, перелічені в таблиці 12-3.

**Таблиця 12-3. Класи залежностей**

|  |  |
| --- | --- |
| **Заняття** | **Визначення** |
| **Фізичний** | Операції залежать від матеріальних результатів іншої інфраструктури через функціональний та структурний зв'язок між входами та виходами двох активів. |
| **Кібер** | Операції залежать від інформації та даних, що передаються через інформаційну інфраструктуру електронними або інформаційними каналами зв'язку. |
| **Географічний** | Операції залежать від місцевого середовища, де будь-яка подія може спричинити зміни в стані операцій у багатьох об'єктах інфраструктури. |
| **Логічно.** | Операції залежать від стану іншої інфраструктури через зв'язки, відмінні від фізичних, кібернетичних чи географічних. Логічна залежність пов'язана з людськими рішеннями та діями і не є результатом фізичних або кібернетичних процесів. |

Рінальді, Перенбум і Келлі стверджують, що ці чотири класи - не єдині характеристики, які слід враховувати при оцінці залежностей від критичної інфраструктури. У Таблиці 12-4 перераховано кілька інших аспектів, які необхідно враховувати в процесі оцінювання.

**Таблиця 12-4. Розмірності залежностей**

|  |  |
| --- | --- |
| **Розміри** | **Визначення** |
| **Робоче середовище** | Охарактеризуйте, як зовнішні фактори можуть впливати на роботу інфраструктури та зв'язки |
| **З'єднання та поведінка у відповідь** | Охарактеризуйте, як інфраструктура реагуватиме на перебої в підключенні або зміни в інфраструктурі |
| **Тип несправності** | Охарактеризуйте поширення наслідків, що виникли в результаті зриву |
| **Характеристики інфраструктури** | Охарактеризувати організацію та функціонування інфраструктури |
| **Стан експлуатації** | Охарактеризуйте стан функціонування критичної інфраструктури |

Підвищення стійкості критичної інфраструктури вимагає кращого розуміння взаємозалежностей між об'єктами критичної інфраструктури та впливу цих взаємозалежностей на функціонування різних інфраструктурних систем. Такий рівень розуміння вимагає розгляду категорій, класів і вимірів, які характеризують інфраструктурні залежності та взаємозалежності. Інтеграція характеристики взаємозалежностей інфраструктури в процес управління ризиками інфраструктури дозволяє зрозуміти, як взаємозалежності впливають на всі компоненти ризику: загрози, вразливості, стійкість і наслідки. Взаємозалежності можуть збільшити інтенсивність техногенних загроз і природних небезпек. Вони також можуть розширити набір вразливостей об'єкта, тобто тих вразливостей, які об'єкт може бути не в змозі ефективно усунути, оскільки елементи взаємозалежності часто перебувають поза контролем об'єкта. Взаємозалежності також впливають на можливості пом'якшення наслідків та реагування. Нарешті, взаємозалежності є основним фактором, що впливає на поширення наслідків - каскадних та ескалаційних збоїв - між інфраструктурними системами та регіонами.

*Каскадні відмови* (або *ефект доміно*) являють собою послідовність збоїв в інфраструктурній системі та між інфраструктурними системами.40 Наприклад, вихід з ладу трансформатора на розподільчій підстанції може унеможливити роботу підстанції і, зрештою, призвести до відключення електроенергії в зоні обслуговування підстанції. Втрата електроенергії потенційно вплине на інші об'єкти інфраструктури, розташовані в цій зоні, а отже, на роботу відповідних інфраструктурних систем. *Ескалація відмови* (або *ефект "снігової кулі*") означає збільшення тяжкості або часу реагування на існуючу відмову інфраструктури.41 Наприклад, якщо розглянути дисфункцію розподільчої підстанції, якщо втрата електроенергії впливає на транспортну систему - наприклад, на роботу диспетчерських центрів і світлофорів - ці проблеми можуть призвести до затримки доступу ремонтної бригади до підстанції для заміни трансформатора, що вийшов з ладу.

Незважаючи на те, що дослідження взаємозалежностей критичної інфраструктури розпочалися в США понад 20 років тому, коли була створена Президентська комісія із захисту критичної інфраструктури, інструменти моделювання, імітації та візуалізації все ще залишаються на проміжному рівні аналізу.

Збір та аналіз даних, як правило, проводяться ізольовано для вирішення фізичних та кіберзалежностей першого порядку.

### Критична інфраструктура Моделювання

З огляду на важливість систем критичної інфраструктури для забезпечення потреб і функціонування громад, аналіз систем критичної інфраструктури є життєво важливим для забезпечення стійкості та здоров'я громад. Однак оцінка взаємозалежності інфраструктури може бути аналітично складною, трудомісткою і дорогою, що, в свою чергу, може обмежувати здатність зацікавлених сторін розуміти і використовувати цю інформацію для прийняття рішень, що враховують ризики.

Для забезпечення власників та операторів інфраструктури різноманітною інформацією розроблено численні методології аналізу інфраструктури. Ці методології, включаючи оцінку вразливості, ризиків і стійкості інфраструктури, дослідження розширення інфраструктури та аналіз взаємозалежності інфраструктури, допомагають планувати інвестиції в інфраструктуру, планувати безперервність бізнесу і приймати оперативні рішення.

Загалом, методології оцінки ризиків та системної інженерії також корисні для аналізу взаємозалежностей критичної інфраструктури. Приклади поширених методологій оцінки інфраструктурних систем включають в себе наступні:

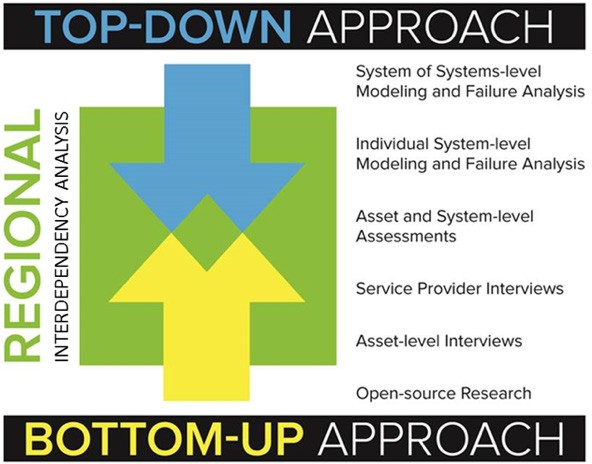
* Мережеве моделювання та теорія графів, включаючи полігони Вороного або Тіссена, моделювання Хаффа та клітинні автомати
* Система з систем моделювання, таких як як багатошарова інфраструктурна мережа
* Моделювання на основі імітаційного моделювання, наприклад, агентне моделювання
  + Економічне моделювання, включаючи моделювання "витрати-випуск
  + Багатокритеріальний аналіз рішень
  + Теорія ігор

Методології моделювання взаємозалежності інфраструктури загалом можна поділити на математичні, геопросторові, системної динаміки, економічні та фізичні. Розроблений для конкретних типів критичної інфраструктури або для конкретних умов, кожен з підходів до моделювання та імітаційного моделювання має свої переваги та обмеження. Ці моделі, які можуть бути детермінованими або імовірнісними за своєю природою, можуть оцінювати продуктивність інфраструктурної системи в один момент часу (статичні) або протягом певного періоду (динамічні). Кожна методологія моделювання інфраструктури має свої переваги і недоліки, включаючи вимоги до даних, припущення, рівень деталізації, складність моделі, а також час розробки і виконання моделі. Жоден тип моделі не є найкращим для всіх типів оцінок інфраструктури. Вибираючи методологію моделювання інфраструктури, аналітики повинні зважити переваги і недоліки різних методологій моделювання з урахуванням потреб зацікавлених сторін і обмежень аналізу.

Аналіз інфраструктурних систем зазвичай відбувається ізольовано, що означає, що безпосереднє моделювання активів у межах інфраструктурної системи є основою для оцінки функціонування системи. Якщо традиційний ізольований підхід і враховує залежності та взаємозалежності, то лише опосередковано, наприклад, через моделі вхідних даних або пояснювальні змінні, що базуються на експертній думці, з'ясуванні або історичних даних. Ізольоване оцінювання інфраструктури суттєво перешкоджає ширшому розумінню динаміки між різними інфраструктурними системами, включаючи каскадні та ескалаційні збої та впливи на ланцюги постачання. Моделюючи залежності з використанням системного підходу, аналітики можуть краще зрозуміти взаємопов'язані операції інфраструктурних систем, що може дозволити виявити окремі точки відмови, які не можуть бути ідентифіковані за допомогою звичайного ізольованого аналізу. Останні роботи характеризують взаємозалежності між інфраструктурними системами, але вони, як правило, зосереджені на мережах життєзабезпечення і вимагають підтримки організацій, що займаються дослідженнями і розробками можливостей. Крім того, більшість існуючих методологій зосереджені переважно на фізичних взаємозалежностях і, до певної міри, на кіберзалежностях; лише деякі роботи включають географічні або логічні залежності.

Підходи до моделювання інфраструктури зазвичай поділяються на дві категорії: низхідні та висхідні. Підходи до моделювання "зверху-вниз" зосереджуються на функціонуванні всієї інфраструктурної системи, а потім оцінюють продуктивність і важливість інфраструктурних підсистем та активів на основі загальної динаміки системи. Підходи висхідного моделювання зосереджуються на характеристиках і функціонуванні окремих об'єктів, що входять до складу інфраструктурної системи, а потім оцінюють загальну роботу системи на основі продуктивності окремих об'єктів. Моделювання за принципом "зверху-вниз" може забезпечити більшу точність загальної роботи системи з меншою деталізацією функціонування окремих об'єктів в рамках системи. І навпаки, висхідні підходи забезпечують високий рівень деталізації функціонування окремих активів, але надають менше інформації про загальну роботу системи. Поєднання підходів "зверху-вниз" і "знизу-вгору" може забезпечити високий рівень деталізації роботи як системи в цілому, так і активів, що входять до її складу.

Системний підхід, що поєднує низхідні та висхідні оцінки в межах систем критичної інфраструктури та між ними, допомагає встановити належний обсяг аналізу взаємозалежності та визначити конкретні стратегії управління безпекою та стійкістю. На Мал. 12-4 показано, як поєднання різних підходів до аналізу може краще охарактеризувати взаємозалежності критичної інфраструктури.



**Рисунок 12-4. Огляд аналізу взаємозалежності стійкості**

(Діаграма Аргонської національної лабораторії)

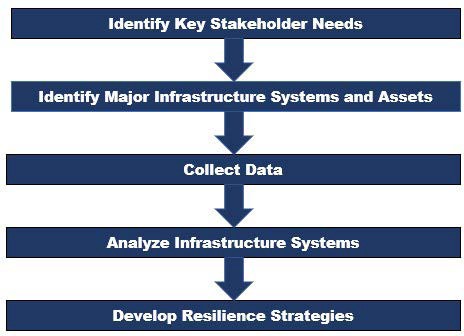
Розробка системного підходу для переходу до передових можливостей аналізу інфраструктури пов'язана з кількома проблемами. Ці виклики включають в себе наступні:

* + Відсутність розуміння роботи інфраструктурних систем та взаємодії між інфраструктурними системами.
  + Відсутність розуміння того, як взаємозалежності інфраструктури впливають на стійкість регіону.
  + Складність у поєднанні імітаційних моделей, спочатку розроблених в ізольованому середовищі та специфічних для певних систем критичної інфраструктури.
  + Труднощі з отриманням даних для запуску імітаційних моделей. Деякі дані є приватною власністю, а деякі невідомі через брак знань.

Сприяння спільному підходу, заснованому на довірі та обміні інформацією, може подолати більшість з цих викликів і внутрішні складнощі, притаманні взаємозалежності критичної інфраструктури.

### Аналіз взаємозалежності критичної інфраструктури Framework

Важливість систем критичної інфраструктури для забезпечення потреб населення, громад і регіонів зумовлює потребу в стандартизованій методології для систематичної оцінки інфраструктурних систем. Враховуючи різноманітність інфраструктурних систем та активів, а також широту методологій аналізу інфраструктури, на рисунку 12-5 запропоновано узагальнену структуру аналізу взаємозалежності критичної інфраструктури.



**Рисунок 12-5. Структура аналізу взаємозалежності**

#### Визначення потреб ключових зацікавлених сторін

Відправною точкою є визначення ключових зацікавлених сторін, таких як власники та оператори інфраструктурних систем, державні установи, неурядові організації та громадськість. Потім, першим кроком в рамках аналізу взаємозалежності критичної інфраструктури є визначення операційних та організаційних потреб цих ключових зацікавлених сторін. Потреби ключових стейкхолдерів включають в себе як висхідні залежності, такі як комунальні підприємства, що надають критичні ресурси, так і низхідні залежності, включаючи споживачів та інші інфраструктурні системи, які потребують товарів або послуг, що надаються ключовими стейкхолдерами. Хоча аналіз залежностей, як правило, зосереджується на впливі втрати попередніх залежностей, не менш важливо враховувати вплив втрати інфраструктурної системи на користувачів, що знаходяться нижче за течією, а також на громаду і суспільне середовище, в якому ця система функціонує. Після події, що призвела до перебоїв, змінюються потреби користувачів, що знаходяться нижче за течією, і операційне середовище можуть - і, можливо, повинні - суттєво впливати на роботу інфраструктури ключових стейкхолдерів.

Однією з основних цілей рамки є надання ключовим зацікавленим сторонам інформації, необхідної для прийняття рішень щодо підвищення стійкості інфраструктури. Таким чином, важливо визначити та окреслити процес прийняття рішень ключовими зацікавленими сторонами, щоб визначити типи та деталізацію вимог до даних, необхідних для прийняття рішень зацікавленими сторонами. Частково цей крок передбачає початкове інформування та залучення зацікавлених сторін для того, щоб відкрити лінії зв'язку та заручитися підтримкою ключових зацікавлених сторін, а також власників та операторів критичної інфраструктури, які управляють інфраструктурою, що залежить від інфраструктури основних зацікавлених сторін.

#### Ідентифікація основних активів та систем

Виходячи з потреб конкретних зацікавлених сторін, бажаного рівня деталізації інформації, а також конкретних соціальних систем і громад, в яких функціонують їхні інфраструктурні системи, другим кроком є визначення відповідних інфраструктурних систем і активів, що становлять інтерес. Ключовою частиною цього кроку є визначення пріоритетності активів в інфраструктурних системах основних зацікавлених сторін та в інфраструктурних системах, які є залежними від цих систем вище за течією. Визначення пріоритетності інфраструктурних активів і систем повинно відображати очікувані наслідки для функціонування інфраструктури зацікавлених сторін, а також для користувачів і клієнтів, що знаходяться нижче за течією, після виведення з ладу або пошкодження цих активів або систем. Частково метою цього кроку є керівництво процесом збору даних.

#### Дані Збір даних

Третій крок полягає у зборі даних про пріоритетні інфраструктурні об'єкти та системи для того, щоб охарактеризувати висхідні та низхідні залежності ключових зацікавлених сторін. Загальнодоступні набори даних з відкритих джерел, опубліковані урядовими, некомерційними, освітніми, торговельними, дослідницькими та іншими неурядовими організаціями, є гарною відправною точкою для збору даних. Дані про інфраструктуру, зібрані приватними організаціями, можуть бути доступними для придбання у власних наборах даних. Обмеження на використання цих наборів даних, однак, можуть забороняти ділитися відповідною інформацією та результатами аналізу з ключовими зацікавленими сторонами, обмежуючи таким чином корисність даних. Перш ніж купувати приватні набори даних, важливо ретельно оцінити обмеження на використання приватних даних. Поза поєднанням публічних і приватних наборів даних

Для отримання відповідних даних про інфраструктуру процес збору також передбачає запит даних безпосередньо від ключових зацікавлених сторін та комунальних підприємств, які надають їм основні послуги. Крім того, опитування, відвідування об'єктів, фасилітовані дискусії та структуровані інтерв'ю з ключовими зацікавленими сторонами є ефективними засобами збору даних. Дані, що становлять інтерес, включають інформацію про вразливості інфраструктури, залежності та операції, а також інформацію про політичне та соціально-економічне середовище, в якому існують та функціонують ці об'єкти інфраструктури.

#### Інфраструктура Аналіз

Після того, як всі необхідні дані зібрані, наступним кроком є оцінка ефективності інфраструктурних систем. Конкретні потреби ключових зацікавлених сторін, визначені на першому етапі, визначають, який тип аналізу інфраструктури слід проводити на четвертому етапі. Методології аналізу на рівні системи (зверху вниз) можуть надати інформацію про функціонування інфраструктурних систем і оцінити каскадні збої в інфраструктурній системі, що виникають після виходу з ладу активів у цій системі. Підходи на рівні активів (висхідні) дозволяють оцінити вразливість і стійкість конкретних об'єктів інфраструктури. Поєднання підходів на рівні системи і на рівні активів дозволяє оцінити каскадні та ескалаційні збої в інфраструктурних системах після виведення з ладу інфраструктурних активів, а також полегшує визначення критично важливих об'єктів інфраструктури для визначення пріоритетних напрямків підвищення стійкості та інвестицій.

#### Визначення стійкості Стратегії

П'ятим кроком концепції є розробка стратегій, спрямованих на усунення недоліків у сфері стійкості, виявлених на всіх інших етапах концепції. Заходи з підвищення стійкості можуть бути спрямовані на усунення вразливості та залежності критично важливих активів, що належать ключовим зацікавленим сторонам та комунальним підприємствам. Цей останній крок має на меті запропонувати стратегії стійкості, що застосовуються як на рівні активів, так і на регіональному рівні. Якщо ключові зацікавлені сторони мають значну вразливість через залежність від видобувних підприємств, стратегії стійкості часто передбачають оцінку потенційних альтернативних або резервних можливостей, а також посилення комунікації з власниками та операторами відповідних комунальних підприємств та інфраструктури. Однією з головних цілей цього кроку є поширення важливих висновків і запропонованих стратегій стійкості за допомогою інформаційних бюлетенів, громадських форумів, фасилітованих дискусій, семінарів, презентацій, звітів та інших методів комунікації.

### Операціоналізація критичних

**Інфраструктурні взаємозалежності**

Для того, щоб бути ефективними, зусилля зі зниження ризиків повинні бути спрямовані на більш широке підвищення стійкості громади або регіону, що вимагає врахування взаємозалежностей всередині та між інфраструктурними системами. Запропонована система використовує класичні підходи до управління ризиками і може здатися спрощеною для розгляду всіх елементів - тобто категорій, класів і вимірів, що характеризують взаємозалежності критичної інфраструктури. Ця простота також є сильною стороною системи. Аналітики знайомі з цією специфічною структурою оцінювання, і вона забезпечує достатню гнучкість для адаптації рівня оцінювання до потреб користувачів і можливостей аналітиків.

Щоб бути по-справжньому ефективною, необхідна система аналізу:

* Робоче середовище, засноване на довірі.
* Процеси роботи з конфіденційною інформацією.
* Координація на рівні громади або регіону.

Розвиток довіри між ключовими зацікавленими сторонами та аналітиками необхідний для сприяння створенню спільного та міждисциплінарного робочого середовища. Різноманітна участь також дає змогу врахувати в аналізі соціальні, економічні та технічні міркування. Процес є повністю ефективним, коли в ньому беруть участь усі ключові зацікавлені сторони, залучені до управління критичною інфраструктурою та управління в надзвичайних ситуаціях, включно з громадськістю. Окрім розбудови довіри, важливо також запровадити механізми впровадження стандартів і політик, які сприяють спільним підходам і партнерству між власниками та операторами об'єктів критичної інфраструктури і представниками уряду.

Коли середовище довіри створено, необхідно впровадити механізми комунікації для підтримки балансу між захистом конфіденційної інформації - з точки зору бізнес-чутливості та/або національної безпеки - і наданням ключовим зацікавленим сторонам, керівникам надзвичайних ситуацій та державним установам необхідної інформації для підтримки стратегій управління стійкістю. Принципи обміну інформацією та розвідданими за участю ключових зацікавлених сторін описані в главі 11. Розуміння регіональних можливостей має першорядне значення для координації стратегій забезпечення стійкості. Однак зловмисники можуть використовувати інформацію про взаємозалежності інфраструктури для створення вразливостей у сфері безпеки. Визначивши слабкі місця системи і визнавши їхня система може вийти з ладу, власники та оператори інфраструктури також можуть втратити довіру громадськості, що потенційно може призвести до серйозних економічних наслідків.

Координація на рівні громади або регіону важлива для визначення прийнятного рівня наслідків не лише для самих об'єктів критичної інфраструктури, ай для всієї території, яку обслуговують системи критичної інфраструктури. Розуміння взаємозалежності критичної інфраструктури і визначення допустимих рівнів порушень є важливим для визначення пріоритетів у захисті, пом'якшенні наслідків, реагуванні та відновленні. Захист критичної інфраструктури, особливо в складних міських районах, які часто стають мішенню для терористів, має бути зосереджений на виявленні та визначенні пріоритетності потенційних точок відмови, які матимуть найтяжчі наслідки. Координація на рівні громади або регіону в поєднанні з аналізом критичності допоможе власникам і операторам інфраструктурних систем та державним установам визначити пріоритетні об'єкти для поглибленої оцінки безпеки та стійкості, а також обґрунтувати інвестиційні рішення щодо забезпечення стійкості.

### Висновок

Інфраструктурна взаємозалежність є важливим елементом для країн-членів і партнерів НАТО, який необхідно враховувати при управлінні системами критичної інфраструктури, посиленні їхньої безпеки і стійкості, а також підтримці суспільних функцій. На взаємозалежність інфраструктури впливає декілька елементів, від різних класів залежностей до характеристик соціально-економічного середовища. Незважаючи на те, що моделювання взаємозалежностей критичної інфраструктури може здатися надто складним, можна оцінити ці складні та динамічні взаємозв'язки шляхом поєднання методів оцінки "зверху-вниз" і "знизу-вгору" в адаптивній і гнучкій системі аналізу. Спираючись на спільний процес, що сприяє обміну інформацією та визначенню пріоритетності об'єктів критичної інфраструктури, система оцінки може сприяти кращому розумінню функціонування інфраструктури і допомогти зацікавленим сторонам передбачити і підготуватися до потенційних каскадних і ескалаційних збоїв.

Мета оцінки взаємозалежностей критичної інфраструктури - вийти за рамки традиційних, ізольованих підходів до оцінки та управління ризиками. Запропонована в цьому розділі концепція може допомогти аналітикам перейти до розробки скоординованих стратегій стійкості, які враховують потреби ключових зацікавлених сторін, різноманітні дані про інфраструктуру та поєднання аналітичних методів, включаючи моделювання між Альянсом і стрес-тестування, що в кінцевому підсумку сприятиме більш ефективному прийняттю рішень.

У світлі ризиків, спричинених складними природними, техногенними і соціально-технічними загрозами, з якими стикається НАТО, аналіз взаємозалежності інфраструктури допоможе країнам-членам і країнам-партнерам отримати міждисциплінарне і багатовимірне розуміння того, як функціонує критична інфраструктура. Використання цього глибшого розуміння того, як ці інфраструктурні активи і системи працюють разом - як у звичайних, так і в напружених умовах, спричинених тероризмом, - буде необхідним для розбудови і збереження довгострокової життєздатності НАТО в XXI столітті.

# - 13 -

## Оцінка та управління ризиками безпеки

Джеффрі Френч

Як Організація Північноатлантичного договору може найкраще управляти і оцінювати ризики для безпеки в умовах, що постійно змінюються? В певному сенсі управління ризиками безпеки є інтуїтивним і природним набором суджень, які люди роблять щодня. Наприклад, використання інформації про погоду або поточні події для прийняття рішень про те, чи варто носити з собою парасольку, брати з собою певні цінності або повністю скасувати захід, є звичайним способом передбачити те, що може статися, і вжити запобіжних заходів проти цього. Однак складні, довгострокові рішення або рішення, що мають серйозні наслідки, не можуть покладатися на інтуїтивні або ситуативні процеси, сподіваючись на стабільно позитивні результати. Організації та громади потребують формальних процесів для визначення ризиків, визначення їхньої пріоритетності та реагування на них. Постійне вдосконалення цих процесів та їхніх результатів вимагає документування та циклічного перегляду. Ці, на перший погляд, прості концепції можуть стати складними, оскільки вони стосуються складних ризиків, таких як стихійні лиха і тероризм, але, тим не менш, вони лежать в основі дисципліни управління безпековими ризиками. У цьому розділі розглядаються ці концепції і те, як вони трансформуються в урядові програми захисту критичної інфраструктури від різних загроз, підкреслюється роль, яку має відігравати національна програма управління ризиками для координації діяльності організацій державного і приватного секторів, що беруть участь в операціях на об'єктах критичної інфраструктури, а також наголошується на необхідних характеристиках високоякісних національних програм управління ризиками.

### Визначення ризиків для безпеки Управління

У середині 1990-х років Сполучені Штати створили Об'єднану комісію з безпеки для перегляду процесів прийняття рішень, які лежать в основі державних інвестицій у фізичну та інформаційну безпеку. Комісія відзначила, що менталітет часів холодної війни призвів до того, що інвестиції в безпеку ґрунтувалися на нереалістичних припущеннях про загрозу і акцент робився на усуненні ризиків. Результатом такої ментальності стало те, що заходи безпеки були несистемними, важко обґрунтованими і дуже дорогими. Комісія рекомендувала підхід, який би збалансовував ризик втрат і збитків з витратами на контрзаходи: "раціональну, економічно ефективну і довготривалу систему, що використовує управління ризиками як основу для прийняття рішень у сфері безпеки". Багато в чому бачення, встановлене комісією, залишається ідеалом, ще не досягнутим і не вдосконаленим. Робота комісії залишається актуальною і через десятиліття, тому що проблеми, які вона визначила, залишаються актуальними.

Офіс урядової підзвітності США (GAO), який, серед іншого, підтримує нагляд Конгресу за установами і відомствами виконавчої влади, вважає управління ризиками безпеки фундаментальною частиною процесу прийняття рішень. GAO заявляє, що впровадження "принципів управління ризиками може допомогти політикам приймати обґрунтовані рішення щодо найкращих способів визначення пріоритетності інвестицій у програми безпеки, щоб ці інвестиції були спрямовані на ті сфери, які найбільше потребують допомоги".2 У цьому сенсі управління ризиками безпеки є невід'ємною частиною планування і комунікації. Воно дозволяє керівництву бачити конкуруючі потреби у сфері безпеки і визначати пріоритети інвестицій в політику, людей, обладнання чи системи. Інформування про ці пріоритети в стратегічному плануванні та організаційній діяльності допомагає сформувати культуру в установі, місцевості чи громаді.

Частиною цієї комунікації є прийняття і послідовне використання термінів та їхніх визначень. Існує багато способів визначити *ризик*. Міжнародна організація зі стандартизації (ISO) визначає ризик як "вплив невизначеності на цілі".3 Хоча це визначення ISO має перевагу широкого застосування в багатьох сферах, воно може бути занадто загальним для простого застосування в контексті безпеки. Науково-технічна організація НАТО визначає ризик для якісного оцінювання ризиків як "потенційну можливість втрат для організації або суб'єкта". Аналогічно, у Спільній публікації НАТО щодо захисту збройних сил ризик визначається як "функція вартості активу і ... порівняно з потенційним впливом використання вразливостей загрозами і небезпеками".5 Важливим елементом усіх цих визначень є те, що ризик безпеки враховує відносну ймовірність - включаючи як загрозу, так і вразливість - і наслідки небажаних подій.

Ці терміни особливо важливі у сфері безпеки та стійкості критичної інфраструктури (CISR), оскільки CISR передбачає консорціум організацій: військових і цивільних, державних і приватних, кожна з яких має власну культуру і словниковий запас. Різноманітність типів інфраструктури, яку потрібно захищати, і типів загроз, які потребують уваги, створює запаморочливо складну ситуацію для лідерів урядів і промисловості. Тому чітка комунікація вимагає чіткої термінології. Простої мови недостатньо. GAO стверджує, що *управління ризиками -* це "стратегічний процес, який допомагає політикам приймати рішення щодо оцінки ризиків, розподілу обмежених ресурсів і вжиття заходів в умовах невизначеності".6 Лідерам потрібен цілеспрямований аналітичний підхід, який допоможе їм зрозуміти короткострокові і довгострокові ризики, щоб вони могли приймати обґрунтовані рішення щодо розподілу ресурсів. Аналіз ризиків безпеки може слугувати таким підходом для організації та її зацікавлених сторін за умови, що організація використовує обґрунтовані методи, впроваджує повторювані процеси та документує свої дані і припущення.

### Управління ризиками Рамки

Перспективи управління ризиками полягають у тому, що за умови достатньої однорідності та послідовності лідери можуть приймати кращі рішення завдяки можливості агрегувати ризики на різних рівнях. Тобто, якщо оцінки тактичних ризиків є сумісними, то лідер може почати характеризувати ризик на оперативному або стратегічному рівні. Складність, однак, полягає в тому, що загрози, методи атак, а також інфраструктурні об'єкти і системи можуть дуже сильно відрізнятися. Надто конкретний набір інструкцій щодо того, як вимірювати ризик в одній сфері, може бути безглуздим в іншій. Підхід до оцінки ризику вибухової атаки на будівлю з боку терористів дуже відрізняється з точки зору даних і аналізу від ризику кібератаки на інтелектуальну власність з боку іноземної спецслужби. З цих причин спільнота CISR вже давно покладається на безпеку системи управління ризиками, а не детальне керівництво. Правильно побудована система являє собою незворотний мінімум частин або характеристик процесу управління ризиками, які забезпечують належну обачність, а не визначає модель або підхід.

У Таблиці 13-1 представлені конкретні кроки, описані в ряді вибраних систем управління ризиками - від ISO, НАТО, GAO та Національного плану захисту інфраструктури США (NIPP), - які були розроблені або адаптовані для управління ризиками безпеки. Між цими системами є багато спільного, а окремі системи можуть поєднувати один або кілька кроків, які в інших моделях розмежовані. Їхні спільні риси вказують на ключові сфери згоди (оскільки ці системи розвивалися протягом багатьох років), а також на те, як модель ISO чітко визначає деякі кроки, які інші моделі мають на увазі. Наприклад, інформування про результати оцінки ризиків і процеси прийняття рішень мають вирішальне значення для узгодженої програми, але в системі ISO воно виділено в окремий етап або дію, щоб підкреслити його важливість. Якщо розглядати кроки пліч-о-пліч, то стає зрозуміліше, які мінімальні етапи, в тому числі ті, які деякі моделі поєднують або передбачають, є обов'язковими.

**Таблиця 13-1. Порівняння етапів, викладених у вибраних системах оцінки ризиків**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Структура ризиків** | | | | |
| **Фази** | **GAO** | **NIPP** | **НАТО** | **ISO** |
| **Мета та контекст** | 1. Стратегічні цілі, завдання та обмеження | 1. Встановіть цілі безпеки |  | 1. Визначте контекст |
| **Скринінг та сфера застосування** |  | 2. Визначте активи, системи, мережі та функції | 1. Виявлення небезпек і загроз | 2. Ідентифікація ризиків |
| **Оцінка ризиків** | 2. Оцінка ризиків | 3. Оцінити ризики | 2. Оцініть небезпеки та загрози | 3. Аналіз ризиків |
| **Аналіз управління ризиками** | 3. Оцінка альтернатив | 4. Розставити пріоритети | 3. Розробити елементи управління | 4. Оцінка ризиків |
| **Управлінське рішення** | 4. Підбір керівництва |  | 4. Впровадити контроль | 5. Лікування ризиків |
| **Реалізація** | 5. Впровадження та моніторинг | 5. Впроваджувати захисні програми |
| **Моніторинг** | 6. Вимірювання ефективності | 5. Контролювати та оцінювати | 6. Моніторинг та огляд |
| **Комунікація** |  |  |  | 7. Комунікація |

Важливим аспектом функціональної системи управління ризиками є її циклічний характер. По-перше, вона сприяє організаційній зрілості. У міру того, як організації все більше знайомляться з циклом аналізу та управління, вони стають більш пристосованими до потреби в інформації та даних, а також до спільного розуміння власних цілей. Оскільки організація оцінює ризик кілька разів протягом багатьох років, вона повинна отримувати або генерувати дані, необхідні для більш чіткого розуміння цього ризику. Іншими словами, впровадження циклічної системи управління ризиками підкреслює необхідність прийняття рішень на основі фактичних даних і надає пріоритет інституційному навчанню та накопиченню інформації для створення доказової бази.

По-друге, це заохочує культуру постійного вдосконалення. Періодичний перегляд рішень з управління ризиками дає зрозуміти, що управління - це процес, який необхідно підтримувати. Оцінка минулих інвестицій допомагає прояснити їхню мету, пов'язуючи їх з показниками або критеріями, які визначають успіх. Така оцінка підкреслює потребу в технічному обслуговуванні обладнання, навчанні персоналу та періодичному оновленні процедур.

По-третє, цикл аналізу не гарантує, що організація виявить нові загрози. Він створює умови для регулярного сканування та оцінки нових загроз (таких як гібридні загрози, про які йшлося в розділі 4). Метою є не створення нескінченного переліку ризиків, які потребують інвестицій, а радше розуміння організацією найбільш пріоритетних поточних, майбутніх і потенційних ризиків.

### Національний ризик Програми

Кожна країна стикається з низкою загроз безпеці, яким необхідно протистояти. Багато - якщо не всі - з цих загроз вимагають спеціальних знань, навичок і даних, які спонукають організаційну структуру зосереджуватися на окремих ризиках або вузькому діапазоні ризиків. Має сенс, наприклад, створювати центри, які вивчають урагани, лісові пожежі, землетруси та інші природні загрози, а також правоохоронні, розвідувальні або академічні центри, що спеціалізуються на організованій злочинності або тероризмі. Промисловість також має спеціалізацію за секторами і підсекторами, а в деяких випадках - за конкретними технологіями, що використовуються в процесах (наприклад, системи промислового контролю або системи наглядового контролю і збору даних). Різні типи організацій, відповідальних за CISR, представляють собою центри експертизи або набори знань, і в міру свого розвитку вони розвивають зв'язки між собою. У розділі 10 розглядаються різні зацікавлені сторони та організації, що беруть участь у CISR. Вони навряд чи створять цілісну мережу вузлів і зв'язків без цілеспрямованого планування та координації, що має бути однією з головних ролей програми управління ризиками на національному рівні.

Національна програма аналізу ризиків передбачає не лише проведення аналізу ризиків, але й спрямування та заохочення до збору та узагальнення даних, корисних для аналізу ризиків, а також забезпечення структури, необхідної для порівняння та об'єднання результатів аналізу, де це доречно.7 Таким чином, національна програма з аналізу ризиків може слугувати центральним центром для надання державним і приватним партнерам допомоги в отриманні авторитетних і надійних джерел даних або аналізу. У деяких випадках уряд може виступати в ролі каналу або органу, який дозволяє і заохочує обмін інформацією між суб'єктами приватного сектору. Огляд основних концепцій, які повинні лежати в основі програм обміну інформацією в рамках СІСР, див. у розділі 11.

Створюючи надійні партнерства та мережу достовірних даних, національна програма з оцінки ризиків підтримує розробку політики, що базується на фактах. Система оцінки ризиків дозволяє використовувати інформацію з однієї сфери в іншій. Яскравим прикладом такої довіри є переведення розвідувальних даних, даних правоохоронних органів та аналізу відкритих джерел у формат структурованого аналізу загроз, щоб державні та приватні партнери розуміли відносні рівні загроз і те, як їх належним чином врахувати в аналізі ризиків. Таке партнерство вимагає розуміння і поваги до фахівців, а також готовності виконувати роль посла, спрямовуючи фахівців так, щоб їхній аналіз був корисним для інших зацікавлених сторін. Надто розмитий аналіз загроз (або такий, що не сприяє розумінню намірів, можливостей чи цілей групи) має дуже обмежену цінність для організацій, які потребують розуміння загроз для завершення оцінки ризиків.

Окрім налагодження зв'язків між партнерами з державного та приватного секторів, національна програма управління ризиками повинна оцінити сукупну цінність цих зв'язків і визначити, де існують прогалини в показниках, даних, аналітичних можливостях або оцінках, а потім скоординувати дії для усунення цих прогалин. Будь-яка сегментація інфраструктури, як висхідна, так і низхідна, ймовірно, матиме прогалини або міститиме зони перекриття. Ці сфери потребують процесу управління ризиками для нагляду за виявленням прогалин і дублювання, визначенням їх пріоритетності та усуненням. У деяких випадках ці прогалини та дублювання можуть мати географічний компонент, коли інфраструктурна функція розподілена між юрисдикціями, і жодна з її частин не є пріоритетом для органів місцевого самоврядування, хоча загальна функція є критично важливою, або коли одна юрисдикція отримує вигоду від інфраструктурної функції, але окрема юрисдикція несе певні витрати, не отримуючи вигоди.

Нарешті, національна програма управління ризиками також має відігравати стратегічну роль в управлінні ризиками. Управління ризиками на національному рівні починається зі зміцнення здатності місцевих органів влади та інфраструктурних секторів оцінювати ризики, спираючись на кроки, описані вище. Хоча в основі лежить обмін інформацією, національна програма управління ризиками зобов'язана забезпечити або спрямовувати розробку інструментів, які допомагають проводити узгоджену і послідовну оцінку ризиків. Від цього виграють не лише місцеві органи влади та галузеві організації, а й країна в цілому. Оскільки місцеві органи влади проводять співставні оцінки ризиків, національна програма управління ризиками може отримати більш глибоке розуміння типів ризиків, з якими стикається країна, відмінностей у сприйнятті та відмінностей в управлінні ризиками. Обмін думками та найкращими практиками сприяє поширенню ефективних заходів реагування та мінімізує менш ефективні або недбалі підходи. Такий підхід "знизу-вгору" також може бути корисним для аналізу загроз на національному рівні; місцеві органи влади та правоохоронні органи можуть стикатися з членами злочинних і терористичних організацій, бачити наслідки їхньої діяльності або отримувати повідомлення про підозрілу активність. Місцева інформація може бути дуже інформативною для побудови загальнонаціональної перспективи.

Хоча національне управління ризиками починається з функції управління ризиками, яка гарантує, що ризики належним чином ідентифіковані, пріоритезовані та керовані, воно на цьому не закінчується. Суб'єкт національного рівня має найкращі можливості для того, щоб побачити потенціал для колективних дій. У деяких випадках це можуть бути великі капітальні інвестиції, але часто це можуть бути політичні механізми, які стимулюють поведінку, що максимізує стійкість громади і мінімізує недалекоглядні дії або інвестиції, які приносять користь невеликій кількості організацій і знижують стійкість сектору інфраструктури або навколишньої громади. У таблиці 13-2 наведено приклади державного контролю за ризиками.

**Таблиця 13-2. Державний контроль ризиків у середовищі критичної інфраструктури**

|  |
| --- |
| Організації, які прагнуть контролювати ризики, можуть інвестувати в приміщення, обладнання або людей, серед інших варіантів. Урядові програми, наприклад, можуть розбудовувати державні спроможності у виявленні загроз, спеціалізованому реагуванні чи комунікації. Однак СІСР - це колективні зусилля, що передбачають прийняття окремими організаціями рішень, які впливають на інших. Відповідні урядові установи можуть працювати разом, щоб впливати на колективні зусилля, але рідко мають можливість спрямовувати інвестиції або дії. Державний вплив часто здійснюється через політику, вказівки, стандарти та правила. Дві основні проблеми в цій сфері полягають у наступному: (1) створення ефективних стимулів і (2) притягнення до відповідальності окремих організацій, якщо вони недостатньо відповідально ставляться до ризиків безпеки. Ефективні стимули заохочують організації враховувати ризики, документувати рішення і робити пропорційні інвестиції. Неефективні стимули можуть призвести до марнотратних інвестицій або заохочувати до прийняття ризиків, коли наслідки для громади значно переважають наслідки для організації. |
| Джерела:  Рік Нуньєс-Ваз, Стівен Лорд і Деніел Білусіч, "Від стратегічних ризиків для безпеки до пріоритетів національних сил і засобів", *Виклики безпеки* 10, no. 3 (2014): 23-50.  Пітер Р. Оршаг, "Захист критичної інфраструктури та приватний сектор: Вирішальна роль стимулів", *Журнал ризиків та невизначеності* 26 (2003): 231-49. |

У наступному розділі буде описано основні способи, за допомогою яких національна програма управління ризиками може заохочувати та спрямовувати практику управління ризиками з метою створення сприятливого середовища для СІСР.

### Управління безпекою Ризики

Занадто часто управління ризиками сприймається як відносно простий процес усунення виявлених ризиків у пріоритетному порядку. Насправді, аналіз, необхідний для підтримки рішень з управління ризиками, є настільки ж складним, як і аналіз, необхідний для характеристики та порівняння ризиків у послідовний спосіб. Національна програма управління ризиками несе відповідальність за надання допомоги місцевим, регіональним та національним органам влади в управлінні ризиками, яке може розпочатися з їх належної характеристики та порівняння. Деякі ризики можна порівняти безпосередньо, тоді як інші можна порівняти лише опосередковано через дуже різні підстави для розгляду загрози, вразливості або наслідків. Наприклад, деякі ризики найкраще розглядати в безпосередньому часовому проміжку, тоді як інші вимагають більш довгострокової перспективи. Деякі загрози є постійними, на відміну від інших, які є рідкісними або епізодичними. Національна програма управління ризиками може допомогти в управлінні ризиками шляхом організації ризиків у портфелі.

Портфелі ризиків містять безпосередньо порівнювані ризики, оскільки вони мають схожі міркування щодо факторів ризику. Наприклад, природні загрози, можна змістовно описати через очікувану частоту виникнення, структурну вразливість, стійкість громади та загальний набір наслідків. Ризики тероризму, навпаки, зазвичай розглядають відносну загрозу, що передбачає розуміння різних терористичних груп, їхніх можливостей, намірів і спроможностей, які потім суттєво впливають на оцінку вразливості та наслідків. Кіберзагрози, аналогічно, вимагають іншого способу мислення щодо ймовірності того, що організація або географічний регіон зіткнеться з ними. Див. розділ 3, де розглядаються специфічні для інфраструктури складнощі ризиків кібербезпеки. Хоча всі ці ризики мають певні спільні риси, найкраще визначати їх у межах портфелів. Міжпортфельний аналіз важливий насамперед для оцінки рішень з управління ризиками. Тобто, обробка ризиків або засоби контролю можуть впливати на ризики в декількох портфелях, що допомагає особам, які приймають рішення, враховувати порівняння на високому рівні між портфелями без прямого порівняння окремих ризиків між портфелями. У таблиці 13-3 наведено приклад міжпортфельного аналізу.

**Таблиця 13-3. Управління ризиками на регіональному рівні**

У 2008 році Національний столичний регіон США (NCR) провів оцінку ризиків безпеки для вивчення ризиків безпеки громади. Співпрацюючи з Управлінням з координації національного столичного регіону при Федеральному агентстві з надзвичайних ситуацій, NCR отримав інформацію від партнерів з федерального рівня, рівня штатів, місцевих органів влади та приватного сектору у співпраці з Управлінням з управління ризиками та аналізу Департаменту внутрішньої безпеки США. Аналіз ризиків ранжував потенційні загрози критичній інфраструктурі за сценаріями і запропонував варіанти зменшення ризиків.

Ризик-орієнтований підхід розділив ризики на два портфелі: природні загрози та тероризм, що дозволило провести пряме порівняння ризиків з однаковим обсягом даних. Візуальне порівняння ризиків у межах портфелів дозволило особам, які приймають рішення, не лише зрозуміти їхню відносну серйозність, але й фактори ризику, які зумовили цю серйозність. Крім того, що оцінка допомогла сформувати загальне розуміння ризиків, з якими стикається NCR, вона також допомогла керівництву оцінити інвестиції в управління ризиками. Аналіз дозволив створити стратегічні інвестиційні теми і визначити сценарії в обох портфелях, які можуть бути зачеплені. Цей процес допоміг керівникам зрозуміти, наскільки широкими можуть бути наслідки інвестицій, а також наскільки вони потенційно знижують ризики шляхом усунення загроз, вразливостей або наслідків.

Джерела:

Вільям О. Дженкінс-молодший, *Національний столичний регіон: Стратегічний план 2010 року в цілому відповідає характеристикам ефективних стратегій* (Вашингтон, округ Колумбія: Управління урядової підзвітності, 2011).

Елізабет Джексон, Вільям Л. Макгілл і Крістофер Гелдар, "Аналіз регіональних ризиків: Скоординовані зусилля" (презентація, Щорічна конференція Асоціації безпеки та управління ризиками, Арлінгтон, Вірджинія, 18 червня 2009 року).

Щоб створити середовище, в якому зусилля кожного суб'єкта підтримують і доповнюють зусилля пов'язаних з ним зацікавлених сторін, національна програма управління ризиками повинна охоплювати два підходи високого рівня. По-перше, вона має допомогти спрямувати місцеві зусилля на максимізацію обміну інформацією та сумісності підходів до управління ризиками, щоб можна було будувати перспективи більш високого рівня знизу вгору. По-друге, він має забезпечити достовірність і точність, коли організації повідомляють про результати оцінки ризиків, щоб сформувати спільне розуміння ризиків. У наступних розділах ці два підходи розглядаються більш детально.

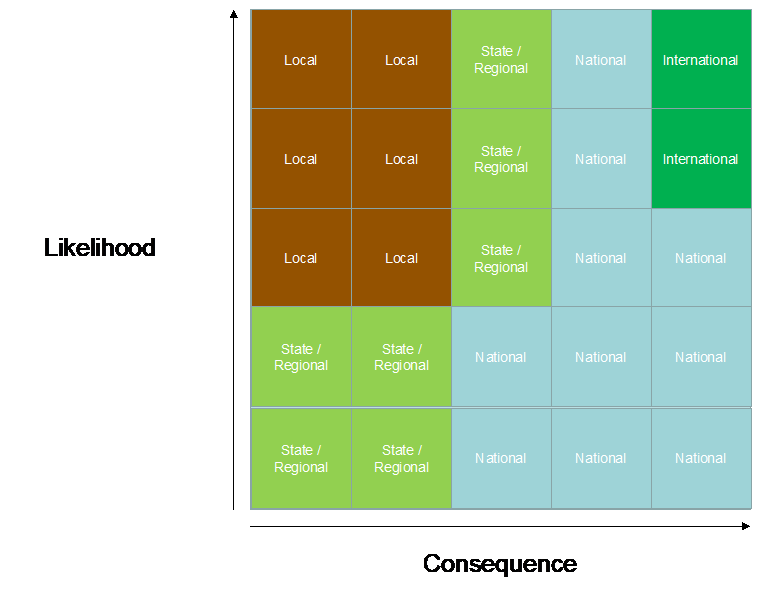
#### Розбудова знизу Вгору

Оцінки ризиків для безпеки, виконані на місцевому рівні, можуть отримати природну перевагу від залучення місцевих експертів, які добре знають географію, небезпеки та населення. На місцевому рівні особи, які приймають рішення, як правило, переймаються насамперед найбільш безпосередніми ризиками: тими, що часто виникають, або тими, що особливо актуальні для даної місцевості. Це має сенс з тієї точки зору, що менеджери з надзвичайних ситуацій хочуть максимізувати інвестиції, які принесуть найбільшу допомогу у вирішенні найпоширеніших проблем. Для того, щоб національна програма ризиків могла скористатися місцевим досвідом, необхідно стандартизувати аналіз ризиків настільки, щоб можна було порівнювати різні оцінки, але без того, щоб він був настільки жорстким або складним, що відволікав би ресурси від зусиль з управління надзвичайними ситуаціями. Певною мірою, найбільш фундаментальною вимогою є те, що основа для розгляду загрози, вразливості та наслідків повинна бути достатньо задокументована, щоб зовнішні експерти розуміли критерії оцінки та визначення пріоритетів.

Національна програма може також надавати вказівки для узгодження цих оцінок, визначаючи період часу для оцінки (наприклад, від одного до п'яти років) або сферу застосування (наприклад, портфелі ризиків або типи загроз, що розглядаються). Там, де державні органи мають регуляторні або наглядові повноваження над секторами інфраструктури, національна програма управління ризиками може заохочувати обмін інформацією з місцевими органами влади для досягнення максимального спільного розуміння ризиків, яким піддаються об'єкти і системи інфраструктури, мінімізуючи при цьому дублювання зусиль. Створення спільноти, яка виробляє обґрунтовані та співставні оцінки ризиків, дозволяє зрозуміти більш складні ризики, такі як аналіз залежностей та взаємозалежностей, про які йшлося в розділі 12. Місцеві органи влади можуть мати власні вимоги до оцінки інвестицій в управління ризиками, але національний уряд може допомогти зробити їх узгодженими, передбачивши аналіз альтернативних варіантів, включаючи початкові витрати, витрати за рік, можливості витрати, сценарії, які отримують вигоду від інвестицій, і ступінь, до якого інвестиції знижують ризики.

Важливо, щоб національні програми управління ризиками зміцнювали взаємозв'язок між різними рівнями влади і розмежовували відповідальність між ними за оцінку та управління ризиками для безпеки. Рисунок 13-1 - це концептуальна модель, яка відображає ці взаємовідносини та обов'язки щодо оцінки та управління ризиками на основі ймовірності їх виникнення та тяжкості наслідків. Вона показує, як місцеві органи влади найкраще підходять для того, щоб зосередитися на ймовірних і керованих на місцевому рівні подіях, тоді як для найбільш ймовірних подій з найбільшими наслідками необхідна міжнародна співпраця. Державні або регіональні органи влади посилюють і розширюють зусилля органів місцевого самоврядування з управління ризиками, в той час як державні програми на національному рівні спрямовані на події з більш серйозними наслідками, навіть якщо вони є малоймовірними.

Забезпечуючи сумісність оцінок ризиків на місцевому рівні та враховуючи вже зібрану галузеву інформацію, програма управління ризиками на національному рівні може агрегувати інформацію для побудови регіональних та національних перспектив.9 Таке порівняння між юрисдикціями має багато переваг. По-перше, воно забезпечує належну ретельність при аналізі ризиків на місцевому рівні. Порівнюючи ризики, які виявляють та оцінюють місцеві юрисдикції, національна програма отримає більш повне розуміння можливих ризиків, заохочуватиме включення пропущених ризиків, де це доречно, та обмінюватиметься найкращими практиками, зокрема потенційними джерелами даних та аналітичними методами. По-друге, міжюрисдикційна перспектива також уможливлює аналіз прогалин, визначаючи ризики, які є надто стратегічними для місцевих юрисдикцій, щоб їх розглядати (як показано на рис. 13-1). По-третє, створення міцної основи для оцінки ризиків у короткостроковій перспективі дає можливість вивчити довгострокові ризики. У таблиці 13-4 наведено приклад одного з підходів до оцінки довгострокових ризиків. Національні програми управління ризиками повинні мати можливість розглядати інвестиції в більш широкому контексті - на великих географічних територіях або в розрізі декількох ризиків.



**Рисунок 13-1. Рівні відповідальності уряду за управління ризиками Таблиця 13-4. Вивчення сценаріїв ризиків з низькою ймовірністю та високими наслідками**

|  |
| --- |
| Розгляд ризиків, які існують у майбутньому або існують, але з низькою ймовірністю, вимагає від осіб, які приймають рішення, впоратися з високим ступенем невизначеності, притаманним цим сценаріям. Існує багато способів вивчення цих ризиків, одним з яких є підхід, відомий як *альтернативний аналіз ф'ючерсів*. Цей підхід зосереджується на визначенні двох основних чинників невизначеності, а потім досліджує їхню взаємодію. Національна розвідувальна рада США використовує цей підхід для свого довгострокового аналізу. Візуальне зображення двох факторів невизначеності створює просту матрицю, а вивчення конкретних сценаріїв у кожному квадранті може зробити ризики більш очевидними.  Важливо розуміти різницю між цими структурованими аналітичними вправами і прогнозами. Такі види аналізу можуть запропонувати багато переваг для керівництва, але не тоді, коли вони обмежують розуміння і дії, зосереджуючись на кількох конкретних сценаріях. Замість цього, такий підхід повинен дозволити лідерам дослідити довгострокові наслідки, які можуть мати нові тенденції, передбачити результати або інновації, найбільш корисні для батьківщини або національної безпеки, а також розглянути партнерів, необхідних для формування цих ризиків. Після цього лідери можуть більш ретельно вивчити певні аспекти нових ризиків і визначити політику, настанови або інші інструменти для максимального підвищення стійкості спільноти критично важливої інфраструктури. |
| Джерела:  Центральне розвідувальне управління (ЦРУ), Структуровані аналітичні методи для покращення розвідувального аналізу (Вашингтон, округ Колумбія: Центр ЦРУ з вивчення розвідки, 2009).  Національна розвідувальна рада, *Картографування глобального майбутнього: Звіт про проект Національної розвідувальної ради до 2020 року* (Вашингтон, округ Колумбія: Урядова друкарня, 2004). |

Розділ 13 Оцінка та управління ризиками безпеки

Ані загрози, ані інфраструктурні системи не прив'язані до національних кордонів. Транспорт, енергетика і телекомунікації мають неминучі міжнародні виміри, які необхідно враховувати. Без транскордонної координації спроби убезпечити окрему частину міжнародної системи ризикують виявитися марними зусиллями. Робота з союзниками може бути прямолінійною, якщо не простою. Угода про політику і стандарти може заповнити багато потенційних прогалин у безпеці. Обмін інформацією і взаємність, і навіть спільне використання технологій можуть мінімізувати тертя в деяких системах, коли вони перетинають кордони. Про те, як Європейський Союз підійшов до цього аспекту управління ризиками, див. розділ 10.

Країни повинні працювати зі своїми союзниками, а також зі своїми конкурентами і супротивниками. У цих випадках значні обмеження перешкоджатимуть обміну деякими технологіями і, можливо, навіть стандартами безпеки, але базове підґрунтя залишається незмінним. Обмін інформацією і комунікація, які забезпечують спільне розуміння переваг безпечної, стійкої інфраструктури, можуть відкрити шляхи для паралельних програм або навіть спільних інвестицій, які забезпечують безпеку транспортних засобів, ланцюгів постачання, доступ до енергетичних і телекомунікаційних систем, серед іншого.

#### Формування спільного розуміння ризиків

Як зазначалося раніше, національна програма з оцінки ризиків несе відповідальність за координацію та інтеграцію аналізу ризиків серед безлічі партнерів з державного та приватного секторів, що беруть участь у КІСР. Така координація не означає нав'язування універсального підходу, але вона означає заохочення використання спільного словника для фахівців з питань безпекових ризиків, щоб складові частини спільноти могли легко спілкуватися один з одним. Це також означає створення механізмів або рубрик для забезпечення порівнянності аналізу ризиків там, де вони не можуть бути однаковими.

Існує багато способів визначити ризик безпеки, його фактори та їх комбінації. На те, який підхід обере та чи інша організація, впливають кілька факторів, зокрема, можливості організації та рівень організаційної зрілості. Зовнішні фактори включають наявність даних та прийнятні кількісні підходи. Що стосується ризику безпеки, то кількісне визначення загрози, вразливості та наслідків може бути дуже складним завданням, а якісні або напівкількісні підходи є єдиними підходами до оцінювання нових ризиків. Пандемія COVID-19 є прикладом ситуації, в якій рішення вимагали врахування ризиків для безпекианаліз до того, як з'явилися дані, але якісні підходи могли б забезпечити розуміння.

Кількісні підходи найкраще підходять для організацій з високим рівнем зрілості в застосуванні ризиків до прийняття рішень, а також там, де існують дані для порівняння сценаріїв, які є достатньо схожими. При об'єднанні або порівнянні аналізів ризиків, проведених кількома організаціями або для різних ризиків, кількісні підходи можуть бути складними для створення або потенційно неможливими. Тому національні програми з управління ризиками повинні запроваджувати найкращі практики у сфері CISR, щоб максимізувати порівнянність, створювати способи змістовного порівняння та об'єднання окремих оцінок ризиків, а також пояснювати, коли слід уникати такої інтеграції. Допомагаючи зацікавленим сторонам і лідерам зрозуміти відносну серйозність ризиків, їхню відмінність і те, які ризики категорично відрізняються, національні програми з управління ризиками можуть сформувати спільне розуміння ризиків і сприяти проведенню освічених дискусій про те, як ними управляти.

Ключовим моментом у цьому спільному розумінні є те, що більшість ризиків безпеки не можна усунути, ними можна лише управляти, і що управління вимагає обговорення компромісів. Наприклад, рівень безпеки в аеропортах можна значно підвищити, але за великі кошти і за рахунок зменшення пасажиропотоку, але суспільство навряд чи буде довго терпіти такі умови. У розділі 6 детально розглянуто компроміси, пов'язані з авіаційною безпекою, а в розділі 7 - як багатогранна природа залізниць ускладнює прийняття рішень щодо інвестицій у безпеку. У будь-якому операційному середовищі контроль ризиків пов'язаний з початковими витратами, а також з втраченими можливостями, які необхідно враховувати безпосередньо. Особливо в середовищі критичної інфраструктури вплив контролю ризиків на функціонування інфраструктурного активу або системи також є необхідним фактором при визначенні, порівнянні та виборі альтернативних інвестицій. Приклад таких рішень з управління ризиками у водному секторі див. у розділі 8. Національна програма управління ризиками може допомогти спільноті CISR впровадити концепції (такі як управління ризиками до "розумно можливого низького рівня") або інші стандарти, які допоможуть зацікавленим сторонам зрозуміти свою індивідуальну та спільну відповідальність.

### Необхідні характеристики якісного ризику Програми

Підходи до аналізу та управління ризиками можуть бути різного рівня зрілості та кількісної оцінки. Наприклад, повністю якісний підхід до ризику може бути корисним і надійним, особливо в питаннях, де відсутні ключові дані або надійний метод кількісної оцінки.13 Проте є три ключові аспекти програми управління ризиками, які не підлягають обговоренню. Оскільки країни-члени і партнери НАТО розглядають і оновлюють свої національні програми управління ризиками, в цьому заключному розділі буде наголошено на необхідності включення цих трьох елементів: прозорість процесу прийняття рішень, чітке інформування про ризики і узгоджене управління ризиками.

#### Прозорість

Управління ризиками впливає на велику кількість зацікавлених сторін. Хоча вигоди мають бути доступними для великої кількості людей, витрати можуть бути розподілені нерівномірно. Існують не тільки альтернативні витрати - інвестиції в людей, обладнання або навчання, які можна було б використати в інших сферах, - але й деякі зацікавлені сторони можуть наражатися на більш високі ризики через загальне управління більшим ризиком. Наприклад, будівництво лабораторії біобезпеки може допомогти державі боротися з небезпечними патогенами в довгостроковій перспективі, але в короткостроковій перспективі це може не сподобатися громаді. Будівництво додаткової електростанції може зміцнити електромережу, але її спорудження також створює екологічні та інші проблеми для громад, розташованих поблизу. Неповні або погано задокументовані оцінки ризиків перешкоджають будь-яким зовнішнім суб'єктам - у тому числі людям, на яких впливають рішення, засновані на оцінці ризиків, - зрозуміти аналіз ризиків, що робить аналіз недійсним, незалежно від якості висновків.

Для того, щоб громади підтримували рішення щодо управління ризиками, лідерам необхідно залучати зацікавлені сторони на кількох ключових етапах. Таке залучення включає розробку сценаріїв ризиків, оцінку наслідків, оцінку методів управління ризиками та моніторинг ефективності. Якщо громади розуміють, на чому ґрунтуються рішення, вони з набагато більшою ймовірністю приймуть ці рішення. Там, де громади були виключені з цих етапів управління ризиками, вони іноді не погоджувалися з остаточними рішеннями, що призводило до затримок або скасування заходів контролю за ризиками. Створення можливостей для належної взаємодії із зацікавленими сторонами покращує якість процесів і підвищує ймовірність прийняття результатів.15

#### Ризик Комунікація

Поширення результатів аналізу ризиків може бути особливо складним завданням. Викладення результатів у зрозумілій для широкого кола зацікавлених сторін формі часто вимагає відходу від наукової або технічної мови, якою користуються аналітики, і переходу до простої мови. Складність полягає в тому, що аналіз ризиків часто містить багато нюансів, і надто просте викладення результатів може перебільшити або применшити ймовірність ризику або серйозність наслідків. Невдале інформування про ризики може викликати паніку або самозаспокоєння. Ситуації, коли політичні інтереси переважають над науковим або професійним консенсусом, підривають розуміння громадськістю ризиків, що може призвести до катастрофічних наслідків.16 Інформування про ризики має починатися до виникнення конкретної загрози або кризи; побудова відносин до кризи підвищує довіру і може підвищити рівень толерантності до ризиків у суспільстві.

Організації повинні планувати комунікацію з громадськістю за допомогою різних методів, щоб ефективно доносити конкретні повідомлення до відповідних аудиторій, особливо під час кризи. Поглиблене обговорення можливостей та інструментів антикризового управління див. у главі 15. Коли криза настає, організації, що займаються консультуванням з питань ризиків, повинні забезпечити своєчасне інформування про ризики і надати конкретну інформацію про характер, місце і час виникнення загроз, а також рекомендації щодо дій у відповідь на загрози. Коли повідомлення про ризики надходять із запізненням, є нечіткими або сприймаються як довільні, вони підривають довіру громадськості та створюють бар'єри для майбутніх комунікаційних зусиль.

#### Ризик Управління

Як зазначалося вище, у більшості країн існує низка різних організацій, що сприяють розумінню ризиків для безпеки, і національна програма з оцінки ризиків має об'єднати їх у цілісну мережу. Частиною цих зусиль є чіткий розподіл ролей і обов'язків між місцевими або регіональними урядовими організаціями та іншими партнерами в приватному і державному секторах. Забезпечення чіткого розуміння кожною організацією того, які ризики вона повинна брати до уваги, допомагає створити середовище співпраці, в якому окремі організації бачать свою роль по відношенню до інших партнерів.20 Такий зв'язок сприяє розвитку культури підзвітності та заохочує організації підвищувати ризики там, де є спільна відповідальність. Регулярні звіти до наглядових органів допоможуть вищому керівництву зрозуміти, які ризики вирішуються (а які потребують додаткових заходів), і максимізувати ймовірність того, що ризики, де немає чітких повноважень або відповідальності, можуть бути ідентифіковані і спрямовані на їх усунення. Коли національні програми управління ризиками допускають високий ступінь невизначеності, вони мінімізують ймовірність того, що вищі керівники визнають ситуації, коли обов'язки перетинаються, але страждають від відсутності співпраці, або коли значні ризики розподіляються між повноваженнями кількох відомств. Чіткі, узгоджені, стратегічні оцінки ризиків у кожному великому портфелі можуть бути одним з основних механізмів, які дозволяють національним урядам зрозуміти ризики для безпеки, з якими вони стикаються, і чи достатніми є заходи з управління ризиками.

# - 14 -

## Підвищення кібербезпеки промислових систем управління

Сонгбек Чо

Завдяки розвитку інформаційно-комунікаційних технологій більшість сучасних об'єктів критичної інфраструктури працює в електронному вигляді. Зловмисники можуть використати будь-які слабкі місця або вразливості в пристроях та обладнанні, що входять до складу цих систем критичної інфраструктури, для здійснення кібератак, які негативно впливають на суспільство та його національну безпеку. Наприклад, кіберінциденти, спрямовані на життєво важливі сектори, такі як електроенергетика, водопостачання та транспорт, можуть не лише спричинити незручності та фінансові втрати для людей і бізнесу, але й викликати соціальні заворушення, зрив військових операцій, а також призвести до людських жертв або загибелі. З цих причин більшість країн розглядають кіберзахист систем та об'єктів критичної інфраструктури як головний пріоритет і докладають значних зусиль для посилення безпеки та стійкості критичної інфраструктури (CISR).

Організація Північноатлантичного договору визначає кібератаки на об'єкти критичної інфраструктури як можливу ситуацію нестабільності, що визначається як майбутня подія, достатньо значна для того, щоб досягти порогу, який вимагає від Альянсу застосування збройних сил.1 Оскільки національні та суспільні функції значною мірою покладаються на інформаційні технології, покращення кібербезпеки стало важливим елементом зусиль держав-членів щодо зміцнення національних СІСР. Так само і НАТО визначила важливий зв'язок між кібербезпекою і здатність виконувати свої основні завдання. На Варшавському саміті 2016 року НАТО офіційно визнала кіберпростір сферою операцій, в якій Альянс повинен "захищатись так само ефективно, як і в повітрі, на суші і на морі". У Варшаві члени Альянсу також пообіцяли зміцнювати і посилювати кіберзахист національних мереж і критично важливої інфраструктури в пріоритетному порядку, підкресливши, що НАТО як організація сильна настільки, наскільки сильна її найслабша ланка.3 НАТО тепер слугує місцем, де члени Альянсу можуть консультуватись з питань кіберзахисту, ділитись інформацією про кіберзагрози, обмінюватись передовим досвідом і координувати діяльність, в тому числі в галузі освіти, підготовки і навчань.4

Залежно від масштабу і тяжкості, кібератака на критичну інфраструктуру країни-члена НАТО може розглядатись так само, як і збройний напад, що виправдовує право країни-мішені на самооборону.5 Руйнівна кібератака також може змусити членів Альянсу застосувати статтю 5 Вашингтонського договору - положення про взаємну оборону, яке передбачає, що напад на одного члена Альянсу є нападом на усіх членів Альянсу, хоча таке рішення буде прийматися Північноатлантичною радою в кожному конкретному випадку окремо. У відповідь на мінливий ландшафт кіберзагроз позиція НАТО проти кібератак була ще більше посилена на Брюссельському саміті в 2021 році, де лідери країн Альянсу визнали, що вплив кумулятивної, зловмисної кібердіяльності може бути прирівняний до збройного нападу.7 Термін "*кумулятивний"* означає, що декілька менш потужних кібератак одного і того ж супротивника з часом можуть бути такими ж руйнівними, як одна масована кібератака.8 Щодо кібероперацій проти супротивників, доктрина НАТО запроваджує концепцію, відому як "Суверенний кібернетичний вплив, добровільно наданий членами Альянсу" - механізм, який дозволяє окремим країнам-членам добровільно підтримувати наступальні кібернетичні сили і засоби інших членів Альянсу в разі збройного нападу на них.

У документі викладені процедури проведення оборонних кібероперацій, включаючи самооборону та колективну оборону, а також визначено порядок проведення оборонних кібероперацій.9

Хоча НАТО вживає заходів для покращення своєї колективної здатності захищатись і реагувати на кібератаки на критично важливу інфраструктуру Альянсу, слід пам'ятати, що першу лінію оборони формують окремі країни-члени. Таким чином, посилення сил і засобів кіберзахисту і вдосконалення політики і процедур CISR є першочерговим обов'язком кожного члена Альянсу. З огляду на ці цілі, ця глава має на меті надати огляд основних питань кібербезпеки, що стосуються критичної інфраструктури, з особливим акцентом на промислових системах управління (ПСУ). Виходячи з цього розуміння, в розділі будуть запропоновані найкращі практики та інструменти для зацікавлених сторін, власників і операторів об'єктів критичної інфраструктури для захисту своїх систем і посилення безпеки і стійкості до кібератак.

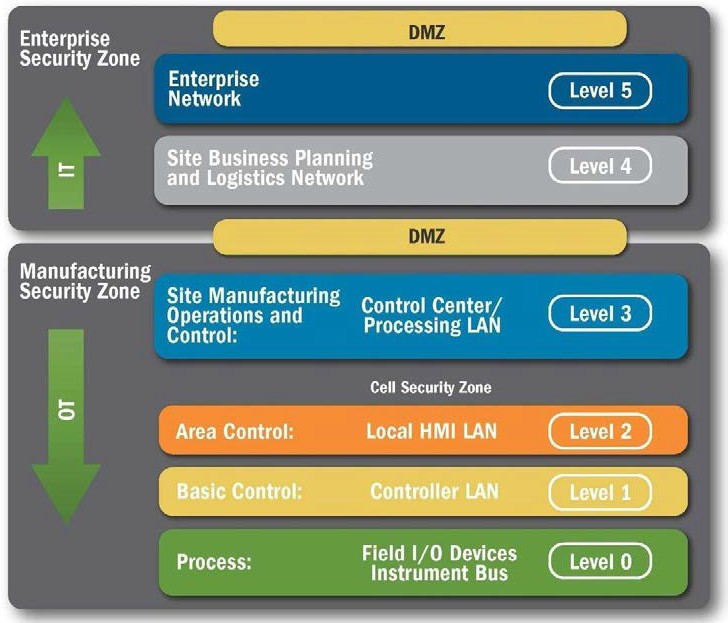
### Огляд промислових систем управління ( ICS)

Розуміння кібербезпеки вимагає належного знання ICS. Термін ICS охоплює різні системи управління, які зазвичай зустрічаються в промислових секторах та критичній інфраструктурі. Також відомі як операційні технології (ОТ), ІКС складаються з комбінацій різних компонентів управління (електричних, механічних, гідравлічних і пневматичних, наприклад) для досягнення промислових цілей, таких як виробництво, транспорт або енергетика.10 Прикладами ІКС є електростанції, електромережі, системи водопостачання та водопідготовки, енергетичний транспорт і залізниця. Хоча ІКС можна конфігурувати і експлуатувати різними способами, є три загальні системи управління, які заслуговують на подальше пояснення.

* Системи диспетчерського контролю та збору даних (SCADA) використовуються для централізованого управління розподіленими активами. Типовими прикладами є розподіл води, збір стічних вод, електромережі, залізниці та інші системи громадського транспорту.
  + Розподілені системи управління (РСУ) керують безперервними виробничими процесами в межах однієї географічної області. Прикладами є нафтопереробні заводи, водоочисні споруди, електростанції, хімічні заводи та фармацевтичні підприємства.
  + Програмовані логічні контролери (ПЛК) - це пристрої, які керують дискретними процесами, наприклад, автомобільними складальними лініями. Хоча ПЛК часто використовується як компонент системи SCADA або DCS, він також може бути реалізований як основний контролер в невеликій ІКС.

Хоча фактичні архітектури ІКС широко варіюються залежно від характеру сектору критичної інфраструктури та типу об'єкта, еталонна архітектура Пердью широко визнана як стандартна модель для загальних систем управління.12 Наявність моделі, яка відображає архітектуру системи управління і показує різні взаємозв'язки між технологічними компонентами, може допомогти організаціям сегментувати різні мережі, розробити зони з чіткими межами і створити рівні заходів кіберзахисту. Міністерство внутрішньої безпеки США (DHS) рекомендує цей процес розробки безпечної мережевої архітектури як засіб обмеження здатності суб'єктів кіберзагроз експлуатувати ІКС, що набагато простіше, коли системи інтегровані і не мають зон або кордонів.13 Міністерство внутрішньої безпеки підтримує розробку багаторівневого кіберзахисту, що складається з п'яти унікальних зон, як показано на рис. 14-1.

**Рисунок 14-1. Еталонна модель ICS**



(Діаграма Міністерства внутрішньої безпеки США)

Перший розділ, зона безпеки підприємства, не має прямого відношення до ІКС. Ця зона забезпечує працівникам доступ до Інтернету, віддалених сайтів та бізнес-мереж, які включають інтрамережу, поштові сервери, веб-сервери та інші бізнес-системи. Зона безпеки підприємства також відома як система інформаційних технологій (ІТ). Корисне пояснення операційних та інформаційно-технологічних систем (ОТ та ІТ) див. у главі 3. Далі йде виробнича зона безпеки, де відбувається переважна більшість моніторингу та контролю. Залежно від розміру ВКІ, ця зона може містити кілька зон камер. Третя секція, зона осередків, містить локальні людино-машинні інтерфейси (HMI), контролери та польові пристрої для моніторингу та управління. HMI - це настільний комп'ютер з керуючим програмним забезпеченням, за допомогою якого операційний персонал маніпулює ICS. Зона осередку також може включати в себе інструментальну систему безпеки, яка є спеціальним контролером, призначеним для автоматичного виконання дій у разі небезпечних умов, таких як надмірний тиск або температура. Протоколи польової шини з жорсткою проводкою зазвичай використовуються між польовими пристроями та контролерами, тоді як Ethernet поширений між контролерами та HMI. Нарешті, демілітаризована зона (DMZ) - це підмережа, яка діє як посередник для захисту внутрішньої мережі. В межах ICS DMZ - це місце, де розташовані реєстратор даних, антивірус або патч, а також шлюз віддаленого доступу. Історик даних - це база даних часових рядів, яка фіксує всі виробничі та технологічні дані для моніторингу та усунення несправностей.

### Проблеми безпеки в ICS

У минулому на об'єктах критичної інфраструктури СУІ працювали виключно в закритому мережевому середовищі. Однак для забезпечення моніторингу в реальному часі та ефективного планування ресурсів на рівні підприємства, в сучасній критичній інфраструктурі переважає практика експлуатації ICS в більш відкритій, взаємопов'язаній мережі з бізнес-мережами. Приклади бізнес-додатків, які можуть підключатися до ICS, включають програми планування і складання графіків виробництва, системи управління виробництвом, системи управління запасами і системи управління технічним обслуговуванням. Крім того, Ethernet та інші технології відкритих стандартів також стають все більш поширеними в ICS. Як наслідок, зловмисникам легше зрозуміти та використати компоненти системи, ніж це було раніше. Ці реалії викликають занепокоєння з приводу безпеки, оскільки ІКС є більш вразливими до кібератак, ніж будь-коли раніше. Якщо порівнювати з ІТ-системами, то наведені нижче системні характеристики ускладнюють захист ІКС перед обличчям численних вразливостей, ризиків і загроз у кіберпросторі.

* Вимоги до своєчасності та продуктивності. Оскільки ICS зазвичай критичні до часу, заходи безпеки, що спричиняють неприйнятну затримку та/або загрожують функціональності системи, не можуть бути розгорнуті.
* Вимоги до доступності. Патчі не можуть бути застосовані вчасно, оскільки вони повинні бути ретельно протестовані на стабільність і надійність. Вимкнення систем для встановлення патчів, як правило, потрібно планувати за кілька тижнів до їх встановлення.
* Вимоги до управління ризиками. Заходи безпеки, які погіршують безпеку, є неприйнятними.
  + Фізичні ефекти. Оскільки в ІКС відбуваються складні фізичні процеси, необхідна хороша комунікація між фахівцями з системи управління та фізичної області.
  + Експлуатація системи. Оскільки операційні системи та мережі ICS часто суттєво відрізняються від ІТ-аналогів, вони вимагають інших навичок, досвіду та рівнів знань.
  + Обмеження ресурсів. Багато компонентів мають обмежені ресурси пам'яті та обчислювальної потужності. Як наслідок, типові сучасні засоби захисту можуть не застосовуватися.
  + Комунікації. Комунікаційні протоколи та засоби зв'язку для польових пристроїв (датчиків та актуаторів) відрізняються від тих, що використовуються в ІТ-середовищі, а отже, потребують інших спеціальностей.
  + Керована підтримка. Враховуючи той факт, що технічне обслуговування часто виконується одним постачальником, використання сторонніх рішень вимагає схвалення постачальника, інакше на ICS більше не буде гарантії.
  + Термін служби компонентів. Термін служби компонентів ІКС часто перевищує 15 років, тоді як ІТ-компоненти потребують оновлення та виправлень набагато частіше.
  + Розташування компонентів. У деяких випадках компоненти ICS можуть бути розташовані на віддалених об'єктах, які потребують значних транспортних зусиль, щоб дістатися до них. Кожен об'єкт має бути належним чином захищений.

Окрім обмежень і перешкод у застосуванні достатніх заходів безпеки, зумовлених самою природою ІКС, існує також низка проблем, пов'язаних з безпекою, які часто зустрічаються в більшості ІКС.

##### Уразливості в ICS Компоненти

Згідно з нещодавнім опитуванням з кібербезпеки, у 2020 році організації розкрили 893 вразливості, характерні для їхніх ІКС, що свідчить про постійне зростання порівняно з 672 у 2018 році та 716 у 2019 році. Дивно, але у 76 відсотках цих вразливостей зловмисники могли здійснювати атаки без необхідності проходити автентифікацію. Ці цифри, однак, не включають вразливості, виявлені у звичайних ІТ-компонентах, таких як персональні комп'ютери співробітників, сервери, бази даних та мережеві комутатори.

Ці компоненти є переважно комерційними готовими продуктами або моделями, створеними на основі цих продуктів на замовлення. Традиційно виробники не вважали безпеку невід'ємною частиною процесу розробки продукту, але ця динаміка змінюється. Незважаючи на нещодавнє зростання занепокоєння щодо безпеки компонентів систем управління під час розробки продукту, рівень безпеки в ІКС відстає і не є настільки всеосяжним, якщо порівнювати з безпекою ІТ-продуктів.18 Тому компоненти ІКС мають багато слабких місць, включаючи вразливість до атак на відмову в обслуговуванні та відсутність перевірок безпеки при оновленні прошивки. Навіть ІТ-компоненти, що використовуються в системах управління, часто налаштовані так, щоб за замовчуванням увімкнути незахищені сервіси, такі як Telnet.

##### Компоненти ІКС, виставлені на огляд в Інтернеті

Багато компонентів ICS підключені до Інтернету без належних заходів безпеки, таких як брандмауери або шлюзи віддаленого доступу. У 2019 році пошук на Shodan - спеціальній пошуковій системі, яку часто використовують для пошуку пристроїв, підключених до Інтернету, - виявив понад 2,6 мільйона компонентів ICS по всьому світу, підключених до Інтернету. Більшість з цих пристроїв, ймовірно, використовувалися в школах для досліджень або невеликими приватними компаніями. Погані практики безпеки або порушення протоколів безпеки (наприклад, відкриття порту брандмауера для віддаленого доступу, а потім забуття його закрити, або навмисне підключення до Інтернету для зменшення робочого навантаження) можуть мати місце навіть у національній критичній інфраструктурі, що робить ці об'єкти та організації однаково вразливими.

### Зв'язок з бізнесом Системи

Згідно з опитуванням 338 організацій, проведеним Інститутом SANS у 2019 році, 57% підключили свої ICS до бізнес-систем, а 35% підключили свої ICS до Інтернету або через демілітаризовану зону, або безпосередньо.21 Якщо таке з'єднання неминуче, його необхідно захистити, щоб запобігти потраплянню шкідливого трафіку в мережу ICS. Для цього можна використовувати брандмауер, але односпрямований мережевий пристрій - спеціальний шлюз безпеки, який також є відомий як діод передачі даних - це оптимальне рішення, оскільки він дозволяє передавати дані лише в одному напрямку. Організації також можуть розглянути можливість використання системи виявлення вторгнень (IDS). Однак, навіть якщо такі пристрої безпеки встановлені, все одно існує ризик проходження шкідливого трафіку через неправильну конфігурацію. Крім того, IDS не можна використовувати, якщо постачальник системи управління не схвалив її через потенційне погіршення продуктивності мережі. IDS частіше зустрічається в ІТ-мережах, ніж в мережах ICS, і навіть якщо вона встановлена, вона може бути не в змозі повністю зрозуміти протоколи ICS.

##### Застарілі Компоненти

Оскільки ІКС зазвичай має дуже довгий термін служби, часто можна зустріти компоненти ІКС, термін експлуатації яких вже закінчився, наприклад, коли на HMI працюють застарілі програми, такі як Windows XP або 7. Навіть якщо організації хочуть оновити старі компоненти, їх неможливо оновити, якщо прикладне програмне забезпечення не підтримує останню версію операційної системи або постачальник не гарантує надійність після оновлення. Встановлення антивірусних програм на старі комп'ютери може бути неможливим через проблеми з продуктивністю та стабільністю. Крім того, коли старе обладнання пошкоджене, може бути нелегко знайти варіанти заміни, які відповідають тим самим технічним характеристикам.

##### Віддалений доступ до керування мережею

З недавнім розвитком хмарних технологій з'явилися хмарні сервіси управління ІТ-системами, і подібні рухи зароджуються і в сфері ІКС. Згідно з опитуванням SANS за 2019 рік, на яке ми вже посилалися раніше, понад 40% респондентів використовували хмарні сервіси для своїх ІКС. Респонденти назвали три основні причини, чому вони використовували ці сервіси: (1) віддалений моніторинг, (2) конфігурація і (3) аналіз, на які припадає 44% повідомлень про використання. Незалежно від типу аутсорсингових послуг, усі види віддаленого доступу повинні контролюватися у максимально безпечний спосіб.

##### Небезпечна природа ICS Протоколи

Всі основні протоколи польових шин, такі як Modbus, DNP3, Profinet та EtherCAT, є вразливими до атак "зловмисника посередині", оскільки вони зазвичай не мають достатньої автентифікації або шифрування.25 Такі атаки можуть порушити роботу мережі або маніпулювати повідомленнями вводу-виводу щоб спричинити збій. Шлюзи протоколів, включаючи перетворювачі послідовного інтерфейсу в Ethernet, які транслюють один протокол ICS в інший, можуть стати додатковим вектором атаки, оскільки вони можуть містити вразливі місця та закони безпеки.

### Основні кібер- інциденти

Через незахищеність конфігурації та управління кіберінциденти в ICS, на жаль, стали звичним явищем. У цьому розділі ми розглянемо деякі з найбільших кібератак, спрямованих на ICS.

##### Stuxnet (2010)

Найбільш історичним кіберінцидентом, пов'язаним з ІКС, стало зараження ядерної програми Ірану вірусом Stuxnet - хробаком, призначеним для проникнення в мережі управління з повітряним зазором через USB-флешки і подальшого саморозмноження шляхом самовідтворення. Хробак Stuxnet, який був виявлений у 2010 році, був точно націлений на центрифуги, що використовуються в іранському процесі збагачення урану, щоб таємно змінювати частоту частотних перетворювачів, які регулюють швидкість обертання двигунів. Вона активується лише тоді, коли виявляється те саме програмне забезпечення - а саме, Siemens WinCC і Step7 - і той самий діапазон частот, що й на іранському об'єкті.27 Хоча фізичні наслідки Stuxnet були обмеженими, оскільки Ірану знадобився лише один рік, щоб повністю оговтатися від наслідків атаки, цей інцидент продемонстрував, що відокремлення мережі ICS від Інтернету більше не можна вважати достатнім заходом безпеки.

##### BlackEnergy (2011)

У 2014 році Група реагування на кібернетичні надзвичайні ситуації в системах промислового управління США (ICS-CERT) попередила, що шкідливе програмне забезпечення BlackEnergy з 2011 року націлене на користувачів таких продуктів HMI, як GE Cimplicity, Advantech/Broadwin WebAccess і Siemens WinCC. Зловмисники обирали підключені до Інтернету HMI, а потім використовували вразливість програмного забезпечення для встановлення BlackEnergy.

шкідливе програмне забезпечення. Хоча зловмисна діяльність не була виявлена, шкідливе програмне забезпечення могло пошкодити, модифікувати або вивести з ладу системи, на які була спрямована атака. Безпекова компанія виявила, що деякі з серверів командування і управління (C2), які використовувалися в цій атаці, були такими ж, як і ті, що використовувалися російською групою Advanced Persistent Threat (APT), відомою під назвою Sandworm. У липні 2021 року уряд США офіційно приписав атаку BlackEnergy російським державним кібератакам.

##### Havex (2013)

Російська група APT, відома як Dragonfly, використовувала Havex у кампанії кібершпигунства, спрямованій на інформаційні системи різних країн, включаючи кілька країн-членів НАТО. Havex - це троянська програма для віддаленого доступу, яка використовувала Open Platform Communications - протокол обміну даними між системами Windows і контролерами - для збору інформації про цільові пристрої. Зловмисники троянізували програмне забезпечення, доступне для завантаження з трьох веб-сайтів виробників ICS, і отримали доступ до мереж систем, на яких було встановлено це програмне забезпечення. Пізніше компанія з безпеки виявила, що 88 варіантів зв'язувалися з 146 серверами C2, які встановлювали з'єднання з 1500 різними адресами Інтернет-протоколу, кожна з яких представляла собою можливу жертву атаки. Хоча основною метою використання Havex було шпигунство, його сервер C2 також міг бути використаний в інших атаках. У 2021 році уряд США поклав відповідальність за атаки через Havex на Росію.

##### Німецький сталеливарний завод (201 4)

Відповідно до щорічного звіту, опублікованого в 2014 році Федеральним відомством з інформаційної безпеки Німеччини (*Bundesamt für Sicherheit in der Informationstechnik,* або BSI), невідомі зловмисники атакували німецький сталеливарний завод, скомпрометувавши окремі компоненти ICS і спричинивши зупинку печі в аномальний спосіб. Зловмисники використовували фішингові електронні листи, щоб викрасти облікові дані для входу в систему, а потім використовували їх для отримання доступу до системи управління комбінатом.

##### Відключення електроенергії в Україні (2015)

Відключення електроенергії в Україні в грудні 2015 року, яке спричинило перебої в електропостачанні для 225 000 людей на заході України на термін до шести годин, стало першим відомим успішним кібервторгненням, що призвело до відключення електромережі, і одним з найсерйозніших інцидентів в історії кібербезпеки. Зловмисники, що входять до складу угруповання Sandworm, здійснили віддалене вторгнення в три енергорозподільчі компанії. Як повідомляється, зловмисники використовували фішинг для отримання облікових даних заздалегідь, що дозволило їм проникнути в компанії, а потім на різні підстанції. Крім того, вони заразили системи Windows шкідливим програмним забезпеченням KillDisk, щоб стерти файли та головний завантажувальний запис, а також пошкодили прошивку перетворювачів послідовного інтерфейсу в Ethernet на підстанціях, щоб зробити їх непрацездатними. Як і у випадку з атаками BlackEnergy та Havex, уряд США також приписав відключення електроенергії у 2015 році Росії.

##### Атомна електростанція RWE, Німеччина (2016)

Комп'ютерні віруси Conficker та W32.Ramnit були виявлені на атомній електростанції німецької комунальної компанії RWE поблизу Мюнхена у квітні 2016 року. Зараженою системою був комп'ютер, який використовувався для перегляду руху ядерних паливних стрижнів, але інфекція не завдала жодної шкоди, оскільки станція була відключена від Інтернету. Таке ж шкідливе програмне забезпечення було виявлено на 18 знімних дисках, які використовувалися для офісних комп'ютерів, що свідчить про те, що принаймні один з офісних дисків був вставлений в заражену систему. Офіційне розслідування також дійшло висновку, що шкідливе програмне забезпечення, ймовірно, прийшло з USB-накопичувача.

##### CrashOverride (2016)

Під час кібератаки на українську підстанцію в грудні 2016 року, яка спричинила невелике відключення електроенергії, угруповання Sandworm використовувало шкідливе програмне забезпечення CrashOverride (також відоме як Industroyer). Цю атаку, як і кілька попередніх прикладів, пізніше приписували російським державним кібератакам. Хоча ця кібератака була меншою за масштабом і тривалістю, ніж та, що спричинила відключення електроенергії в Україні, CrashOverride був розроблений для створення набагато масштабнішого відключення, ніж те, що сталося у 2015 році. Шкідливе програмне забезпечення CrashOverride може надсилати шкідливі команди безпосередньо на віддалені термінальні пристрої - контролери, що використовуються в системах SCADA (наприклад, в електромережах), - використовуючи відсутність автентифікації та авторизації в протоколі ICS. Шкідливе програмне забезпечення також може перешкоджати законному зв'язку з польовими пристроями, викликати відключення реле і використовувати свій модуль очищення, щоб зробити систему Windows інертною і, таким чином, вимагати перезбірки або відновлення з резервної копії.45 Після атаки Stuxnet використання шкідливого програмного забезпечення CrashOverride у 2016 році є лише другим відомим випадком використання шкідливих кодів, навмисно створених для виведення з ладу фізичних систем. Для більш детального пояснення та оцінки кібератак на енергосистему України див. огляд, представлений у розділі 5.

##### TRITON (2017)

Після загадкової зупинки цілого нафтохімічного заводу в Саудівській Аравії у 2017 році подальше розслідування виявило, що зловмисники отримали віддалений доступ до інженерної робочої станції - комп'ютера, який використовувався для налаштування інструментальної системи безпеки (SIS) - за допомогою шкідливого програмного забезпечення TRITON. TRITON, також відомий як TRISIS, - це шкідливе програмне забезпечення, яке атакує SIS Triconex, розроблену компанією Schneider Electric. Шкідливе програмне забезпечення TRITON дозволяло зловмисникам перепрограмувати SIS, що призводило до автоматичного вимкнення контролерів. Хоча достеменно невідомо, хто несе відповідальність за кібератаку, є свідчення, що російський Центральний науково-дослідний інститут хімії та механіки підтримав розробку TRITON. У жовтні 2020 року Міністерство фінансів США наклало санкції на цю російську дослідницьку установу за її причетність до ТРИТОН.48

##### Водоочисна станція, США (2021)

У лютому 2021 року невідомий зловмисник зламав водоочисну станцію в Олдсмарі, штат Флорида. Отримавши віддалений доступ до станції, зловмисник спробував підвищити рівень гідроксиду натрію у водопостачанні до 100 разів більше, ніж зазвичай. На щастя, оперативний персонал швидко помітив цю аномалію і повернув гідроксид натрію до нормального рівня. Пізніше розслідування встановило, що зловмисник отримав доступ до системи через програмне забезпечення для віддаленого доступу під назвою TeamViewer, яке працівники заводу встановили і використовували для перевірки стану системи та реагування на тривоги.49 Міська влада зазначила, що автоматизовані засоби захисту, такі як тестування рН, спрацювали б ще до того, як комусь було б завдано шкоди, навіть якби працівник не помітив і не зупинив атаку.50 Однак цей інцидент чітко показав, що диверсійні атаки, спрямовані на національну критичну інфраструктуру, можуть статися будь-якої миті. Більше інформації про кібератаку в Олдсмарі див. у розділі 8.

##### Колоніальний трубопровід (2021)

Colonial Pipeline, найбільша трубопровідна компанія в США, була змушена на шість днів зупинити свій 5500-мильний трубопровід на східному узбережжі через атаку російського злочинного угруповання DarkSide з метою вимагання викупу.51 Оскільки нафтопровід зазвичай транспортував понад 110 мільйонів галонів пального на день, атака мала руйнівні наслідки: 88 відсотків заправок у Вашингтоні, округ Колумбія, залишилися без пального, як і понад 50 відсотків заправок у Південній Кароліні, Північній Кароліні та Вірджинії. Хоча атака була спрямована лише на ІТ-системи, компанія була змушена зупинити роботу свого трубопроводу, оскільки не могла виставляти рахунки своїм клієнтам. Фундаментальна проблема у цьому інциденті дані, необхідні для роботи трубопроводу, не повинні зберігатися в ІТ-мережі.

### Рекомендації з безпеки для ICS

Для захисту від кібератак, спрямованих на об'єкти критичної інфраструктури, організаціям необхідно дотримуватися належних практик кібергігієни та належним чином впроваджувати методи захисту. У цьому розділі наведено огляд основних практик кібергігієни та рекомендованих заходів захисту критично важливих інфраструктурних об'єктів.

##### Основи кібергігієни Практики

Як фундаментальний принцип кібербезпеки, належна кібергігієна встановлює прості та рутинні заходи для зменшення ризиків від суб'єктів кіберзагроз. У звіті уряду Великої Британії за 2015 рік зазначено, що 80 відсотків кібератак можна було б запобігти, якби організації впровадили прості засоби контролю безпеки.56 Хоча цей відсоток не є специфічним для атак на ІКС організації, аналогічне правило 80-20 може бути застосоване і до них. Більшість згаданих вище інцидентів сталися через неналежні практики безпеки, такі як підключення ICS до Інтернету або бізнес-мережі без належних заходів безпеки, залишення точок віддаленого доступу відкритими без моніторингу, а також відсутність контролю безпеки знімних дисків.

Не існує чіткої сфери застосування кібергігієни. Згідно з опитуванням щодо практик кібергігієни, проведеним Агентством Європейського Союзу з кібербезпеки (ENISA), кібергігієна загалом включає в себе такі загальні практики.

* Ідентифікація апаратного та програмного забезпечення, щоб визначити, чим керувати.
* Застосування безпечної конфігурації та зміцнення для всіх пристроїв.
  + Виправлення систем, щоб підтримувати їх в актуальному стані.
  + Управління вхідними та вихідними даними.
  + Сканування всіх вхідних листів.
  + Мінімізація кількості адміністративних рахунків.
  + Проведення регулярного резервного копіювання даних.
  + Створення плану реагування на інциденти.
  + Забезпечення безпеки по всьому ланцюгу постачання.
  + Включення відповідних засобів контролю безпеки до будь-яких договорів про надання послуг.

Подібно до цих рекомендованих заходів в ЄС, Агентство кібербезпеки та безпеки інфраструктури США (CISA) опублікувало у 2021 році свій "Початковий набір з кібербезпеки" (Cyber Essential Starter Kit) для просування базових практик кібергігієни та сильної культури кіберготовності. Посібник CISA висвітлює основні кроки, які необхідно зробити організації для забезпечення кіберготовності в шести ключових сферах: управління, працівники, критичні системи, оточення, дані та план реагування на інциденти.

##### Основні заходи кібербезпеки для ICS

В той час як члени і партнери Альянсу розглядають шляхи посилення своїх сил і засобів кібербезпеки, існує багато настанов, довідників і стандартів, на які оператори і системні інтегратори КІС можуть посилатись для подальших кроків і рекомендацій з кібербезпеки КІС. Ці документи представляють широкий спектр поглядів і найкращих практик, що застосовуються в різних країнах-членах НАТО:

* + Канада та США: Стандарти захисту критичної інфраструктури Північноамериканської корпорації електричної надійності
  + ЄС: ENISA захищає промислові системи управління
  + Франція: Детальні заходи Національного агентства кібербезпеки (ANSSI): Кібербезпека для промислових систем управління
  + Німеччина: Компендіум з безпеки ІКС Федерального відомства з інформаційної безпеки (BSI)
  + Міжнародний: серія стандартів Міжнародної електротехнічної комісії 62443, яка наразі включає дев'ять стандартів, технічних звітів і технічних специфікацій для забезпечення безпеки систем промислової автоматизації та управління63
  + Сполучені Штати:
    - Каталог DHS з безпеки систем управління: Рекомендації для розробників стандартів
    - Рекомендована практика Міністерства національної безпеки США: Покращення кібербезпеки промислових систем управління за допомогою стратегій глибокої оборони
    - Посібник Національного інституту стандартів і технологій з безпеки промислових систем управління

Оскільки ці документи містять величезні обсяги інформації, в цьому розділі неможливо розглянути їх більш детально. Натомість для членів і партнерів Альянсу і партнерів, які прагнуть посилити безпеку і стійкість своїх критично важливих об'єктів інфраструктури, більш корисною основою є "*Сім кроків до ефективного захисту* критично важливих об'єктів інфраструктури". Проаналізувавши майже 300 повідомлень про кібервторгнення в 2015 році, цей звіт МНБ США визначає сім основних принципів безпеки, які можуть допомогти вдалося запобігти 98 відсоткам цих інцидентів. Принципи та відповідні заходи безпеки, викладені у звіті DHS, наведені нижче.

* + Впровадьте білий список додатків. Цей крок дозволяє запускати лише програми та програми, попередньо визначені адміністратором, ефективно запобігаючи виконанню шкідливого програмного забезпечення.
  + Забезпечити належну конфігурацію та управління виправленнями. Оскільки незапатковані системи є більш вразливими для зловмисників, цей крок наголошує на імпорті та впровадженні перевірених патчів. Він включає відстеження необхідних патчів для кожного ІТ-активу, отримання оновлень з перевірених джерел, перевірку їх автентичності за допомогою цифрових підписів і хеш-значень, тестування на системі, оснащеній функціями виявлення шкідливого програмного забезпечення, а також обмеження підключення зовнішніх ноутбуків до ICS.
  + Зменшення площі поверхні атаки. Щоб мінімізувати вразливості, цей крок спрямований на ізоляцію мережі ICS від будь-яких ненадійних мереж, блокування всіх невикористовуваних портів, вимкнення всіх невикористовуваних служб, обмеження зовнішнього підключення, використання одностороннього зв'язку для зовнішнього підключення, якщо це можливо, і застосування таких заходів, як обмеження мережевого порту або шляху, коли необхідний двосторонній зв'язок.
  + Створіть захищене середовище. Щоб обмежити збитки від порушень в мережі, цей крок передбачає сегментацію мережі на менші логічні анклави (віртуальні локальні мережі), обмеження шляхів зв'язку між хостами та використання безпечних засобів для передачі даних з мереж управління до бізнес-мереж.
  + Керуйте автентифікацією. Оскільки зловмисники прагнуть отримати контроль над законними обліковими даними, цей крок спрямований на обмеження такого незаконного доступу. Ключові кроки включають впровадження багатофакторної автентифікації, коли це можливо, надання користувачам найменших привілеїв, необхідних для виконання обов'язків, впровадження суворих політик управління паролями та відмову від спільного використання серверів автентифікації між ICS та бізнес-мережами, коли використовується централізована автентифікація.
  + Впровадити безпечний віддалений доступ. Щоб протидіяти спробам противника отримати несанкціонований доступ до ICS, цей крок спрямований на усунення віддаленого доступу, де це можливо. Важливими заходами є обмеження будь-якого доступу, який залишається безперервним, реалізація доступу тільки для читання з використанням апаратних односпрямованих мережевих пристроїв, вимога, щоб віддалений доступ був обмежений у часі та контролювався операційним персоналом, застосування однакових шляхів віддаленого доступу для постачальників та співробітників, а також використання двофакторної автентифікації з різними типами токенів.
  + Відстежуйте та реагуйте. У сучасному кібернетичному операційному середовищі активний моніторинг має важливе значення. На цьому етапі рекомендується здійснювати моніторинг трафіку Інтернет-протоколу на кордонах ICS та всередині мереж ICS, використовувати рішення безпеки на основі хостів для виявлення шкідливого програмного забезпечення, переглядати дії входу в систему для виявлення використання викрадених облікових даних, відстежувати зміни в засобах контролю доступу та розробляти обґрунтований план реагування.

Щодо поточних загроз і вразливостей, а також відповідних заходів безпеки для їх пом'якшення, різні організації по всьому світу - в тому числі органи кібербезпеки, групи реагування на комп'ютерні надзвичайні ситуації, групи реагування на інциденти комп'ютерної безпеки, постачальники ІКС і охоронні компанії - постійно публікують поради, попередження, оповіщення і звіти. Оператори та системні інтегратори ІКС можуть бути в курсі нових кіберзагроз та відповідних заходів безпеки, посилаючись на ці документи.

### Управління ризиками для ICS Кібербезпека

Процес управління ризиками є фундаментальним завданням для досягнення кібербезпеки, оскільки він дозволяє ідентифікувати активи, які піддаються ризикам, оцінити рівень цих ризиків, впровадити відповідні заходи, співмірні з рівнями ризиків, а також здійснювати постійний моніторинг та управління ефективністю цих кроків зі зниження ризиків. Розглядаючи практики управління ризиками для ІТ-систем загалом, а не для СУІБ зокрема, мабуть, найавторитетнішим стандартним документом є "*Управління ризиками інформаційної безпеки"* (ISO/IEC 27005)*.*69 Цей документ доповнює міжнародний стандарт "*Вимоги* до *систем управління інформаційною безпекою" (Information Security Management Systems-Requirements)*, впровадження, експлуатація, моніторинг та підтримка ІТ-безпеки. Як показано в документі "*Управління ризиками інформаційної безпеки"*, загальний процес управління ризиками складається з п'яти основних етапів, які описані нижче.

* + Визначення контексту. Цей етап включає підготовчі заходи, такі як встановлення базових критеріїв, визначення обсягу та створення команди з управління ризиками. Базові критерії включають критерії оцінки ризику (як оцінювати ризики), критерії впливу (як вимірювати вплив) і критерії прийняття ризику (порогові значення для бажаного цільового рівня ризику).
  + Ідентифікація ризиків. Цей етап починається з ідентифікації активів, включаючи апаратне та програмне забезпечення, дані, інформацію, системи та процеси. Потім визначається наступна інформація: загрози для цих активів, існуючі заходи протидії, вразливості, якими можуть скористатися загрози, а також потенційні наслідки або збитки, які можуть виникнути в результаті.
  + Аналіз ризиків. Цей крок може бути виконаний з різним ступенем деталізації. Його методологія може бути якісною - масштаб і ймовірність інциденту описуються як низький, середній або високий, або кількісною, яка використовує числові значення, а не описи. Поєднання ймовірності та наслідків визначає рівень ризику для кожного інциденту.
  + Оцінка ризиків. Цей етап допомагає визначити, чи потрібно проводити заходи з управління ризиками для кожного з них, і визначає пріоритетність заходів за рівнем ризику.
  + Лікування ризиків. Існує чотири варіанти обробки ризиків. По-перше, модифікація ризиків полягає у впровадженні заходів безпеки для зменшення ризиків до прийнятного рівня, посилаючись на набір стандартів і найкращих практик. По-друге, утримання ризиків передбачає прийняття ризиків лише тоді, коли їхні наслідки є незначними або перебувають у межах діапазону допустимих результатів. По-третє, уникнення ризиків спонукає зацікавлені сторони змінювати умови або припиняти діяльність, пов'язану з ризиками. Нарешті, розподіл ризиків використовує такі методи, як страхування, щоб підготуватися до залишкових ризиків, які залишаються.

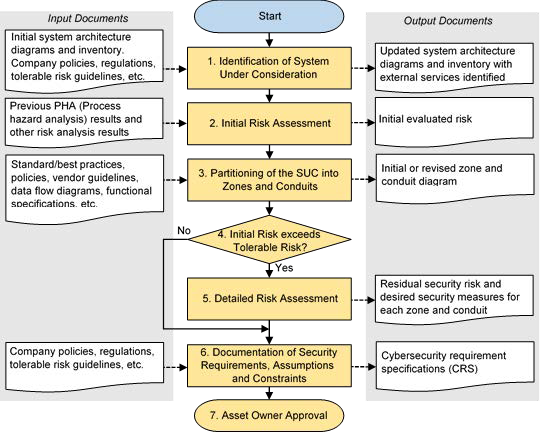
*Управління ризиками інформаційної безпеки* рекомендує організаціям здійснювати процес управління ризиками ітеративно, починаючи з початкової оцінки високого рівня, щоб стисло визначити найбільш критичні ризики з більш широким поглядом на них. Потім організації повинні провести детальну оцінку, яка всебічно аналізує активи, вразливості, загрози та наслідки на другій ітерації та в подальшому. Крім того, організації повинні регулярно здійснювати управління ризиками, враховуючи мінливий характер сучасного середовища безпеки. Див. детальне пояснення процесу оцінки та управління ризиками, викладене в главі 13.

##### Методологія оцінки ризиків для ICS

У 2020 році Міжнародна електротехнічна комісія опублікувала міжнародний стандарт для *оцінки* ризиків ІКС - Оцінка *ризиків безпеки при проектуванні систем* (IEC 62443-3-2) - і прийняла його як частину більш широкої *серії стандартів безпеки для систем промислової автоматизації та управління.*71 Ключовим поняттям в *Оцінці ризиків безпеки при проектуванні систем* є розгляд зон і каналів ІКС. Зона - це сукупність логічних і фізичних активів, що мають однакові характеристики з точки зору вимог безпеки, критичності, а також логічних і фізичних взаємозв'язків. Канал - це логічне об'єднання каналів зв'язку, які мають однакові вимоги до безпеки, і кожен канал являє собою з'єднання між двома або більше зонами.

Ще одним відмінним аспектом стандарту IEC 62443-3-2 є те, що в ньому використовується поняття рівня безпеки (SL) - міра впевненості в тому, що СВК не має вразливостей і функціонує належним чином, щоб допомогти організаціям у визначенні необхідних заходів безпеки. На основі міжнародного стандарту "*Вимоги до системної безпеки та рівні безпеки"* (IEC 62443-3-3), стандартною практикою є присвоєння мітки кожному заходу безпеки від SL1 (базовий рівень безпеки) до SL4 (найсучасніший рівень безпеки).72 Після присвоєння цих позначок організації використовують їх для визначення рекомендованих заходів безпеки, що відповідають їх цільовому рівню захисту. Наприклад, щодо вимог безпеки, пов'язаних з "ємністю сховища системних журналів", IEC 62443-3-3 припускає, що використання сховища з достатньою ємністю буде достатнім для SL1, а для досягнення SL2 або вище слід додати функцію попередження про недостатній обсяг дискового простору.

Подібно до ітеративного підходу, що використовується в *управлінні ризиками інформаційної безпеки,* процес оцінки ризиків ІКС, описаний в IEC 62443-3-2, також поділяється на два рівні, а саме: початкова оцінка ризиків і детальна оцінка ризиків. Процес оцінки ризиків ІКС складається з семи етапів, які описані нижче та проілюстровані на рис. 14-2.



**Малюнок 14-2. Схема робочого процесу для управління ризиками ІКС**

(Діаграма Міжнародної електротехнічної комісії)

* + Ідентифікація системи, що розглядається (SUC). Крок 1 - ідентифікація SUC, включаючи визначення меж ICS, точок доступу та всіх активів ICS.
  + Початкова оцінка ризику. Крок 2 визначає найгірші сценарії, припускаючи, що ймовірність їх реалізації становить 100 відсотків. Метою початкової оцінки є визначення та встановлення пріоритетності сфер для проведення детальної оцінки.
  + Розподіл СУК на зони та канали. Крок 3 включає групування активів СУІБ на основі результатів початкової оцінки таким чином, щоб активи з однаковими характеристиками були згруповані в однакові зони. Організаціям рекомендується групувати незвичайні пристрої (наприклад, бездротові пристрої та пристрої, підключені до зовнішніх мереж) в окремі зони, оскільки вони потребують особливого догляду.
  + Порівняння ризиків. На Кроці 4 організації визначають, чи потрібна додаткова детальна оцінка ризиків для СУП (або її частини), порівнюючи початково оцінений ризик з рівнем ризику, який організація може витримати. Якщо оцінений ризик перевищує допустимий ризик, то організація повинна провести детальну оцінку ризику.
  + Детальна оцінка ризиків. Крок 5 ґрунтується на попередніх кроках і передбачає більш детальне вивчення системи за допомогою низки мікрокроків. На цьому етапі організації (1) визначають усі загрози, які можуть вплинути на активи в межах зони або каналу, (2) визначити сфери, в яких активи є вразливими до цих загроз, (3) розробити найгіршу оцінку потенційного впливу, (4) оцінити ймовірність виникнення таких інцидентів, (5) оцінити рівень ризику для кожної загрози, (6) порівняти оцінений ризик з допустимим ризиком, щоб визначити, чи слід прийняти, передати або зменшити ризик, (7) оцінити залишкові ризики, які залишаються після застосування заходів щодо зменшення ризику, та

(8) визначити додаткові заходи, коли залишкові ризики перевищують допустимі.

* + Документування вимог безпеки, припущень та обмежень. Крок 6 стосується документування всіх висновків, зроблених на попередніх кроках. Специфікація вимог до кібербезпеки містить опис обов'язкових заходів безпеки, а також детальну інформацію про СУК, зони та канали, середовище загроз, політику організації та допустимі ризики.
  + Затвердження власником активів. На останньому етапі кожної ітерації оцінки ризиків власники активів, відповідальні за безпеку та надійність процесів контролю, розглядають та затверджують результат.

##### Детальна оцінка ризиків Підхід

Оскільки детальний підхід до оцінки ризиків забезпечує глибоке розуміння природи ризиків, він лежить в основі управління ризиками для ICS та їх більш ефективного захисту. Процес оцінки ризиків вимагає від організації оцінити ймовірність загрози та наслідки потенційних інцидентів для кожної пари активів та загроз. Цей процес може бути нудним і забирати багато часу та ресурсів, оскільки він вимагає величезних зусиль для отримання значущих і достовірних результатів.

Для оцінки можна використовувати якісні або описові показники, такі як *високий*, *середній* і *низький* рівень, однак вони все одно потребують детального керівництва, щоб максимально зменшити кількість суб'єктивних і неоднозначних суджень. Крім того, вплив має численні характеристики, що вимагають поглибленого аналізу з різних точок зору, наприклад, перебої в роботі, втрата точності процесу, а також вплив на здоров'я, безпеку та навколишнє середовище. Після того, як організація оцінить максимальну потенційну величину впливу та його ймовірність для кожної пари "актив-загроза", вона може визначити рівень ризику.

З іншого боку, якісний аналіз використовує просту логіку відображення для визначення рівня ризику. Наприклад, ризик є високим, якщо ймовірність і вплив оцінюються як високі. Ця логіка, як правило, виражається в матриці, яка називається *матрицею ризиків*, де рядки представляють якісні значення ймовірностей, а стовпці - якісні значення впливів. У кількісному аналізі використовуються числові показники (наприклад, очікувані річні збитки), тобто сума грошових збитків, помножена на ймовірність їх виникнення. Вимірювання та оцінка ризиків слугують основою для прийняття рішення про те, які ризики є пріоритетними за ступенем важливості.

##### Підхід до безпеки на основі сценаріїв Базовий рівень

Для організацій, які не мають досвіду або знань щодо детальної оцінки ризиків, підхід до зниження ризиків на основі сценаріїв може бути корисним як відправна точка для розробки більш надійної та ефективної системи кібербезпеки ICS. Цей підхід розглядає минулі випадки інцидентів або потенційні сценарії для визначення необхідних заходів безпеки, щоб запобігти виникненню таких інцидентів. Він також може бути використаний для оцінки ефективності поточного стану безпеки з відносно меншими витратами часу і ресурсів.

Відповідно до підходу, заснованого на сценаріях, організація спочатку повинна визначити активи, зони та канали в межах ICS, а потім створити каталог сценаріїв загроз, що можуть бути застосовані до них. Для створення якісного каталогу категорій загроз організації можуть збирати звіти про інциденти та попередження або рекомендації з безпеки з різних джерел. Потім організація повинна визначити необхідні заходи безпеки, посилаючись на кращі практики і стандарти або шляхом мозкового штурму з відповідними зацікавленими сторонами та експертами. Наступним кроком є оцінка здійсненності визначених заходів безпеки. Якщо якийсь конкретний захід безпеки не може бути реалізований через бюджетні або технічні обмеження, організація повинна шукати альтернативні або компенсуючі засоби контролю (наприклад, додати процедури ручного контролю або фізичний контроль).

Ключова перевага підходу, заснованого на сценаріях, полягає в тому, що для зменшення ризиків не потрібні додаткові навички аналізу, тому організації можуть виконати цей тип оцінки швидше, ніж детальну оцінку ризиків. Основним недоліком, однак, є те, що деякі важливі ризики можуть бути проігноровані, особливо ті сценарії ризиків, які не мали місця в інших сферах, а отже, не розглядаються як можливі.73 Іншим недоліком є те, що обрані заходи безпеки мало обґрунтовуються з точки зору економічної ефективності, оскільки такий підхід не враховує вплив та ймовірність інцидентів. Надійний каталог сценаріїв загроз міг би певною мірою зменшити ці недоліки.

При створенні каталогу сценаріїв загроз членам Альянсу і партнерам може стати в нагоді "Тактика, методи і загальні знання" (ATT&CK) корпорації MITRE для систем управління промисловістю (ICS) як інструмент і посібник. MITRE розпочала розробку ATT&CK для ІТ-систем у 2013 році, і зараз вона широко використовується як основа для документування та аналізу тактик і методів, що використовуються кібератаками. ATT&CK для ІКС від MITRE, запущений у 2020 році, містить детальну інформацію про 78 методів атак, які зловмисники застосовують у природі, а також відповідні заходи з пом'якшення наслідків, яких організації можуть вжити для посилення своєї кібербезпеки. Ще одним цінним джерелом інформації є Топ-10 загроз і заходів протидії для ICS, який німецький BSI почав публікувати в 2014 році, щоб висвітлити найбільш серйозні, але поширені кіберзагрози і окреслити відповідні заходи безпеки, які повинні вживати організації.

**Захист від кібератак: Погляд у майбутнє**

Кроки, яких власники та оператори критичної інфраструктури вживають для управління ризиками та загрозами у своїх операційних середовищах, є життєво важливими для досягнення кібербезпеки. Уряди цих країн також повинні відігравати проактивну роль у розбудові стійкості та підготовці до потенційних кібератак як на національному, так і на міжнародному рівнях. У наступному розділі обговорюються важливі зусилля, яких мають докласти уряди.

**Зусилля на національному рівні для CISR**

Національні уряди тією чи іншою мірою здійснюють управління кібербезпекою через центральні міністерства та відомства, а також розробляють і оновлюють свої відповідні стратегії кібербезпеки, які передбачають необхідні заходи для захисту критично важливої національної інфраструктури. У 2016 році ENISA опублікувала перелік передових практик на основі детального аналізу різних видів управлінської діяльності в 15 країнах-членах ЄС. Деякі з ключових практик, які у звіті рекомендується запровадити країнам-членам ЄС, наведені нижче.

* + Партнерство з приватними зацікавленими сторонами. Оскільки приватні компанії керують багатьма системами та активами критичної інфраструктури, важливо мати міцне партнерство між урядом і приватним сектором в інституційній формі, наприклад, у вигляді національного комітету із захисту критичної інфраструктури або консультативної наради. Рекомендації щодо державно-приватного партнерства див. у главі 11.
  + Схема обміну інформацією. Інформація про кіберзагрози повинна поширюватися серед усіх відповідних державних установ та приватних операторів критичної інфраструктури через заздалегідь встановлені схеми обміну інформацією. Ці встановлені процедури дозволяють відповідним зацікавленим сторонам оперативно отримувати актуальну інформацію та вживати належних заходів безпеки.
  + Розвивати спільноту команд реагування на інциденти комп'ютерної безпеки. Створення інституційної основи для співпраці між державними та приватними командами реагування може призвести до взаємних переваг, таких як підвищення рівня знань та більш ефективний розподіл ресурсів.
  + Оцінка ризиків. Уряд повинен спрямовувати та підтримувати приватних операторів у визначенні ризиків та впровадженні заходів безпеки відповідно до запитів.
  + Управління кіберкризами. Управління кіберкризою має включати визначення ролей та обов'язків, а також процедур прийняття рішень між відповідними зацікавленими сторонами.
  + Комплексна правова база. Країни повинні мати закони та нормативні акти, що стосуються захисту критичної інфраструктури, які передбачають обов'язкові вимоги до впровадження основних заходів безпеки та повідомлення про кіберінциденти.

Всі перераховані вище кроки важливі, але найбільш життєво важливою практикою є обмін інформацією. Приватні оператори, як правило, не хочуть, щоб їхні інциденти ставали надбанням громадськості, а національні та військові розвідувальні служби, як правило, неохоче діляться своєю конфіденційною інформацією з приватним сектором. Щоб подолати цю проблему, необхідно побудувати довіру до того, що інформація, якою ми ділимося, ніколи не потрапить до інших сторін. Уряд повинен встановити офіційну політику обміну інформацією, включаючи процес санітарної обробки для видалення конфіденційного контенту при поширенні інформації від конкретного оператора до інших операторів. Крім того, підписання угоди про нерозголошення між сторонами також може сприяти зміцненню довіри. Для більш детального обговорення корисних практик обміну інформацією та розвідувальними даними див. главу 11.

Для ефективного та оперативного поширення інформації уряд повинен використовувати засоби зв'язку на основі ІТ-технологій. Залежно від розміру країни, в ній можуть бути тисячі об'єктів критичної інфраструктури, що робить своєчасне поширення інформації про загрози серед усіх власників та операторів майже неможливим за допомогою ручних процедур. У більшості ситуацій інформаційні технології забезпечують більш ефективний і своєчасний майданчик для багатовекторного обміну інформацією між урядом і всіма зацікавленими сторонами. У Сполучених Штатах є два приклади таких програм: Інформаційна мережа національної безпеки (HSIN) та Автоматизований обмін показниками (AIS), якими керують відповідно Міністерство внутрішньої безпеки США та Агентство з питань безпеки і співробітництва в Європі (CISA). HSIN - це інформаційний портал для надійного обміну інформацією між федеральними, державними, місцевими, міжнародними та приватними партнерами. На відміну від HSIN, AIS - це автоматизований механізм поширення інформації в режимі реального часу, який надсилає учасникам спільноти AIS машинозчитувані індикатори кіберзагроз - артефакти, що спостерігаються в мережі або операційній системі, які вказують на кібервторгнення. Прикладами таких індикаторів є адреси Інтернет-протоколу, доменні імена серверів C2 та хеш-значення шкідливого програмного забезпечення.

Окрім рекомендацій, наведених у звіті ENISA, ще дві найкращі практики - це використання кібернавчань та безпека ланцюгів постачання. Оскільки системи і сектори критичної інфраструктури тісно пов'язані між собою, атака на певний об'єкт може вплинути на інші об'єкти інфраструктури, а не обмежитися лише первинною метою атаки. Зокрема, атаки на сектори життєзабезпечення (такі як електроенергетика і телекомунікації) можуть вплинути на всі інші сектори. Для підготовки до кіберкриз на національному рівні уряд повинен регулярно проводити навчання з усіма зацікавленими сторонами. Ці навчання повинні включати процедури прийняття рішень і комунікації в усіх урядових сферах, а також процедури реагування окремих операторів на кібератаки та інформування про них уряду. Найбільшими кібернавчаннями в США є "*Кібершторм",* які зосереджені на управлінні кризовими ситуаціями, пов'язаними з кібератаками, - це найбільші кібернавчання в США. Аналогічно, "*Кібер Європа" - це* масштабні кібернавчання, які тестують процедури, комунікації та прийняття рішень на рівні ЄС.80

Безпека ланцюгів постачання є відносно новою сферою занепокоєння. Ланцюг постачання апаратного і програмного забезпечення, що використовується для критичної інфраструктури, повинен бути захищений від навмисних і випадкових модифікацій, які можуть відбуватися протягом усього життєвого циклу продукції, включаючи розробку, постачання і обслуговування. Зловмисне втручання з боку національної держави у співпраці з виробниками, розташованими на її території, наприклад, шляхом вбудовування "чорного ходу" в компоненти ІТ/ОТ, неймовірно складно виявити. Більше того, злочинні або терористичні групи також можуть завдати шкоди компонентам ІТ/ОТ, проникаючи в середовище розробки виробників для модифікації вихідних кодів. Тому уряд повинен створити структуру для перевірки надійності виробників та забезпечення безпеки продуктів протягом усього їхнього життєвого циклу.

##### Зусилля на міжнародному рівні для CISR

Міжнародна співпраця також має важливе значення для захисту критичної інфраструктури через те, що кіберпростір не має кордонів. Окремій країні практично неможливо ретельно проаналізувати транскордонні атаки і заблокувати подальші, оскільки атаки, як правило, відбуваються в кілька етапів у кількох країнах. Більше того, одна країна може володіти розвідданими, яких немає в іншої. Таким чином, повний аналіз, розслідування та встановлення винуватця атаки вимагають тісної міжнародної співпраці. В ідеалі, всі державні установи, залучені до захисту критичної інфраструктури (такі як національний орган з кібербезпеки, національна і військова розвідка (агентства, кіберкомандування, правоохоронні органи та групи реагування на інциденти комп'ютерної безпеки) повинні мати тісні канали міжнародної співпраці з відповідними колегами в інших країнах. Багатосторонні договори або угоди, такі як Конвенція Ради Європи про кіберзлочинність, також відома як Будапештська конвенція, можуть відігравати вирішальну роль, оскільки всі учасники будуть зобов'язані співпрацювати без необхідності укладати окремі двосторонні угоди один з одним. Будапештська конвенція, яку наразі підписали 66 країн, є міжнародним договором про кіберзлочинність, що передбачає низку повноважень і процедур, необхідних для правоохоронної діяльності. Стаття 23 конвенції передбачає, що міжнародне співробітництво між учасниками повинно здійснюватися в якомога ширшому обсязі.

Так само участь в міжнародних платформах обміну інформацією про шкідливе програмне забезпечення (MISP), таких як MISP, що фінансується НАТО і ЄС, надасть країнам-учасницям актуальну інформацію про глобальні загрози і відповідні індикатори компрометації в режимі реального часу.82 MISP - це платформа обміну інформацією з відкритим кодом, розроблена групою експертів з кібербезпеки з Центру реагування на комп'ютерні інциденти в Люксембурзі, Міністерства оборони Бельгії і НАТО. MISP може обмінюватись, зберігати і співвідносити індикатори компрометації, розвіддані про загрози, інформацію про вразливості і навіть антитерористичну інформацію.83 Члени і партнери Альянсу також можуть розглянути можливість участі в HSIN і AIS, оскільки за певних умов доступ до них може бути наданий і неамериканським організаціям.

Сфери міжнародного співробітництва не обмежуються обміном інформацією про загрози, розвідданими та підтримкою розслідувань. Натомість вона має включати обмін різноманітними ноу-хау і передовим досвідом у сфері кібербезпеки, такими як уроки, винесені з певних типів кіберінцидентів, детальна інформація про технічні заходи кібербезпеки, політики захисту ланцюгів постачання від кіберзагроз, а також інструменти для оцінки рівня кібербезпеки в організації. Оскільки країни обмінюються такою інформацією і надають одна одній технічну підтримку і консультації за запитом, їхня співпраця допоможе створити спільні можливості для досягнення кібербезпеки, захисту і стійкості на рівнях, достатніх для захисту критично важливої національної інфраструктури. Міжнародна співпраця має першорядне значення важливість енергетичної безпеки в цілому, але особливо для країн-членів ЄС, тому що багато секторів і систем європейської критичної інфраструктури взаємопов'язані між собою. Європейська енергосистема, а також нафто- і газопроводи є двома ключовими прикладами такого зв'язку.84 Інцидент в одній країні може вплинути на інші країни, що потенційно може призвести до каскадного ефекту. Більш детально про характер залежностей і взаємозалежностей між секторами критичної інфраструктури див. у главі 12.

### Висновок

У цьому розділі представлено короткий огляд характеристик критичної інфраструктури, основних кіберінцидентів, спрямованих проти неї, основних заходів кібербезпеки та методологій управління ризиками. Кіберінциденти проти об'єктів критичної інфраструктури продовжують відбуватися через неналежні практики управління безпекою, неправильну конфігурацію системи та людські помилки. Оскільки критична інфраструктура відіграє важливу роль у суспільному добробуті та національній безпеці, оператори повинні зберігати відчуття місії кібербезпеки, бути пильними щодо кібератак та інцидентів, а також докладати постійних зусиль для зміцнення систем.

Уряди також повинні докладати величезних зусиль для захисту своєї критичної інфраструктури, встановлюючи обов'язкові вимоги до безпеки об'єктів критичної інфраструктури, забезпечуючи дотримання цих вимог власниками та операторами, а також надаючи консультації з питань безпеки в разі потреби. Крім того, уряди повинні бути прозорими в питаннях безпеки і оперативно ділитися інформацією про загрози з операторами критичної інфраструктури.

Урядові організації, охоронні компанії та виробники мають різні можливості та спеціалізації. Тому необхідно створити інституційний механізм співпраці (наприклад, державно-приватну раду з питань безпеки критичної інфраструктури та спільну групу з питань кібербезпеки), щоб унікальні можливості зацікавлених сторін могли бути інтегровані на національному рівні. Кожна країна також повинна розбудовувати довіру з міжнародними партнерами та активно обмінюватися інформацією та розвідданими. Така співпраця дозволить країнам-однодумцям не лише своєчасно виявляти, запобігати та розслідувати атаки, але й створити основу для міжнародної співпраці, в рамках якої вони зможуть спільно працювати над покращенням кібербезпеки та стійкості, визначати авторство кібератак і вживати узгоджених заходів проти суб'єктів загрози, які їх здійснюють.

# - 15 -

## Кризовий менеджмент та реагування

Малкольм Бейкер

Організація Північноатлантичного договору описує врегулювання *криз* як "скоординовані дії, спрямовані на розрядку криз, запобігання їх ескалації у збройний конфлікт і стримування бойових дій, якщо вони все ж таки відбудуться".1 Як таке, врегулювання криз є важливим компонентом зобов'язань Альянсу щодо посилення стійкості, оголошених у червні 2021 року в рамках ініціативи НАТО - 2030. Невід'ємною частиною цього зобов'язання є філософія Статті 3 - індивідуальна і колективна здатність членів Альянсу протистояти збройному нападу - і здатність НАТО виконувати свої три основні завдання: колективна оборона, безпека на основі співробітництва і врегулювання криз.2 Це зобов'язання ще раз підкреслює, що стійкість країн-членів і партнерів НАТО є одночасно "національною відповідальністю і колективним зобов'язанням".3 Щодо критичної інфраструктури в офіційному оголошенні про НАТО - 2030 також йдеться про посилення зусиль із "забезпечення стійкості нашої критичної інфраструктури (на суші, на морі, в космосі і кіберпросторі) і ключових галузей промисловості, в тому числі шляхом захисту їх від шкідливої економічної діяльності".

Проте, в рамках загальної концепції стійкості і комплексного підходу НАТО до своїх основних місій, чи відповідає нинішня філософія Альянсу щодо врегулювання криз основним тенденціям розвитку сучасного кризового менеджменту і ідейного лідерства? Що ще важливіше, в рамках зусиль із забезпечення безпеки і стійкості критичної інфраструктури (CISR), чи підхід НАТО - 2030 до врегулювання криз все ще відповідає поставленим цілям, чи може він бути вдосконалений для того, щоб відповідати на майбутні виклики взаємопов'язаних систем критично важливої інфраструктури?

У відповідь на ці питання в цьому розділі розглядається широке питання кризового менеджменту в контексті програм СІСР на організаційному рівні Альянсу, а також серед членів і партнерів Альянсу. Наприклад, як врегулювання кризових ситуацій пов'язане з ширшою концепцією стійкості і, відповідно, СІСР? У цьому розділі також розглядається, як ефективні заходи СІСР можуть бути вдосконалені шляхом розробки і впровадження надійних структур і процесів врегулювання кризових ситуацій. Тому при розгляді питань CISR і кризового управління важливо зосередитись на ролі, яку відіграє критична інфраструктура в НАТО, її країнах-членах і партнерах, і на потенційних впливах або наслідках для операцій НАТО, які можуть виникнути, якщо послуги критично важливої інфраструктури будуть ускладнені або недоступні з інших причин. Насамкінець у розділі розглядаються нові події і нові теми у сфері стійкості і врегулювання криз, а також пропонуються пропозиції щодо того, як НАТО може краще узгодити свою діяльність у цій дисципліні на підтримку НАТО - 2030.

### Критично важлива інфраструктура

Як зазначено в розділі 1 на початку цієї книги, Об'єднане командування ОЗС НАТО з питань операцій визначає критичну інфраструктуру як "інфраструктурні активи, об'єкти, системи, мережі і процеси країни, які підтримують військове, економічне, політичне і/або соціальне життя, від яких залежить країна і/або НАТО". У цьому визначенні представлено три різні підкатегорії критичної інфраструктури - критично важлива національна інфраструктура, життєво важлива для місії інфраструктура і ключова інфраструктура - для того, щоб пояснити важливість цих об'єктів або послуг для національної безпеки і/або операцій Альянсу.

За своїм визначенням, критично важлива інфраструктура передбачає надання основних послуг національній державі, її економіці, громадам і громадянам. Звідси випливає, що будь-яка деструктивна подія, що негативно впливає на критичну інфраструктуру, призведе до відповідних негативних наслідків для безперервного постачання цих життєво важливих послуг. Багато сучасних об'єктів критичної інфраструктури є дуже залежними та взаємозалежними від інших секторів критичної інфраструктури, і їхнє функціонування залежить від енергетики, телекомунікацій та інших служб - таких як аварійні служби, правоохоронні органи, а також потенційно місцеві, регіональні та державні комунальні служби - для належного та ефективного функціонування. Поглиблене обговорення залежностей і взаємозалежностей див. у розділі 12.

Критично важливі об'єкти інфраструктури часто є складними, і з часом вони стали більш стійкими до загроз, небезпек і ризиків загалом. Державні та національні програми досягли прогресу в посиленні безпеки об'єктів критичної національної інфраструктури та підвищенні їхньої стійкості до інцидентів, надзвичайних ситуацій і криз. Однак кожен сектор, як правило, підвищує свою стійкість ізольовано, а не комплексно, що частково зумовлено практикою тих секторів, які підлягають державному регулюванню.

### Чому управління кризовими ситуаціями та реагування на них є важливим?

Оскільки вона надає послуги, які впливають на сучасне життя і національну безпеку, критична інфраструктура є економічно важливою для країн-членів і партнерів НАТО, а також для громадян, які покладаються на ці послуги. Критична інфраструктура може належати або державі, або юридичній особі в приватному секторі. У багатьох випадках держава регулює або керує критичною інфраструктурою з точки зору того, як вона функціонує, що вона виробляє або які ціни вона встановлює на товари і послуги, які вона надає. Тому керівники, члени правління та директори компаній об'єктів критичної інфраструктури можуть відповідати перед зовнішніми суб'єктами, такими як держава, державні відомства, регуляторні органи або інвестори.

Залежно від характеру критичної інфраструктури або сектору, в якому вона функціонує, можуть також існувати міжнародні договори або інші багатосторонні угоди чи конвенції, які регулюють, як організація чи об'єкт повинні підтримувати послуги, безпеку та зобов'язання щодо захисту. Такі договори та конвенції також накладають подібні зобов'язання на власників, керівників та операторів об'єктів критичної інфраструктури, які виходять за рамки їхніх традиційних ролей та обов'язків. Директори та члени ради директорів можуть мати обов'язки щодо ефективного та результативного управління організаціями, включаючи управління кризовими ситуаціями та плани реагування, якщо щось піде не так.

### Інциденти, надзвичайні ситуації та кризи: У чому відмінність ?

Терміни "*інцидент"*, "*надзвичайна* ситуація" та "*криза"* часто помилково використовують як взаємозамінні або синонімічні слова для опису події, що сталася, або сценарію, який розгортається. Незважаючи на відмінності, кожен з цих термінів використовується для пояснення негативних або небажаних наслідків. Інциденти, надзвичайні ситуації та кризи можуть мати не лише негативні наслідки, але й інколи створювати позитивні результати або можливості для організацій.

Науковці вже давно пишуть про кризи і управління кризами і розробили визначення того, що є *кризою*. Проте НАТО не має узгодженого або опублікованого визначення *кризи*. Якщо НАТО, її країни-члени і партнери мають намір розвивати структури і процеси врегулювання криз, то життєво важливо мати спільне розуміння терміна "*криза*". Зокрема, які типи сценаріїв Альянс, країни-члени і країни-партнери прагнуть врегулювати, і як ці події - чи то інциденти, чи то надзвичайні ситуації, чи то кризи - можуть бути врегульовані або розв'язані, а їх наслідки пом'якшені або зведені до мінімуму? Чи існує універсальне рішення, яке могло б впоратися з усіма подіями?

У науковій літературі існує безліч визначень того, що таке *криза*. Патрік Лагадек, спираючись на свій ґрунтовний огляд літератури, описує анатомію *кризи* як поєднання невизначеності, невідомості, немислимого, неуявного та непередбачуваного.6 Стівен Фінк визначає *кризу* як "нестабільний час або стан справ, коли насуваються вирішальні зміни - або з явною можливістю вкрай небажаного результату, або з явною можливістю вкрай бажаного і надзвичайно позитивного результату". Інше визначення описує *кризу* як "руйнівну подію або серію подій, які демонструють емерджентні властивості, що перевищують здатність організації впоратися з поставленими перед нею завданнями, і мають наслідки, які можуть вплинути на значну частину організації, а також на інші органи". Деніс Сміт і Домінік Елліотт далі пояснюють, як кризи можуть проявлятися або бути спровоковані внутрішніми або зовнішніми інцидентами, які викривають внутрішню латентну вразливість, притаманну організації. Ці визначення є лише трьома з безлічі інших, запропонованих у Лагадек вважає, що персонал, відповідальний за реагування на кризу та управління нею, потребує більш практичного, а не теоретичного опису, але припускає, що він потребує більш практичного, а не теоретичного опису.

Тому в пошуках більш практичного і реального визначення, яке б відповідало потребам читачів, у таблиці 15-1 пропонуються наступні визначення, що ґрунтуються на опублікованих посібниках з антикризового управління та передовому досвіді Великої Британії.

**Таблиця 15-1. Ключові визначення в антикризовому управлінні у Великій Британії**

|  |  |
| --- | --- |
| **Інцидент** | Несприятлива ситуація, яка може призвести до зриву, збитків або надзвичайної ситуації, але не відповідає пороговому значенню або визначенню кризи, прийнятому в організації. |
| **Надзвичайна ситуація** | Інцидент, який вимагає негайного реагування для мінімізації людських жертв або серйозних травм/пошкоджень; або серйозної шкоди майну. |
| **Криза** | Складна за своєю суттю, ненормальна і нестабільна ситуація, яка через свій масштаб, тривалість і вплив загрожує стратегічним цілям, діяльності, репутації або життєздатності організації, або має стратегічні наслідки для організації. |
| **Кризовий менеджмент** | Розвинена спроможність організації (організацій) готуватися до криз, передбачати їх, реагувати на них та відновлюватися після них. |

Ці визначення, швидше за все, будуть зрозумілі власникам і операторам об'єктів критичної інфраструктури. Крім того, наведене тут визначення *кризового управління* є більш доречним і актуальним для критичної інфраструктури, ніж визначення НАТО, згадане на початку розділу. Зобов'язання посилювати стійкість, яке лежить в основі Стратегії НАТО - 2030, передбачає широкий підхід, що охоплює "весь уряд, приватний і неурядовий сектори, програми і центри експертизи з питань стійкості, створені членами Альянсу, а також наші суспільства і населення з метою посилення стійкості наших країн і суспільств".11 Зважаючи на прагнення Альянсу до реалізації ініціативи НАТО - 2030, розуміння врегулювання криз виключно в контексті збройних конфліктів та інших бойових дій може більше не бути доречним або оптимальним, особливо коли йдеться про різні фізичні, кібернетичні і гібридні загрози, про які йшлося раніше в розділах 2-4. Тому НАТО - 2030 надає можливість оновити зусилля з розвитку більшої стійкості та оновлення підходів до цивільно-військового співробітництва та врегулювання кризових ситуацій.

Визначення, наведені в таблиці 1, що базуються на стандартах, розроблених урядами країн-членів НАТО, можуть виявитися корисними і сприяти виконанню Стратегії НАТО - 2030. Розроблені в результаті вивчення досвіду врегулювання складних, взаємопов'язаних і взаємозалежних криз протягом тривалого періоду часу, вони представляють сучасний і оновлений підхід до стійкості і врегулювання криз.

Також корисно вивчити природу криз, щоб, коли зацікавлені сторони критичної інфраструктури та особи, які приймають рішення, стикаються з такими подіями, вони розуміли типові характеристики кризи і були краще підготовлені до ефективного реагування на неї. Таблиця 15-2 підкреслює унікальну природу криз, порівнюючи їх з інцидентами або надзвичайними ситуаціями на основі шести характеристик.

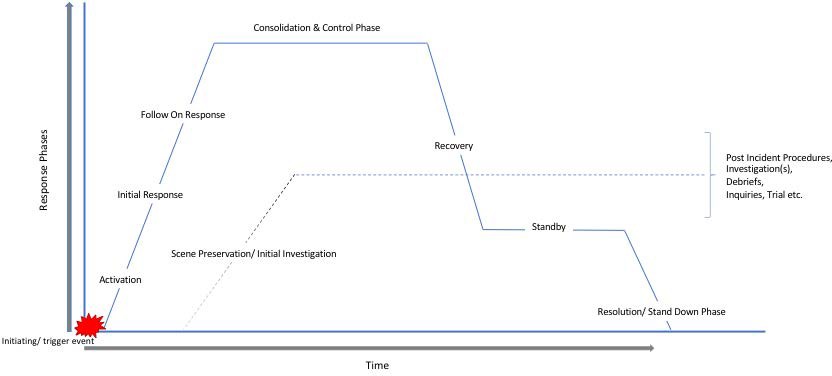
**Таблиця 15-2. Відмінності між кризами та інцидентами або надзвичайними ситуаціями**

|  |  |  |
| --- | --- | --- |
| **Характеристики** | **Інциденти/надзвичайні ситуації** | **Кризи** |
| **Передбачуваність** | * Як правило, передбачувані та керовані за допомогою заздалегідь визначених планів реагування або планів на випадок надзвичайних ситуацій * Терміни, обсяг, тип та   інцидент, і його вплив може бути різним  і непередбачувані в деталях | * Часто рідкісні, непередбачувані, складні та нестабільні за своєю суттю * Може загостритися через неправильне управління подіями * Ставте стратегічні виклики, які   загрожують виживанню організації   * Не реагувати на аварійні плани та заздалегідь визначені   відповіді |
| **Початок** | * Може статися раптово, без попередження або з незначним попередженням * Може з'явитися з часом через поступову відмову або прихований дефект у системах і процесах * Іноді індикатори та попередження про проблему можна відстежувати та розпізнавати як потенційний тригер або фактичну проблему | * Може статися раптово, без попередження або без попередження * Може сформувати подію висхідного припливу, пов'язану з інцидентом, що загострився, і   наразі становить організаційні загрози та стратегічні виклики   * Може проявлятися через латентні   невирішені питання або системні недоліки в організації   * Створюють безпрецедентні репутаційні виклики для організації |

**Таблиця 15-2 (продовження). Відмінності між кризами та інцидентами або надзвичайними ситуаціями**

|  |  |  |
| --- | --- | --- |
| **Характеристики** | **Інциденти/надзвичайні ситуації** | **Кризи** |
| **Невідкладність і тиск** | * Тривалість події та необхідне реагування зазвичай нетривалі * Своєчасне вирішення інциденту запобігає його довгостроковим або згубним наслідкам для організації | * Потребують більшого відчуття організаційної нагальності та стратегічної уваги * Може проявлятися протягом тижнів, місяців або довше * Організація повинна працювати протягом більш тривалого періоду, щоб пом'якшити та мінімізувати вплив |
| **Складність: Масштаб, тривалість та наслідки** | * Часто відбуваються з відносною частотою, тому є зрозумілими та передбачуваними * Організації часто мають заздалегідь розроблені плани та механізми реагування, які можуть бути реалізовані * В окремих випадках може мати ширший вплив | * Може виходити за межі організаційних та територіальних кордонів * Мають потенціал і схильність підривати діяльність багатьох організацій або різних секторів (уряд, приватний сектор або громади) * Часто асоціюється з невизначеністю та недостатньою, неточною або двозначною інформацією * Справжні масштаби та наслідки можуть бути відомі не одразу |
| **Репутація:**  **Увага ЗМІ та громадський резонанс** | * Здебільшого позитивні та прихильні, якщо вони вирішуються надійно та професійно і швидко. * Можуть бути негативними, навіть якщо вони успішно вирішуються * Несприятливе висвітлення може перерости в організаційну кризу | * Створити інтенсивну, стійку увагу громадськості та інтерес ЗМІ * Тривале негативне висвітлення може зашкодити репутації організації * Соціальні медіа та "громадянська журналістика" можуть збільшити кількість неточних повідомлень * Розслідування, слухання або судові процеси після події можуть продовжити інтерес ЗМІ до неї |
| **Вирішення: Керованість за допомогою існуючих планів і процедур** | * Часто вирішуються за допомогою заздалегідь визначених планів, процедур і заходів реагування * Може включати заходи для запобігання інциденту, а також пом'якшення наслідків і відновлення * У більшості випадків наявні адекватні ресурси | * Рідко вирішуються за допомогою звичайних, заздалегідь визначених планів і процедур через притаманну їм складність, нестабільність, нечастість і непередбачуваність. * Потребують гнучкого та інноваційного стратегічного командування та контролю протягом тривалого періоду часу * Може вимагати більше ресурсів і тривалішого періоду * Реагування має досягати стратегічних цілей усіх залучених організацій |

Виходячи з характеристик, наведених у таблиці 15-2, стає зрозуміло, що кризи є більш складними і важкими з точки зору їхньої природи та кроків, необхідних для ефективного реагування на них. Рисунок 15-1 поєднує частини різних моделей антикризового управління, щоб наочно показати анатомію кризи та подальші етапи реагування.



**Малюнок 15-1. Анатомія кризи**

Як показано на рисунку 15-1, подія, що ініціює процес реагування, або тригер, запускає його, але ця подія може бути повільною або поступовою, а не раптовою. Діаграма являє собою загальне зображення, що ілюструє ключові фази кризи. Досягнення консолідації і контролю над кризою може зайняти певний час - це стало надто очевидним під час спалаху пандемії COVID-19 - і ще більше подовжиться через громадські розслідування і слухання, які, ймовірно, відбудуться після цього.

Після того, як ми заклали основу для розуміння природи кризи, доречно розглянути елементи реагування на кризу та управління нею. У корисній концепції Фінк виділяє чотири ключові етапи антикризового управління, які більш детально пояснюються нижче.

* + Продромальна стадія кризи. Це стадія попередження, яку іноді називають передкризовою стадією. Не завжди існує передкризова стадія, оскільки бувають випадки, коли криза приходить без будь-якого попередження. Однак, якщо попередження є, і

якщо її пропущено, то наступна стадія, можливо, є першою ознакою того, що організація перебуває в кризі. На рисунку 15-1 цей етап приблизно дорівнює подіям, що передують події-ініціатору та самій події-триггеру.

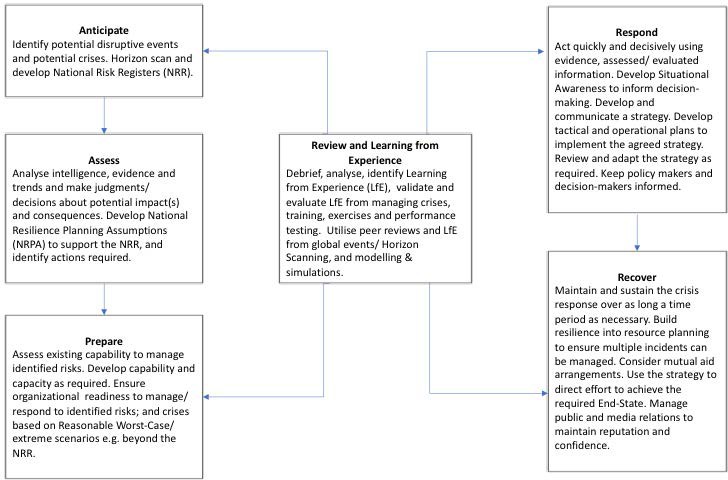
* + Стадія гострої кризи. Цей етап іноді називають "точкою неповернення", оскільки якщо організація не відреагувала на етапі раннього попередження, то вона втратила цю можливість. Однак організація може контролювати деякі аспекти кризи, впроваджуючи заходи з пом'якшення наслідків або обмеження збитків. Гостра стадія є синонімом стадії активації, початкової та подальшої фаз реагування, а також фази консолідації (рис. 15-1).
  + Етап хронічної кризи. На цій стадії відбуваються розслідування, запити та аналіз подій, які часто призводять або до звинувачень і встановлення винуватців, або до визнання успіхів і можливостей.
  + Етап розв'язання кризи. Цей етап зазвичай відображає розв'язання кризи і, якщо воно було успішним, то за часом має бути максимально наближеним до продромальної фази. Цей етап означає, що організація оговталася від події.

Отже, якщо криза не може бути врегульована заздалегідь визначеними планами і процедурами або не піддається успішному розв'язанню за допомогою таких заходів, то це свідчить про потребу в іншій конструкції антикризового управління. Дійсно, потрібен потенціал антикризового управління. Рисунок 15-1 як спрощена модель узгоджується з концепцією Фінка і є відповіддю на заклик Лагадека до менш теоретичного опису антикризового управління. Ключовими елементами ефективного антикризового управління є раннє попередження, ефективна стратегія, хороша комунікація, лідерство і швидке прийняття рішень.

### Розвиток кризового менеджменту Спроможність

Протягом останнього десятиліття багато країн прийняли концепцію, подібну до британської концепції інтегрованого управління надзвичайними ситуаціями, для розробки своїх національних програм стійкості. Ця концепція, заснована на потенційних загрозах, небезпеках і ризиках, охоплює шість етапів: (1) передбачення, (2) оцінка, (3) запобігання, (4) підготовка, (5) реагування та (6) відновлення управління. Багато в чому ця доктрина і підхід можуть бути застосовані до розбудови спроможностей з антикризового управління, хоча їхні результати відрізняються. Замість того, щоб розробляти плани реагування на інциденти та надзвичайні ситуації як продукти, застосування цього процесу аналогічним чином допомагає розробити систему управління кризами. Ці рамки, своєю чергою, допомагають створити управлінську структуру і процес для ефективного врегулювання криз. НАТО як організація і збройні сили її країн-членів загалом добре обізнані з концепцією і практикою розвитку сил і засобів та спроможностей. Розвиток сил і засобів під час врегулювання криз може відбуватись на основі усталеної, визнаної передової практики розробки вимог до сил і засобів, виявлення прогалин у силах і засобах та визначення ключових кроків, необхідних для розбудови сил і засобів та розвитку потенціалу.

На рисунку 15-2 НАТО, уряди країн-членів і організації приватного сектора (в тому числі власники і оператори об'єктів критичної інфраструктури) мають перевірену систему врегулювання кризових ситуацій.15 Виходячи з попереднього аналізу природи кризи, наведеного в таблиці 15-2, ця система не включає етап запобігання, який міститься в шестиступеневій концепції інтегрованого управління кризовими ситуаціями, тому що кризам рідко можна запобігти. Ця концепція є ітеративною моделлю, яка передбачає постійне вдосконалення, оскільки організації завжди повинні вчитися на власному досвіді. Далі в цьому розділі буде розглянуто кожну фазу або етап концепції.



**Рисунок 15-2. Загальна структура антикризового управління**

(Діаграма Британського інституту стандартів)

##### Передбачайте та Оцінюйте

Ці перші два етапи системи антикризового управління вимагають від організації (такої як НАТО, її держави-члени і країни-партнери або власники і оператори критичної інфраструктури) визнання і розуміння причинно-наслідкових зв'язків між її стратегічними цілями, управлінням ризиками і визначеними викликами, що стоять перед організацією. По суті, організація повинна мати чітко визначений і розроблений реєстр ризиків. Цілком ймовірно, що більшість країн-членів або партнерів Альянсу вже створили реєстр, подібний до Національного реєстру ризиків (НРР), що включає перелік ідентифікованих і оцінених ризиків для держави. Неспроможність розробити надійну і змістовну оцінку ризиків означає, що організація буде неминуче приречена на провал у разі виникнення кризи.

Як правило, доречним є підхід "всі небезпеки, всі загрози", який дозволяє уряду врахувати весь спектр потенційно деструктивних подій, з якими він може зіткнутися. Див. обговорення підходу "всі небезпеки, всі загрози" в розділі 2. Цей процес передбачення включає визначення ризиків, оцінку ймовірності або вірогідності їх виникнення, розуміння безпосереднього впливу та екстраполяцію впливу для розуміння довгострокових наслідків. Як частина методології оцінки ризиків в організації має бути добре розроблений, ретельний і наочний процес сканування горизонту, а також активне раннє попередження, що гарантує, що організація розпізнає ідентифікований ризик на ранній стадії.

Сканування горизонту надає членам і партнерам Альянсу і партнерам корисний інструмент для допомоги в розробці або оновленні національної оцінки ризиків (НОР). Глобальні події і кризи можуть спровокувати або ініціювати процес, коли організація задається питанням, наскільки вона готова, якщо така криза станеться. Для розробки НРР та НОР уряди зазвичай створюють міждисциплінарні групи, яким допомагають відповідні експерти з конкретної теми. У випадку зловмисних загроз було б розумно залучити до цього процесу органи національної безпеки, розвідки та правоохоронні органи. Реєстри ризиків будуються знизу вгору, ефективно включаючи ризики, з якими стикаються організації та відомства на різних рівнях влади. Потім держави складають і оцінюють реєстри ризиків на національному рівні, формуючи НРР і визначаючи ризики найвищого рівня, які мають бути включені в основу НОР. НРР та НОР є основою для розробки системи раннього попередження для виявлення появи будь-якого з ризиків найвищого рівня з метою реагування на них до того, як вони проявлять себе у кризовій ситуації.

##### Приготуватися

На етапі підготовки основна увага повинна приділятися розвитку загальних або специфічних спроможностей, які дозволять організації реагувати на будь-яку ситуацію. Так званою "золотою ниткою", що проходить через цей етап, є зв'язок між реєстрами ризиків, НОР (або його приватною, організаційною версією) та стратегічним поєднанням спроможностей, необхідних для ефективного реагування. Тут потрібен набір припущень щодо планування національної стійкості (НПСР). НПОР - або аналогічний набір припущень планування на рівні організації, власника та оператора критичної інфраструктури - визначає і визначає набір параметрів для кожного ризику. Ці параметри можуть включати, наприклад, оцінку ймовірних смертельних випадків, поранень, оцінки збитків і прогнози щодо того, як довго організація може витримати збій, перш ніж він завдасть серйозної шкоди або збитків. Існує можливість включити фінансові дані (наприклад, оціночні витрати через загибель людей, прогнозовані збитки, спричинені збоями та пошкодженнями, репутаційні витрати та схильність до ризику) до кожного параметра.

Цей набір припущень планування, підкріплений даними, що містяться в НПОР (або його еквіваленті для організації), формує характеристики, наведені в таблиці 15-2, і допоможе визначити вимоги до раннього попередження. Як зазначалося вище, НПРН також допоможе визначити потреби в ресурсах сил і засобів. На цьому етапі є чотири ключові елементи: (1) план управління кризовими ситуаціями (ПУКС), (2) плани і процеси управління інформацією та ситуаційної обізнаності, (3) команда з управління кризовими ситуаціями (КУКС) з чіткою, прийнятною структурою, складом і рівнями повноважень, і (4) стійкість і спроможність КУКС, включаючи добре підготовлений, компетентний і забезпечений достатніми ресурсами персонал.

Важливою умовою ефективного антикризового управління є розробка гнучкого, гнучкого та актуального КПП, стислого та зрозумілого для всіх, хто може бути залучений до його реалізації. КПП повинен містити ключову інформацію, зокрема:

* Рівні повноважень та делеговані повноваження
* Контактні дані ключових співробітників CMT
* Кризові комунікації
* Детальна інформація про те, як активувати CMP та CMT
* Інформація про реагування організації на кризу разом із заходами, які необхідно вжити
* Логістична інформація про місце проведення СМТ, її мету та завдання, а також логістична підтримка у вигляді журналів прийняття рішень, шаблонів управління інформацією та ситуативної обізнаності.

Однією з ключових характеристик кризи, наведених у таблиці 15-2, є притаманний їй рівень невизначеності, який змушує тих, хто реагує, оперувати неоднозначною або недостатньою інформацією. Така нестача інформації перешкоджає ефективному прийняттю рішень. Імперативом під час будь-якої кризи є надання політикам і особам, які приймають рішення, якомога повнішого набору інформації або підкреслення різниці між (1) відомою інформацією і тією, що є в наявності, (2) якої інформації бракує або вона невідома, і (3) які робочі припущення керують прийняттям рішень до отримання конкретної інформації. Тому дуже важливо розробити інформаційні вимоги на ранній стадії, щоб допомогти особам, які приймають рішення, і гарантувати, що під час прийняття рішень рівень невизначеності буде зафіксований.

*Ситуаційна обізнаність -* це термін, що описує стан знань про подію, який може ґрунтуватися на максимальних зусиллях команди під час загострення кризи. Для успішного розв'язання кризи дуже важливо створити і підтримувати ситуаційну обізнаність, а також досягти рівнів спільної ситуаційної обізнаності серед тих, хто керує кризою, і тих, хто реагує на неї. Досягненню високого рівня обізнаності може перешкоджати швидка зміна обставин, масштаб кризи, технологічні обмеження, а також організаційні конфлікти і розбіжності. У деяких випадках для роз'яснення даних можуть знадобитися профільні експерти, або ж питання національної безпеки можуть перешкоджати звичайному обміну інформацією. Доцільно створити інформаційну групу, групу ситуаційної обізнаності або об'єднану групу, укомплектовану представниками різних відомств, які б спільно координували збір, аналіз і поширення інформації. Про найкращі практики обміну інформацією та розвідданими див. розділ 11.

##### Реагування та відновлення

Через характер криз, наведених у таблиці 15-2, важко передбачити реакцію на конкретну кризу до того, як вона виникне, або під час її виникнення. Тому вкрай важливо якнайшвидше задіяти як КМУ, так і КМУ. Хоча можуть існувати деякі загальні перші кроки або дії, які можна здійснити негайно, CMT повинна якнайшвидше створити командний центр, забезпечити загальну обізнаність про ситуацію і розробити робочу стратегію. Визначивши проблеми, прийнявши рішення і призначивши або доручивши дії, стратегія перетвориться на ефективні тактичні та оперативні плани. CMT повинна реєструвати всі прийняті рішення, дії, які були поставлені і виконані, а також ключові нотатки з усіх відповідних зустрічей. У рамках ЦВС і ЦГМ слід встановити ранній бойовий ритм або темп роботи, щоб усі відомства могли звітувати про прогрес і розвивати спільну обізнаність про ситуацію. Парадоксально, але необхідність швидкого реагування і прийняття рішень на ранній стадії часто відбувається в умовах невизначеності і браку інформації. Затримка з прийняттям рішень і розгортанням ресурсів на ранній стадії кризи в очікуванні більшої ясності або визначеності може зашкодити якнайшвидшому врегулюванню і відновленню.

Стратегічне планування раннього відновлення слід розпочинати якомога раніше. Як це часто буває під час операцій за участю багатьох державних установ та представників приватного сектору, ролі та обов'язки змінюються протягом усього періоду управління будь-яким інцидентом, надзвичайною ситуацією або кризовою ситуацією. Тому важливо включити такі протоколи і плани передачі повноважень до ЦПІ.

##### Команда кризового менеджменту та керівництво

Ефективне лідерство в рамках БГК має важливе значення під час управління кризою. Як зазначалося раніше, БГК доведеться мобілізуватися швидко і часто в найкоротші терміни. Через природу та особливості кризи, ситуація не є ідеальною, коли лідери можуть комфортно приймати рішення. Серед багатьох обмежень кризи лідерам доводиться вести переговори в ситуації, що швидко розвивається, часто в середовищі, яке характеризується неточною або нечіткою інформацією, двозначністю, іноді хаосом, і принциповою нестачею часу, щоб збалансувати обережність і зволікання.

У такому середовищі лідерство в СМТ має вирішальне значення для ефективного врегулювання та відновлення після кризи. Лідери і ЦГМ зіткнуться з надзвичайним тиском і складнощами під час подолання кризи, але успішне розв'язання залежить від своєчасного прийняття рішень і належної комунікації. Ці слова справді звучать правдиво: дотримання правильного балансу має вирішальне значення. Як правило, дієве рішення, прийняте вчасно, є більш ефективним, ніж ідеальне рішення, прийняте навіть із запізненням.

##### Тренінги, вправи та навчання від Кризи

Найефективніший спосіб відбору та розвитку лідерів і членів БГЗО - це процес занурення, суворого і реалістичного навчання та тренувань. Організації повинні продемонструвати справжню відданість справі забезпечення персоналу ЦГМ необхідними навичками та знаннями для виконання своїх обов'язків. КМП повинен включати послідовну стратегію, яка забезпечує керівникам і ГВП належні можливості для навчання, розвитку та відпрацювання різних аспектів плану. Організація повинна забезпечити достатню кількість можливостей для повторних тренувань і навчань, щоб БГК могла відпрацювати кілька сценаріїв, варіантів і змінних для відточування своїх навичок, знань і ставлення до кризового менеджменту. Слід чітко розуміти, що навчання призначене для персоналу, який виконує функції керівників і членів ЦГК, тоді як тренування - це відпрацювання плану і взаємодія з іншими установами.

Власники і оператори об'єктів критичної інфраструктури, а також ті, хто відповідає за захист національних активів, повинні оцінити цінність ретельної підготовки і структурованих навчань для підтримки і розробки ефективних заходів і планів з управління кризовими ситуаціями. Навчання забезпечують "процес підготовки, оцінки, відпрацювання і підвищення ефективності діяльності організації".17 Ефективні навчання залучають відповідні об'єкти та організації на місцевому, регіональному та національному рівнях для того, щоб усі партнери розуміли, розробляли та впроваджували необхідні плани реагування, включно з відповідними ПЗК. Навчання надають унікальну можливість різним агентствам з реагування, зацікавленим сторонам і місцевим органам влади перевірити політику, плани і процедури, а також оцінити підготовку, обладнання та міжорганізаційні домовленості. Така перевірка і оцінка повинна включати системи і процеси розробки і реалізації угод і механізмів обміну інформацією та розвідданими.18 Обмін розвідданими та інформацією між партнерами допоможе у прийнятті рішень і забезпечить ефективне врегулювання кризових ситуацій, сприяючи загальній обізнаності про ситуацію.

Належним чином сплановані та проведені навчання є недорогими, але цінними інвестиціями у відносному вираженні. Процес навчання на власному досвіді приносить організаціям багато переваг, і дуже важливо включати цей досвід в оновлені версії ПЗК та оновлені настанови для КГК, щоб забезпечити постійне вдосконалення. Також важливо, щоб власники ПЛМ і КГП регулярно переглядали звіти після інцидентів і огляди кризових ситуацій, які трапляються в інших місцях. Навчання на чужих успіхах, помилках та виявлених сферах для вдосконалення допоможе організації у розробці та вдосконаленні ПЦП та СМТ.

##### НАТО і криза Управління

НАТО визначає врегулювання криз як одне зі своїх фундаментальних завдань у сфері безпеки, а Стратегічна концепція 2010 року окреслює роль Альянсу в врегулюванні криз. В рамках своїх організаційних можливостей врегулювання криз і реагування на них НАТО може використовувати традиційні військові засоби або цивільно-військове співробітництво для дій в умовах безлічі різних криз. НАТО регулярно тренує, навчає і випробовує свої сили і засоби врегулювання криз, які вона може застосувати у відповідь на низку криз, спричинених природними чи гуманітарними катастрофами або іншими деструктивними подіями, що виникають у військово-політичній сфері.

НАТО поважає роль суверенних держав і не розгортає війська, якщо не отримує на це політичних повноважень. Країни-члени НАТО і країни-партнери визначають в кожному конкретному випадку, чи підтримувати операції НАТО з врегулювання криз. НАТО також визнає, що лише військове рішення не вирішить кризу; скоріше, для ефективного врегулювання кризи потрібен комплексний набір політичних, цивільних і військових заходів реагування.

Проте сучасне міжнародне оперативне середовище розвивається і стає дедалі складнішим: конфлікти, некеровані держави, протести, пандемії, зміна клімату, екстремальні погодні явища, глобалізація, стихійні лиха і нові загрози є серед цих нових динамічних явищ. На цьому тлі НАТО стикається з більшими викликами, оскільки очевидна зміна балансу сил у світі загрожує міжнародному верховенству права. Тому НАТО може знайти можливості для посилення національної спроможності своїх членів і партнерів врегульовувати кризи на регіональному або національному рівні.

##### Розвиток кризового менеджменту та стійкості

Власники та оператори об'єктів критичної інфраструктури стикаються з дедалі складнішими структурами, системами та компонентами, які надають основні послуги системам критичної інфраструктури. Сектори критичної інфраструктури стають все більш залежними і взаємозалежними від ланцюгів постачання та інших секторів критичної інфраструктури. Детальний аналіз цих залежностей і взаємозалежностей див. у розділі 12. Зі зростанням складності структур, систем і компонентів не лише у відповідних секторах, а й у ланцюгах постачання, зростає вразливість, притаманна їм, а також можливість однієї загрози порушити роботу кількох секторів критично важливої інфраструктури одночасно. Цей тісний взаємозв'язок - ключовий елемент теорії звичайних аварій, який підкреслює вразливість і пов'язані з нею недоліки, що виникають внаслідок взаємопов'язаного і взаємозалежного технологічного прогресу -зростає в більшості секторів критичної інфраструктури. Як наслідок, попередні дослідження, що стосуються організацій високої надійності (ОВН), зараз переглядаються науковцями та операторами таких організацій. Теорія ОВН пояснює, що традиційне розуміння критичної інфраструктури не визнає складності ОВН, і виступає за інший підхід до безпеки та стійкості. Наступні п'ять принципів, як правило, є основними характеристиками ОПР:

* Заклопотаність невдачами. Переважно жорстко регульовані галузі, де розглядаються технічні, людські або технологічні збої, а також висока схильність до уникнення ризиків.
* Небажання спрощувати. Деякі галузі є складними за своєю природою, наприклад, авіація, транспорт, енергетика, водопостачання та телекомунікації.
* Чутливість до операцій. Чітко зосереджуючись на тому, що надає організація, цей погляд з переднього краю допомагає приймати рішення.
* Прихильність до стійкості. Здатність і спроможність передбачати настання інцидентів, надзвичайних ситуацій і криз, а також адаптуватися до них і долати їх.
* Повага до досвіду. Визнаючи важливість досвіду, а не авторитету, вони залучають фахівців та експертів для подолання невизначеності та обставин, що швидко змінюються, а також для оцінки ситуації на місцях.

В контексті посилення позиції, сил і засобів, а також політики у сфері СІСР ці п'ять принципів можуть виявитись дуже корисними для НАТО як організації, а також для її держав-членів і країн-партнерів. У цьому розділі також підкреслюється актуальність і корисність національного стандарту Великої Британії з врегулювання криз, який члени і партнери Альянсу можуть вважати чудовим підґрунтям для розвитку або оновлення сил і засобів врегулювання криз на місцевому, регіональному або національному рівнях. Крім того, в розділі рекомендується використовувати навчання для підготовки персоналу і перевірки планів і процедур як засіб покращення СІСР в уряді чи організації. Члени Альянсу і партнери можуть ознайомитись з цим міжнародним стандартом, опублікованим Міжнародною організацією зі стандартизації і використовується у Великій Британії та інших країнах - корисний для керівництва щодо планування, проведення та вивчення навчань.

У недержавних секторах, включаючи критичну інфраструктуру та інші регульовані сектори, також відбулися зрушення у вирішенні таких ключових питань, як принципи управління ризиками, антикризове управління, управління активами, управління інформацією, гарантії та безпека, безперервність бізнесу, управління репутацією, екологічний менеджмент, а також, дедалі частіше, інші форми регулювання. Як наслідок, з'явилася тенденція та інтерес до об'єднання деяких з цих дисциплін разом. Прагнення корпоративного сектору та урядів гармонізувати або синхронізувати такі розрізнені, але пов'язані та взаємозалежні види діяльності призвело до зростання інтересу до концепції організаційної стійкості. *Організаційна стійкість* визначається як здатність "передбачати, готуватися, реагувати і адаптуватися до поступових змін і раптових збоїв, щоб вижити і процвітати". По суті, організаційна стійкість дозволяє організації адаптуватися до умов, що змінюються, зберігаючи при цьому свої основні цінності, мету та бачення. Іноді така адаптація означає, що організація впроваджує варіанти реагування, які вона розробила до порушення. В інших випадках це вимагає від організації адаптації її структур або дій, щоб пристосуватися до нових умов.

З огляду на оголошення НАТО в червні 2021 року про посилення зобов'язань щодо стійкості, для Альянсу може з'явитися можливість інтегрувати свою доктрину врегулювання криз з іншими важливими функціями і посилити ці зобов'язання, визначивши організаційну стійкість як нове основне завдання. Крім того, НАТО також відіграє центральну роль у цивільно-військовому співробітництві (CIMIC), а в Польовому посібнику з CIMIC окреслено внесок оборони в забезпечення стійкості і допомоги цивільним органам влади. Разом такі напрями, як організаційна стійкість і CIMIC, пропонують потенційні наступні кроки НАТО з посилення своєї колективної сили і засобів реагування на СІСР.

### Резюме та Висновок

Таким чином, у цій главі ми розглянули унікальні аспекти управління кризою на відміну від звичайного управління інцидентами та надзвичайними ситуаціями, а також те, чому ці традиційні підходи не дають змоги ефективно вирішити кризу. Якщо в першій частині глави були представлені різні стадії і фази криз і відповідні заходи реагування, то в наступних розділах обговорювалися такі питання, як ключову роль НАТО в ефективному врегулюванні криз і можливості, які відкриває нещодавнє зобов'язання Альянсу щодо посилення стійкості. У розділі також визначено нові ініціативи з розвитку організаційної стійкості і переглянуто попередні організаційні теорії, що мають відношення до політики і практики СІСР. Ці концепції, зокрема організаційна стійкість, можуть допомогти НАТО в двох важливих аспектах. По-перше, вони можуть покращити підтримку, яку НАТО як організація надає своїм країнам-членам і країнам-партнерам під час виникнення або розгортання криз. По-друге, вони можуть допомогти зацікавленим сторонам критично важливої інфраструктури серед членів і партнерів Альянсу і партнерів посилити безпеку і стійкість, що сприятиме національній безпеці і стійкості і дасть змогу НАТО виконувати свої основні завдання. На завершення слід зазначити, що кризи не залишаються статичними, як і технології, які забезпечують надання важливих послуг критично важливою інфраструктурою. Тому структури, процеси і мислення, які лежать в основі СІСР і кризового менеджменту, повинні розвиватись для того, щоб протистояти загрозам підриву, з якими країни стикаються сьогодні.

З огляду на оголошення про зобов'язання щодо стійкості, яке було зроблене в червні 2021 року, і роботу над оновленою Стратегічною концепцією, що відповідає нинішньому міжнародному безпековому середовищу, для НАТО існують ключові можливості в галузі СІСР і врегулювання криз, які вона може реалізовувати. Зокрема, НАТО має переглянути розробку настанов з організаційної стійкості і існуючих стандартів врегулювання криз на підтримку своїх посилених зобов'язань щодо стійкості. Такий перегляд дозволить провести порівняльний аналіз чинної доктрини НАТО з метою визначення сфер, які потребують вдосконалення у виконанні основного завдання Альянсу - надання підтримки країнам-членам і країнам-партнерам у реагуванні на кризи і врегулюванні кризових ситуацій.

## Про дописувачів

Кріс Андерсон - експерт з управління інцидентами та захисту інфраструктури з тридцятирічним досвідом роботи в уряді, армії та приватному секторі. Наразі він є головним радником з питань національної безпеки та готовності до надзвичайних ситуацій в Lumen, американському глобальному мережевому провайдеру та технологічній компанії, що базується в США. Раніше він обіймав різні керівні посади у сфері управління надзвичайними ситуаціями та національної безпеки у Федеральній комісії зв'язку США та Міністерстві внутрішньої безпеки США. Андерсон розпочав свою кар'єру пілотом вертольота ВМС США, прослуживши 24 роки на дійсній службі та в резерві. Він отримав ступінь магістра зі стратегії національної безпеки в Національному військовому коледжі та з управлінських інформаційних систем в Університеті штату Боуї, а також ступінь бакалавра в Університеті Вірджинії.

Малкольм Бейкер має великий досвід у сфері національної безпеки, управління надзвичайними ситуаціями, управління інцидентами та кризами, а також захисту критичної національної інфраструктури. Наразі Бейкер є директором компанії Resilience Limited у Великій Британії. Він продовжує підтримувати програму COE-DAT з безпеки та стійкості критичної інфраструктури. Він багато працював з різними установами британського уряду, включаючи служби з надзвичайних ситуацій, армію та національну безпеку. Раніше Бейкер був старшим офіцером Контртерористичного командування та Антитерористичного відділу столичної поліції. Він отримав ступінь магістра наук в Оборонному коледжі управління та технологій при Академії оборони Великої Британії в Шрівенемі. Наразі Бейкер навчається на сертифікованого фахівця з управління безпекою та дипломованого фахівця з безпеки.

Рональд Бірс - експерт з питань захисту критичної інфраструктури та готовності національної безпеки, має понад 23 роки досвіду роботи в міністерствах оборони, внутрішньої безпеки та казначействі США. Він є ад'юнкт-професором Массачусетської морської академії і радником Центру передового досвіду НАТО з питань захисту від тероризму (COE-DAT), де він викладає на навчальній програмі COE-DAT із захисту критичної інфраструктури від терористичних атак. Бірс отримав ступінь бакалавра політології та радянології в Массачусетському університеті в Амхерсті та ступінь магістра державного управління в Університеті Джорджа Вашингтона. Він є почесним випускником Університету національної оборони США і колишнім старшим науковим співробітникому Центрі захисту інфраструктури та національної безпеки Університету Джорджа Мейсона.

Саліх Бічакчі - доцент кафедри міжнародних відносин Університету Кадір Хас у Стамбулі, Туреччина, та науковий співробітник Центру кібербезпеки та захисту критичної інфраструктури при університеті. Його дослідження зосереджені на кібербезпеці, захисті критичної інфраструктури, гібридній безпеці, конфіденційності даних та тероризмі. Бічакчі є радником Центру передового досвіду НАТО з питань захисту від тероризму (COE-DAT) і часто читає лекції в COE-DAT і Центрах передового досвіду НАТО з питань командування і управління та морської безпеки. Він також викладає курси з кібербезпеки та безпеки на Близькому Сході в Академії Збройних сил Турецького військового коледжу. Бічакчі готував звіти з кібербезпеки для атомних електростанцій і керував симуляційними навчаннями та тренінгами для вищого керівництва кількох організацій.

Стів Бібер має більш ніж 30-річний досвід керівництва розвитком та реформами у сфері водної безпеки, державної політики та екологічного регулювання. Наразі він є директором програм з водних ресурсів Ради урядів столичного округу Вашингтон (MWCOG) і відповідає за управління програмами з водних ресурсів, включаючи регіональне Партнерство з відновлення Анакостії, програми з водної безпеки, планування питної води та стічних вод, управління посухами, відновлення міських струмків та інші пов'язані з ними екологічні програми для органів місцевого самоврядування та водоканалів у Вашингтоні. Бібер отримав ступінь бакалавра зоології в Університеті штату Мічиган, ступінь магістра океанографії в Університеті Старого Домініону та ступінь магістра державного управління в Університеті Балтимора.

Сонгбек Чо зараз працює дослідником у відділі стратегії в Центрі передового досвіду НАТО з питань кіберзахисту (CCD-COE) в Таллінні, Естонія. CCD-COE НАТО - це багатонаціональний міждисциплінарний центр кіберзахисту, який надає НАТО і країнам-членам унікальну міждисциплінарну експертизу в галузі досліджень, тренувань і навчань з кіберзахисту, що охоплює такі основні сфери, як технології, стратегія, операції і право. Наукові інтереси Чо включають управління ризиками кібербезпеки, захист критичної інфраструктури, національну стратегію кібербезпеки, обмін інформацією, сертифікацію та акредитацію у сфері безпеки.

Адріан Дуайєр - експерт з майже 40-річним досвідом роботи у сфері боротьби з тероризмом. Адріан служив у Королівських інженерних військах Британської армії як офіцер-сапер та інструктор контртерористичного крила у Королівській школі військової інженерії. Згодом він був призначений головним радником з антитерористичних ризиків британської транспортної поліції - посаду, яку він обіймав понад 20 років. Двайер також працював консультантом з управління ризиками в різних галузях промисловості, від перестрахування ризиків до нафтохімії. Він є членом Інституту королівських інженерів та Інституту інженерів-вибухотехніків. Має ступінь магістра наук з управління ризиками, кризами та катастрофами, а також ступінь доктора філософії Університету Глазго.

Керол В. Еванс є директором Інституту стратегічних досліджень та прес-служби Військового коледжу армії США у Карлайлі, штат Пенсильванія. Інститут стратегічних досліджень є провідним аналітичним центром армії США з питань геостратегічних досліджень та аналізу національної безпеки. Вона має 30-річний досвід у сферах забезпечення місій, управління кризами та їх наслідками, асиметричної війни, тероризму, морської безпеки та внутрішньої безпеки. З 2014 року Еванс є викладачем Центру передового досвіду НАТО з питань захисту від тероризму (COE-DAT) в Анкарі, Туреччина, де вона викладає на навчальній програмі COE-DAT "Захист критичної інфраструктури від терористичних атак". Вона має ступінь магістра та доктора філософії Лондонської школи економіки.

Джеффрі Френч працює у сфері захисту критичної інфраструктури з 1990-х років. Наразі він очолює групу з аналізу та управління ризиками в робочій групі по боротьбі з COVID Агентства кібербезпеки та безпеки інфраструктури США. Раніше Френч був директором з аналізу ризиків безпеки в компанії CENTRA Technology, Inc., де він підтримував численні програми та розробив кілька методологій оцінки ризиків для Міністерства внутрішньої безпеки США, включаючи інструменти для оцінки терористичних ризиків для інфраструктури, ризиків для безпеки під час спеціальних заходів та ризиків усіх видів небезпек для регіону. З 2015 року Френч також є лектором програми НАТО COE-DAT. Френч отримав ступінь бакалавра історії в Університеті штату Вічіта і ступінь магістра мистецтв у галузі досліджень національної безпеки в Джорджтаунському університеті.

Девід Харелл має понад 40 років досвіду у сфері антитерористичної діяльності, захисної безпеки та управління ризиками у державному та приватному секторах. Він надає консультації та проводить тренінги для урядів і великих корпорацій з широкого кола актуальних аспектів безпеки, включаючи готовність, захист критичної інфраструктури, управління ризиками та реагування на кризові ситуації. Під час своєї кар'єри у сфері державної безпеки він працював регіональним менеджером з безпеки авіакомпанії El Al у Скандинавії та був командиром курсу Ізраїльського агентства безпеки (ISA) для менеджерів з авіаційної безпеки. Після виходу на пенсію після 24 років служби в АНБ, Харелл став співзасновником і виконавчим директором

провідної та відомої міжнародної консалтингової компанії з питань безпеки. Наразі він викладає на магістерській програмі з управління безпекою в Берлінській школі економіки та права.

Алессандро Лазарі працює фахівцем із захисту критичної інфраструктури, стійкості та кібербезпеки з 2004 року. Наразі він є старшим менеджером по роботі з ключовими клієнтами в компанії 24 AG, що спеціалізується на управлінні інцидентами та кризовими ситуаціями в Європі. У 2010-19 роках він надавав політичну підтримку двом ключовим ініціативам Європейської комісії: Європейській програмі захисту критичної інфраструктури та зміцненню кіберстійкості Європи. Лазарі є науковим співробітником з правової інформатики в Школі права Університету Лечче (Італія) та викладачем курсу COE-DAT "Захист критичної інфраструктури від терористичних атак". Він є автором книги "*Європейський захист критичної інфраструктури"*, опублікованої у 2014 році видавництвом Springer Inc. Має ступінь магістра права та доктора філософії в галузі комп'ютерної інженерії, мультимедіа та телекомунікацій.

Реймонд Мей має понад 35 років досвіду роботи у сфері безпеки, в тому числі 23 роки у федеральних правоохоронних органах та антитерористичній діяльності. Він працював на різних керівних посадах у Федеральному бюро розслідувань США (ФБР), включаючи забезпечення безпеки великих політичних і спортивних заходів, управління кризовими ситуаціями та звільнення заручників. Мей проводив оцінку вразливості безпеки для багатьох компаній зі списку Fortune 500 та урядових організацій, а також розробляв стратегічні плани безпеки та навчальні програми для покращення та посилення безпеки та захисту. Здобув ступінь магістра психології в Коледжі Род-Айленда та ступінь бакалавра соціології/психології в Університеті Род-Айленда. Випускник Академії ФБР, Мей був нагороджений медаллю ФБР "За заслуги" та "Щитом хоробрості" ФБР.

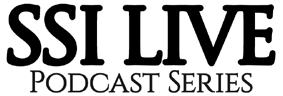
Тереза Сабоніс-Хелф очолює магістерську програму з науки, технологій та міжнародних відносин у Школі дипломатичної служби Джорджтаунського університету. Раніше вона була професором стратегії національної безпеки в Національному військовому коледжі. Вона жила і працювала в семи країнах колишнього СРСР, допомагала двом країнам у розробці їхніх перших стратегій національної безпеки, а також була співредактором двох томів про політичні та економічні перетворення в Центральній Азії. Сабоніс-Хелф багато публікує та читає лекцій з питань енергетичної безпеки, політики у сфері зміни клімату, пострадянської енергетики та екології, регіональної водної політики, регіональної торгівлі та транзиту, а також політики у сфері електроенергетики. Вона часто консультує Державний департамент США та Агентство США з міжнародного розвитку, а також є членом Ради з міжнародних відносин.

Дуейн Вернер - керівник групи з оцінки стійкості у Відділі наук про прийняття рішень та інфраструктуру Аргонської національної лабораторії. З 2009 року він надає підтримку в розробці методології та реалізації проектів для Міністерства внутрішньої безпеки США. Вернер є активним членом Європейського центру передового досвіду з протидії гібридним загрозам та делегатом Форуму високого рівня ризиків Організації економічного співробітництва та розвитку. У 2018 році він був призначений цивільним експертом Комітету НАТО з цивільного планування на випадок надзвичайних ситуацій для консультування з усіх аспектів регіональної енергетичної стійкості. Раніше Вернер був менеджером проектів у приватній інжиніринговій компанії в Нью-Йорку, працював у сфері транспорту, внутрішньої безпеки та оборони. Він є сертифікованим планувальником зі ступенем магістра мистецтв у галузі міського планування.

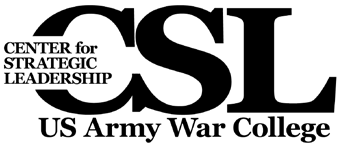
Військовий коледж Сухопутних військ США навчає і розвиває лідерів для служби на стратегічному рівні, одночасно просуваючи знання про глобальне застосування сухопутних сил.

Метою Військового коледжу Сухопутних військ ЗС США є підготовка випускників, які вміють критично мислити і вирішувати складні проблеми у сфері глобального застосування сухопутних сил. Водночас, наш обов'язок перед армією - діяти як "фабрика думок" для командирів і цивільних лідерів на стратегічному рівні в усьому світі і регулярно брати участь у дискусіях і дебатах про роль сухопутних військ у досягненні цілей національної безпеки.

Інститут стратегічних досліджень публікує дослідження та аналітику з питань національної безпеки та стратегії, щоб впливати на політичні дебати та подолати розрив між військовими та академічними колами.

Серія подкастів SSI в прямому ефірі надає доступ до аналітичних матеріалів SSI та науковців з питань, пов'язаних з національною безпекою та військовою стратегією, з акцентом на геостратегічний аналіз. https://ssi.armywarcollege.edu

/ssi-live-archive

Центр стратегічного лідерства надає стратегічну освіту, ідеї, доктрину та можливості для армії, Об'єднаних сил та країни в цілому. Армія, Об'єднані сили та національні партнери визнають Центр стратегічного лідерства стратегічною лабораторією, яка генерує і розвиває стратегічну думку, тестує стратегічні теорії, підтримує стратегічну доктрину, навчає стратегічних лідерів і підтримує прийняття стратегічних рішень.

Школа стратегічних сухопутних сил надає підтримку меті, місії, баченню Військового коледжу Сухопутних військ США та академічним кафедрам шляхом ініціювання, координації та управління політикою, планами, програмами та процедурами, пов'язаними з навчанням, з акцентом на розробці, виконанні та оцінці навчальних планів; плануванні та виконанні незалежних та/або міжкафедральних навчальних програм; розвитку студентів та викладачів; а також виконанні академічних функцій, які можуть бути визначені комендантом.

Центр спадщини та освіти армії США надає сучасні та історичні матеріали, пов'язані зі стратегічним лідерством, глобальним застосуванням сухопутної сили та спадщиною армії США, для інформаційного забезпечення досліджень, навчання міжнародної аудиторії та вшанування солдатів, як минулих, так і теперішніх.

Програма стратегічної освіти Сухопутних військ здійснює професійну військову освіту для всіх генеральських офіцерів Сухопутних військ по всій армії і проводить оцінку для інформування вищого керівництва і підтримки програмних змін шляхом прийняття рішень на основі фактичних даних.

