СПІЛЬНА ГРУПА ЄС-НАТО ЗІ СТІКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ЗВІТ З ПІДСУМКОВОГО ОЦІНЮВАННЯ

ЧЕРВЕНЬ 2023

СПІЛЬНА ГРУПА ЄС-НАТО ЗІ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
ЗВІТ З ПІДСУМКОВОГО ОЦІНЮВАННЯ

Вступ

З огляду на зростаючу наполегливість стратегічних конкурентів і зростаючу складність загроз безпеці, забезпечення стійкості інфраструктури, яка має вирішальне значення для держав-членів ЄС і союзників по НАТО, є важливим елементом стратегічного партнерства та співпраці між двома організаціями. На цій основі 11 січня 2023 року президент Європейської комісії та генеральний секретар НАТО оголосили про створення спеціальної робочої групи НАТО-ЄС із стійкості критичної інфраструктури.

Цільова група ЄС-НАТО повністю інтегрована в існуючий структурований діалог НАТО-ЄС щодо стійкості та додатково його посилює. Цей звіт, підготовлений співробітниками ЄС і НАТО, доповнює 8-й щорічний звіт про хід реалізації спільного набору пропозицій, поданих спільно Генеральним секретарем НАТО та Верховним представником/віце-президентом двом Радам у червні. У ньому описується важливість критичної інфраструктури, оцінюється поточний контекст безпеки, який характеризується підвищеним рівнем ризику, і розглядаються чотири ключові сектори (енергетика, транспорт, цифрова інфраструктура та космос), а також міжсекторальні міркування. У звіті представлені конкретні рекомендації щодо дій, які можуть сприяти зміцненню стійкості критичної інфраструктури на підтримку держав-членів ЄС і союзників по НАТО.

НАТО та ЄС продовжуватимуть працювати над тим, щоб зробити критичну інфраструктуру, технології та ланцюги поставок більш стійкими до загроз і ризиків, що постійно змінюються, на основі паралельних і скоординованих оцінок, а також вживатимуть заходів для пом'якшення потенційної вразливості.

Співробітники ЄС і НАТО виконуватимуть рекомендації цього звіту на основі багаторічної співпраці та з повною відповідальністю до узгоджених керівних принципів, закріплених у трьох Спільних деклараціях щодо співпраці між ЄС і НАТО. Структурований діалог НАТО-ЄС щодо стійкості забезпечить узгодженість подальшої роботи Цільової групи, беручи до уваги політичні вказівки відповідних Рад щодо подальшого розвитку цієї роботи.

ВАЖЛИВІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Наші економіки та наші демократичні суспільства покладаються на критично важливу інфраструктуру, яка надає необхідні послуги нашим громадянам і підтримує нашу економіку. Збройні сили також значною мірою покладаються на державну та приватну цивільну інфраструктуру, щоб мати можливість виконувати свої обов'язки.

Стійкість критично важливої інфраструктури держав-членів і членів Альянсу є насамперед національною відповідальністю. Стійкість охоплює здатність запобігати, захищати, реагувати, протистояти, пом'якшувати, поглинати, пристосовуватись і відновлюватися після інцидентів, які можуть порушити надання основних послуг. Це особливо важливо для критичної інфраструктури, оскільки повний захист, як правило, неможливий. Інфраструктура часто перетинає кордони або надає послуги, які перетинають кордони. Тому співпраця на регіональному та міжнародному рівнях, у тому числі через міжнародні організації, є необхідною.

Для НАТО основна увага приділяється критичній інфраструктурі, яка дозволяє виконувати основні завдання організації щодо стримування та оборони; запобігання кризовим ситуаціям та управління ними; та кооперативна безпека. Забезпечення національної та колективної стійкості має вирішальне значення для всіх основних завдань НАТО та лежить в основі зусиль НАТО щодо захисту членів Альянсу, їхніх суспільств і спільних цінностей.

Для ЄС критична інфраструктура не лише тісно пов'язана з політикою та законодавством, що забезпечує функціонування внутрішнього ринку ЄС, але й із його програмою безпеки та оборони, включаючи стратегічний пріоритет захисту Союзу та його громадян, а також Свобода дій ЄС. Критична інфраструктура необхідна для надання основних державних послуг та економічної діяльності на внутрішньому ринку, а також для безпеки та оборони.

Збої в критичній інфраструктурі можуть мати значні негативні наслідки для життєво важливих функцій уряду, основних послуг для населення та економічної діяльності в членах Альянсу та державах-членах. Вони також можуть перешкоджати військовій діяльності, включаючи навчання, розгортання, посилення та підтримку. Крім того, складні взаємозалежності означають, що збій у критичній інфраструктурі може мати каскадні або взаємопідсилювальні наслідки. Наприклад, перебої з електропостачанням можуть вплинути на комунальні послуги та постачання життєво необхідних товарів. Такі наслідки можуть також перетинати кордони через взаємозв'язки мереж і той факт, що в деяких випадках сама інфраструктура охоплює більше ніж одну країну.

Критична інфраструктура у багатьох випадках перебуває у приватній власності, управляється або експлуатується. Оскільки вона забезпечує критично важливі державні послуги та основні послуги для населення та суб'єктів господарювання, а також у деяких випадках служить цілям безпеки та оборони, уряди повинні забезпечити її стійкість до збоїв. Це включає розгляд інвестицій, які можуть знадобитися.

Держави-члени та члени Альянсу працюють над посиленням стійкості своєї критичної інфраструктури. Це, наприклад, підвищення обізнаності шляхом моніторингу та обміну інформацією; запобігання збоїв за допомогою заходів безпеки та заходів готовності; мінімізація наслідків потенційного збою за допомогою швидкого та ефективного реагування, резервування або резервних заходів, включаючи можливості відновлення/ремонту; а також забезпечення своєчасного відновлення після збою за допомогою планування на випадок надзвичайних ситуацій і готовності.

СИСТЕМА БЕЗПЕКИ

Як внесок у роботу Цільової групи НАТО-ЄС, гібридний термоядерний осередок ЄС та відділ гібридного аналізу підрозділу виробництва розвідувальних даних Об'єднаного відділу розвідки та безпеки НАТО провели паралельну та скоординовану оцінку (PACA) ландшафту загроз, пов'язаних із критичною інфраструктурою відповідно до усталеної практики співпраці між НАТО та ЄС. Паралельно вона була надана державам-членам ЄС і союзникам НАТО.

Збої в критичній інфраструктурі можуть виникати з багатьох джерел, як природних, так і антропогенних. Більше того, через те, що економіка та суспільство все більше переплітаються та взаємопов'язані, збої в роботі критичної інфраструктури можуть мати значні наслідки для різних секторів та кордонів.

Критична інфраструктура вразлива до навмисних атак або аварій. Багато типів критичної інфраструктури широко розкидані, а деякі легкодоступні. Враховуючи ступінь приватної власності та необхідність забезпечення, серед іншого, фінансової життєздатності, жорсткі заходи безпеки можуть бути неможливими. Таким чином, супротивник може розглядати критичну інфраструктуру як «м'яку мішень», особливо щодо гібридної тактики, яка дозволяє здійснювати такі атаки під маскою правдоподібного заперечення. Навмисні атаки також можна розрахувати так, щоб максимізувати руйнівний вплив.

Агресійна війна росії проти України показала, що критичну інфраструктуру можна атакувати різними способами: шляхом шпигунства та збору розвідданих, фізичної атаки, ворожої розвідки, зловмисної гібридної та кіберактивності, використання залежностей або захоплення. У той же час приклад України довів, що можна протистояти навіть широкомасштабним атакам, і підкреслив, наскільки важливими є стійка критична інфраструктура та постійне надання основних послуг для здатності та рішучості країни захищати себе.

Своїми діями в Україні росія вже продемонструвала, що розглядає критичну інфраструктуру як мішень. Вона також наносить на карту критичну інфраструктуру в євроатлантичному регіоні, на яку може націлитися. росія та пов'язані з нею групи використовували кібератаки як засіб для переривання основних послуг у євроатлантичному регіоні.

Терористичні організації також становлять загрозу для критичної інфраструктури. Різні терористичні групи кілька разів атакували транспортну інфраструктуру членів Альянсу та держав-членів.

Стихійні лиха або екстремальні погодні умови можуть завдати фізичної шкоди інфраструктурі, тим самим порушуючи процес надання послуг. Ця проблема посилюється зі зміною клімату, яка піддасть інфраструктуру впливу підвищення рівня моря, зміни погодних умов і більш частих екстремальних погодних явищ.

У контексті зростаючої стратегічної конкуренції важливо визначити та пом'якшити стратегічні вразливості та залежності, якими можна скористатися. Іноземний контроль над ключовими технологічними та промисловими секторами, критичною інфраструктурою та стратегічними матеріалами та ланцюгами поставок може дозволити іноземним суб'єктам збирати конфіденційну інформацію про діяльність НАТО та ЄС, а також потенційно забороняти та порушувати доступ до критичної інфраструктури або перешкоджати послугам, які вона надає.

Морське дно є сферою зростаючого стратегічного значення через зростаючу залежність від підводної інфраструктури та особливих проблем із її захистом від гібридних загроз і фізичної шкоди.

ГАЛУЗЕВИЙ АНАЛІЗ

Кожен сектор (галузь) основних послуг спирається на певну критичну інфраструктуру. Тим не менш, було визначено чотири міжсектори, які надають послуги, що підтримують інші сектори: енергетика, транспорт, цифрова інфраструктура та космос. Ці сектори стикаються з особливими проблемами, які необхідно вирішити, щоб підвищити стійкість.

ЕНЕРГЕТИКА

Наші економіки та наші суспільства залежать від надійного постачання енергії з різноманітних джерел. Розгалужені енергетичні торговельні зв'язки між державами-членами та членами Альянсу підкреслюють важливість міжнародного співробітництва у сфері енергетики.

Енергетична безпека стала ще складнішою в поточному геополітичному середовищі, оскільки ворожі гравці та стратегічні конкуренти здійснюють зловмисну діяльність у кіберпросторі, маніпулюють поставками енергії та застосовують економічний примус. Військова діяльність значною мірою залежить від цивільних енергетичних мереж і поставок, що ще більше підкреслює необхідність забезпечення безпеки критичної енергетичної інфраструктури та ланцюгів постачання.

Диверсія на газопроводі Nord Stream ілюструє вразливість енергетичної інфраструктури. Ризик дефіциту внаслідок агресивної війни росії проти України також підвищив усвідомлення потенційної шкоди повсякденному життю. Енергетична інфраструктура простягається на великі відстані (наприклад, трубопроводи, електричні кабелі), що ускладнює постійний моніторинг або захист; одноразової атаки може бути достатньо, щоб завдати значної шкоди, як у випадку з дамбою гідроелектростанції, як показала недавня атака в Україні. Енергетична інфраструктура також об'єднана в мережу, тому збій в одному місці може вплинути за межі цієї локальної області, а інформація про її розташування та маршрут зазвичай є загальнодоступною. Як засвідчили попередні інциденти, значні інвестиції в цифровізацію енергетичної інфраструктури роблять її потенційно вразливою до цілеспрямованих кібератак, а також до загальних збоїв у роботі цифрової інфраструктури та послуг.

Ці виклики ускладнюються підводною енергетичною інфраструктурою, яка є розгалуженою та складнішою для огляду та захисту. Крім того, очікується, що мережа підводної енергетичної інфраструктури в євроатлантичному регіоні зростатиме, оскільки морські енергетичні платформи стануть дедалі більшими.

Енергетична інфраструктура трансформується, оскільки члени Альянсу та держави-члени вживають заходів, щоб зменшити свою залежність від російських енергоресурсів і зменшити викиди у відповідь на зміну клімату.

Наприклад, рішучі кроки, вжиті державами-членами та союзниками щодо диверсифікації від російської енергетики, призвели до збільшення використання зрідженого природного газу (ЗПГ) і розгортання плавучих терміналів ЗПГ. Ці термінали складаються з плавучих і наземних компонентів, а також з'єднань між ними.

Інфраструктура також трансформується в міру зростання використання відновлюваних джерел енергії та електрифікації. Це може посилити стійкість, оскільки збільшує різноманітність джерел і автономію, тоді як наявність численних децентралізованих учасників зменшує залежність від єдиної центральної системи. З іншого боку, більша кількість віддалених і розосереджених джерел енергії та зберігання енергії, а також нових з'єднань, які вони потребують, створюють нові виклики щодо захисту інфраструктури.

Збільшення залежності від відновлюваних джерел енергії також створює потенційну вразливість ланцюга постачання, оскільки виробництво сонячних панелей, вітряних турбін, акумуляторів і багатьох їхніх критичних компонентів все ще здебільшого зосереджено за межами НАТО та ЄС. Розвиток більшої кількості морської інфраструктури відновлюваної енергетики також ускладнює моніторинг, але в той же час дає можливість створити стійкість за допомогою проєкта.

Крім того, енергетичний сектор має особливі характеристики, які вимагають спеціальних заходів для забезпечення стійкості, а саме:

i. Вимоги до реального часу: деякі енергетичні системи повинні реагувати дуже швидко, у деяких випадках до мілісекунд, і не передбачають додаткового часу обробки.
ii. Каскадні ефекти: раптовий збій в електромережі може викликати швидкий ефект доміно збоїв, що може швидко призвести до порушення постачання великої кількості споживачів у різних країнах і секторах.
iii. Поєднання технологій: застарілі технології та інфраструктура, термін служби яких становить 30-60 років, потребуватимуть підтримки одночасно з впровадженням нових технологій і цифровізації.

ТРАНСПОРТ

Транспортна інфраструктура життєво важлива для нашого населення, нашої економіки та наших збройних сил. Крім того, вона обширна і включає дороги, залізниці, внутрішні водні шляхи, аеропорти, морські та внутрішні порти. Вона може бути державною, приватною або результатом державно-приватного партнерства.

Дуже важливо підтримувати функціональну транспортну інфраструктуру, включаючи інфраструктуру, визначену в транс'європейській транспортній мережі, яка представляє основні транспортні артерії по всій Європі та в сусідніх третіх країнах. Однак, враховуючи розгалужену мережу транспортної інфраструктури на територіях держав-членів і членів Альянсу, існує велика кількість резервів і доступно багато альтернативних варіантів маршрутів, включаючи рішення для інтермодального транспорту. Тим не менш, деякі ключові вузли критичні, в тому числі для військових цілей, і їх нелегко замінити. Це стало очевидним в останні роки, коли природні небезпеки призвели до збоїв, які тимчасово зменшили доступ до частин європейської транспортної мережі. Ці ключові вузли включають великі аеропорти, морські порти, головні залізничні вузли та певні внутрішні водні шляхи, а також мережу інфраструктури, яка дозволяє перевозити великі обсяги негабаритних військових вантажів і небезпечних вантажів, включаючи боєприпаси. Ця інфраструктура також є важливою з точки зору оборони. Її необхідно буде додатково зміцнити й модернізувати, щоб відповідати вимогам військової діяльності, навчань і потенційних місій і операцій, у тому числі в умовах боротьби.

Інфраструктура громадського транспорту стала об'єктом терористичних атак у членах Альянсу та державах-членах. Заходи безпеки були посилені, але потреба в тому, щоб транспортна інфраструктура залишалася доступною для громадськості, обмежує ступінь її захисту.

Транспортна інфраструктура, включаючи аеропорти та морські порти, також вразлива до кібератак, які можуть завдати значних економічних збитків і потенційно порушити або заборонити її використання збройними силами. Наші військові значною мірою покладаються на цивільні та комерційні транспортні засоби та інфраструктуру для розгортання та підтримки своєї діяльності. Морські порти, аеропорти та міцний внутрішній інтермодальний зв'язок є ключовими передумовами для швидкого розгортання та підтримки військових сил у Європі, через Європу та з неї. Хоча збій у будь-якому вузлі може мати значні наслідки для військових операцій, збої у великих морських портах, ймовірно, матимуть більші наслідки, оскільки існує менше варіантів для пом'якшення зриву руху масових вантажів як для цивільних, так і для військових цілей. Подібним чином будь-який значний збій у роботі ключового аеропорту може вплинути на стратегічне та оперативне розгортання військових сил, залежно від характеру та місця кризи. Доступ до інфраструктури може змінюватися, тому необхідний безпечний обмін інформацією між власниками/операторами інфраструктури та користувачами, щоб бути в курсі таких питань, як планове технічне обслуговування чи інші дії, які можуть знизити доступність інфраструктури.

Транспортний сектор зазнає впливу та має значний вплив на кожен з інших секторів, розглянутих у цьому документі, і ці взаємозалежності зростають. Посилення електрифікації транспорту призведе до більшої залежності від електричної мережі, акумуляторів та пов'язаної з ними інфраструктури, на додаток до існуючої залежності від трубопроводів для вуглеводневих продуктів, які залишаться частиною енергетичної суміші в осяжному майбутньому. Більше того, транспортна інфраструктура

все більше цифровізується, що робить її залежною від цифрової інфраструктури та водночас більш вразливою до зловмисних кібердій та збоїв. Нарешті, транспортна інфраструктура спирається на космічні системи, зокрема для позиціонування, навігації та часу. Наприклад, навіть для портового обладнання потрібні дані, надані Глобальною навігаційною супутниковою системою, щоб розвантажувати контейнери з кораблів.

ЦИФРОВА ІНФРАСТРУКТУРА

Цифрова інфраструктура забезпечує основу для комунікацій, які підтримують усі основні функції суспільства та економіки. Наші громадяни все більше покладаються на цифрову інфраструктуру у своєму повсякденному житті, і це є ключовою можливістю, яка дозволяє урядам спілкуватися зі своїми громадянами, особливо під час кризи.

Для надання інформаційно-комунікаційних послуг потрібен широкий спектр інфраструктури, від підземних і підводних волоконно-оптичних кабелів до базових станцій стільникового зв'язку та супутників. Резервування значною мірою вбудовано в комунікаційні мережі, хоча залишається важливим планування на випадок непередбачених ситуацій (наприклад, шляхом визначення основних, альтернативних, непередбачених і надзвичайних вимог). Крім того, існують певні вузли, критично важливі для маршрутизації трафіку або керування мережею, включаючи центри обробки даних і точки обміну Інтернетом, а також певні типи інфраструктури, які нелегко замінити, зокрема підводні кабелі.

Підводні кабелі зв'язку є важливою частиною глобальної комунікаційної мережі, через яку передається 95% світового інтернет-трафіку. Враховуючи їхню довжину та складність спостереження за ними, вони можуть розглядатися як приваблива ціль для ворога. Одночасний розрив кількох підводних кабелів зв'язку становив би значний ризик для держав-членів і членів Альянсу, оскільки можливості ремонту в усьому світі обмежені, а з огляду на віддалене розташування багатьох кабелів ремонт потребує часу.

Мережі 5G дедалі більше забезпечують магістраль для широкого спектру послуг, необхідних для суспільних послуг і економічних функцій, таких як енергетика, транспорт, банківська справа та охорона здоров'я, а також промислові системи управління. Залежність багатьох критично важливих послуг від мереж 5G і від мереж наступного покоління в майбутньому зробить наслідки системного та широкомасштабного збою особливо серйозними. Мережі 5G представляють більшу поверхню вразливості, що дає зловмисникам більше точок входу, і тому вони вимагають посилених заходів безпеки та стійкості. Крім того, головна роль постачальників мережевого обладнання та послуг вимагає оцінки та усунення стратегічних ризиків, особливо ризику втручання з боку конкретних третіх країн, які мають закони про безпеку та корпоративне управління, що створює потенційні ризики для безпеки Альянсу та держав-членів.

Уряди та збройні сили значною мірою покладаються на цифрову інфраструктуру, якою володіють і керують компанії приватного сектору. Тому зростає розуміння важливості забезпечення безпеки та стійкості цієї інфраструктури, а також отримання кращих знань про те, де зберігаються та обробляються дані.

Частина цифрової інфраструктури, що використовується урядами та збройними силами, також належить їм і ними керується. Хоча це повна національна компетенція, надзвичайно важливо підвищити її стійкість, зокрема військову та правоохоронну цифрову інфраструктуру. Існуюче законодавство та політика, що застосовуються до державного сектору, можуть мати значення для військової сфери, і навпаки.

Крім того, цифрова інфраструктура спирається на ланцюги поставок, які охоплюють весь світ. Це робить їх вразливими до випадкових збоїв через погодні умови чи людську помилку, а також до навмисних збоїв заради політичної, військової, фінансової чи кримінальної вигоди. Критичні компоненти, отримані з-за меж ЄС або НАТО, також можуть не відповідати тим самим стандартам щодо безпеки чи захисту даних і можуть створити вразливі місця в мережах Альянсу або держав-членів.

КОСМОС

Космічна інфраструктура включає як космічні засоби, так і наземні системи, включаючи передачу даних та інші радіочастотні канали, які можуть бути вразливими до різних видів антропогенних і природних ризиків.

Космічні засоби можуть належати та управлятися ЄС (Galileo, Copernicus, IRIS), державами-членами, союзниками та, все частіше, комерційними структурами.

Стратегічні конкуренти та потенційні супротивники інвестують у, розробляють, випробовують та вводять в дію складні протикосмічні засоби та доктрини, які можуть загрожувати доступу НАТО та ЄС до космічної сфери та свободі діяти в космічній сфері, погіршити нашу оборону та зашкодити нашій безпеці. Націлюючись на цивільну та військову інфраструктуру, вони можуть порушити, погіршити, ввести в оману, відмовити або знищити космічні можливості та послуги, від яких залежить інша критична інфраструктура держав-членів та союзників. Крім того, космічна інфраструктура стикається з унікальними ризиками космічного сміття, яке може завдати побічної шкоди та знизити доступність і зручність використання орбіт. Космічна погода також може впливати як на елементи на орбіті, так і на наземний зв'язок і електричні мережі.

Багато важливих послуг, включаючи енергетичну, транспортну, фінансову та цифрову інфраструктуру, покладаються на космічні дані, продукти та послуги, які забезпечують зв'язок, полегшують точне визначення часу, забезпечують точне позиціонування, підтримують моніторинг і прогнозування, а також забезпечують спостереження Землі. Ймовірно, це збільшиться з огляду на динамічний розвиток космічного сектора та збільшення доступності космосу, в тому числі через суб'єктів приватного сектора. Перебої в доступі до цих даних, продуктів і послуг можуть мати наслідки для стійкості Альянсу та держав-членів, перешкоджаючи наданню послуг, знижуючи ефективність і збільшуючи витрати.

Стійкість до збоїв можна посилити за допомогою резервування. У цьому контексті космічні дані, продукти та послуги, що надаються державами-членами та членами Альянсу, а також космічний потенціал ЄС є взаємодоповнюючими.

МІЖСЕКТОРАЛЬНІ (МІЖГАЛУЗЕВІ) ВИКЛИКИ

Специфічні для сектору елементи, розглянуті вище, вказують на міцні фізичні та цифрові взаємозв'язки, які існують між секторами, включаючи інші поза межами поточного аналізу (наприклад, охорона здоров'я, водопостачання чи сільське господарство, щоб назвати декілька). Завдяки цьому високому ступеню взаємозалежності між різними типами інфраструктури наслідки збоїв в одному секторі можуть каскадуватись, впливаючи також на критичну інфраструктуру в інших секторах. Ці зв'язки необхідно краще зрозуміти, щоб передбачити потенційні каскадні наслідки, визначити заходи для їх пом'якшення та сприяти ефективній і доповнюючій відповіді за допомогою цивільних і військових засобів, у тому числі тих, які доступні через Механізм цивільного захисту Союзу (UCPM).

Швидко зростаюча цифровізація кожного з чотирьох секторів, оцінених вище, робить їх уразливими до зловмисної кібер-діяльності. Кіберпростір завжди є предметом боротьби. Зловмисники виявляють все більшу готовність здійснювати зловмисну кіберактивність проти критичної інфраструктури для досягнення своїх стратегічних цілей, зокрема шляхом проведення масштабної розвідки; здійснення атак, у тому числі на ланцюги поставок; використання вразливостей апаратного та програмного забезпечення; використання переваг поганої кібергігієни та безпеки як у державних, так і в приватних організаціях.

Володіння або контроль з боку потенційних супротивників над критичною інфраструктурою та допоміжними ланцюжками поставок в членах Альянсу та державах-членах також становить потенційну проблему. Це може надати доступ до даних та інформації або може бути використано для погіршення, переривання чи заборони доступу чи припинення послуг. Наприклад, право власності або контроль над транспортною інфраструктурою може бути використано для отримання інформації

про військову техніку чи операції або для перешкоджання чи затримки розгортання.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

ЄС і НАТО мають спільний інтерес у запобіганні збоїв у роботі критично важливої інфраструктури, яка надає громадянам необхідні послуги та підтримує нашу економіку. Завдяки роботі Цільової групи НАТО-ЄС щодо стійкості критичної інфраструктури персонал підтвердив, що вони мають спільну точку зору щодо потенційних загроз і ризиків. Обидві організації продовжуватимуть взаємодоповнювати та взаємопідсилювати співпрацю, щоб створити стійкість і бути готовими до подолання збоїв із будь-якого джерела.

Держави-члени ЄС та союзники по НАТО продовжують підвищувати свою готовність протистояти збоям у критичній інфраструктурі. І НАТО, і ЄС підтримують своїх членів керівництвом, сприяють обміну передовим досвідом, проводять навчання, надають ресурси та пропонують додаткові інструменти для підвищення стійкості. Країни-члени ЄС і союзники по НАТО заохочуються використовувати їх у повній мірі.

Штаби НАТО та ЄС визначили наступні рекомендації щодо розвитку співпраці:

1. Забезпечення швидкої взаємодії між високопосадовими особами ЄС і НАТО у випадку виявлення великої загрози для критичної інфраструктури або суттєвої зміни в контексті безпеки;
2. Розробка регулярних паралельних та скоординованих оцінок загроз критичній інфраструктурі на основі оцінки, проведеної навесні 2023 року;
3. Посилення структурованого діалогу щодо стійкості та структурованого діалогу щодо військової мобільності та розширення існуючих штабних переговорів щодо кібернетики, космосу, моря та енергетики, а також між Міжнародним військовим штабом НАТО та Військовим штабом ЄС з метою:

   а) Поглиблення розуміння відповідних інструментів і процесів, які доступні кожній організації;

   б) Аналіз спостережень загарбницької війни росії проти України щодо стійкості критичної інфраструктури;

   с) Подальший аналіз і проведення глибшої оцінки наслідків для безпеки критичної інфраструктури відповідних ланцюгів постачання, енергетичного переходу та нових технологій.
4. Повне використання синергії між відповідними процесами, що випливають із політики та програм критичної інфраструктури ЄС і НАТО, включно з регулярними перехресними брифінгами для Групи стійкості критичних об'єктів ЄС та Військової групи Politico, а також Комітету стійкості НАТО;
5. Систематичне врахування стійкості критичної інфраструктури в будь-яких майбутніх паралельних і скоординованих навчаннях;
6. Проведення спеціалізованих обговорень на основі сценаріїв між персоналом для кращого розуміння викликів, взаємозалежностей і каскадних ефектів, у тому числі через прогнозний семінар ЄС-НАТО та за підтримки Європейського центру передового досвіду з протидії гібридним загрозам;
7. Підвищення обізнаності щодо наслідків для безпеки участі в критичній інфраструктурі або контролю над нею суб'єктами стратегічних конкурентів, а також про потенційні ризики, пов'язані з постачальниками з цих країн, у тому числі в мережах 5G;
8. Вивчення можливостей для обміну питаннями про те, як покращити моніторинг і захист критичної інфраструктури у морській сфері відповідними органами влади, а також обговорення шляхів підвищення обізнаності про морську ситуацію;
9. Сприяння обміну найкращими практиками між цивільними та військовими суб'єктами щодо впровадження відповідної політики та законодавства, пов'язаного з кібернетичною діяльністю, включно з відповідним законодавством, спрямованим на підвищення стійкості критичної інфраструктури до кібернетичної ситуації для більш стійкої армії;
10. Обмін найкращими практиками щодо підвищення стійкості критичної інфраструктури та

визначення потенційних шляхів її подальшого зміцнення, наприклад, шляхом оцінки необхідності, актуальності та здійсненності конкретних вимог до певної транспортної інфраструктури з метою пристосування до ваги, розміру чи масштабу військовий транспорт;

11. Визначення альтернативних транспортних шляхів як для цивільних, так і для військових цілей у разі значного порушення певного маршруту;
12. Сприяння взаємодії між членами Альянсу, державами-членами та приватним сектором, у тому числі щодо проектної безпеки критичної інфраструктури;
13. Сприяння обміну інформацією щодо управління міжсекторальними наслідками серйозних збоїв у роботі критичної інфраструктури, зокрема шляхом посилення співпраці між НАТО та Координаційним центром реагування на надзвичайні ситуації ЄС (ERCC).
14. Визначення синергії та потенційних сфер співпраці в дослідницькій діяльності безпеки, пов'язаній з критичною інфраструктурою, включаючи виклики, пов'язані з новими технологіями чи безпекою ланцюга постачання..

Структурований діалог ЄС-НАТО щодо стійкості координуватиме впровадження цих рекомендацій.

0840-23