SECURITY & DEFENCE QUARTERLY

https://securityanddefence.pl/

Захист критичної інфраструктури – фактори, суб'єкти та системи

Якуб М. Годзимірський

jmg@nupi.no

https://orcid.org/0000-0002-0396-8135

RAIT, Norwegian Institute of International Affairs NUPI, CJ Hambros plass 2 D, 0130, Oslo, Norway

Анотація

Основна мета цієї статті — дослідити, як у Норвегії вирішується питання захисту критичної інфраструктури. У статті розглядаються два важливі підпитання: що слід розуміти в поточному історичному та конкретному норвезькому контексті як важливі елементи національної КІ та яке поточне розуміння захисту КІ від ризиків і загроз. Ця стаття базується на детальному кількісному та якісному дослідженні офіційних норвезьких документів і заяв щодо питань, пов'язаних із різними аспектами захисту КІ в Норвегії. У першому розділі обговорюються структурні фактори, які відіграли важливу роль у формуванні норвезького мислення щодо КІ. У другому розділі подано короткий підсумок поточної дискусії щодо елементів КІ в Норвегії. У третьому розділі обговорюється офіційне норвезьке сприйняття загроз і те, як вони вирішують питання, пов'язані з КІ. У четвертому розділі розглядається поточний офіційний підхід до захисту КІ в країні. Процес побудови існуючої системи захисту КІ в Норвегії був зумовлений як внутрішніми, так і міжнародними проблемами. Система повинна дозволяти громадянам задовольняти свої потреби через доступ до різноманітних важливих суспільних функцій, але вона також має уможливлювати вирішення викликів, які виникають у міжнародному середовищі.

Ключові слова:

критична інфраструктура (КІ), загрози, Норвегія, безпека суспільства, національна безпека

Article info

Received: 30 October 2021

Revised: 12 June 2022

Accepted: 7 July 2022

Available online: 3 September 2022

Citation: Godzimirski, J. M. (2022) 'Protection of critical infrastructure in Norway – factors, actors and systems', Security and Defence Quarterly, 39(3), pp. 45–62. doi: 10.35467/sdq/151964.

Вступ

Метою цієї статті є вивчення того, як у Норвегії вирішуються питання, пов'язані із захистом КІ. Ці питання піднімаються на національному та міжнародному порядках денних протягом багатьох десятиліть і це привернуло увагу академічної спільноти та національних і міжнародних політиків (щодо нещодавньої публікації, яка розглядає ці теми, див. Collier and Lakoff, 2021). Як національні органи влади (Brunner and Suter, 2009), так і міжнародні організації, такі як ООН (Офіс ООН з боротьби з тероризмом і Рада Безпеки ООН, 2018) і ЄС (Європейська Комісія, 2005, 2013; див. Haemmerli et al., 2010), приділили підвищену увагу цим питанням у зв'язку з подіями, які виявили серйозні недоліки та вразливі місця в існуючих системах захисту КІ та антикризового менеджменту. Питання захисту КІ, що вирішується у національному та міжнародному контекстах, полягає в тому, що КІ відіграє роль у забезпеченні фундаментальних потреб населення та функціонуванні державних структур. У різних країнах ці питання вирішуються по-різному. У цій статті розглядається, як ці питання вирішуються в Норвегії, яка є відносно успішною у вирішенні цих питань, про що свідчить той факт, що вона займає дуже високі позиції в різних міжнародних рейтингах якості життя та управління.

У Норвегії, як і в багатьох інших демократичних країнах із добре розвиненою системою соціального забезпечення, ідея задоволення базових потреб населення шляхом забезпечення доступу до КІ незалежно від того, де люди живуть, є однією з ключових ідей, що інформують національну політику про КІ. Ця стаття намагається відповісти на питання про те, як ці загальні ідеї щодо надання доступу до КІ були перетворені на реальну політику захисту КІ в Норвегії. Щоб дати відповідь на це важливе питання, вкрай важливо відобразити, як різні структурні фактори вплинули на розвиток існуючої системи КІ в країні з історичної точки зору; представити ключові елементи поточної системи КІ та те, наскільки важливими вони сприймаються національною політико-політичною спільнотою; показати, як політико-політичне співтовариство та спеціалізовані національні органи оцінюють ризики та загрози, яким може піддатися КІ країни, що важливо при прийнятті рішень щодо розробки ефективної системи захисту КІ.

Щоб відповісти на ці важливі питання, ця стаття поділена на кілька розділів. У І-му розділі надається деяка інформація про структурні чинники, які зіграли важливу роль у формуванні норвежського погляду на КІ з більш тривалої історичної перспективи. ІІ-ий розділ містить короткий опис ключових елементів КІ в Норвегії. У ІІІ-му розділі обговорюється, які загрози для КІ визначені в офіційних норвезьких оцінках загроз, що є важливим внеском у процес формування політики в цій сфері, як це показано в роботі над новим законом про безпеку. У IV-му розділі розглядається, як питання, розглянуті в попередніх розділах, сприяли створенню поточного офіційного підходу, а також містить коротке обговорення інституційних обов'язків, законодавчої бази та впливу міжнародних подій і нормативних актів на поточний норвезький підхід. на це важливе питання.

Методологія

Ця стаття базується на детальному кількісному та якісному дослідженні набору з 35 офіційних норвезьких документів, створених переважно між 2014 і 2020 роками, в яких термін «kritisk infrastruktur» (КІ норвезькою) згадується понад 1600 разів. Зокрема, після російської інтервенції в Україну в 2014 році національні дебати з цих питань набули важливого повороту. Технологічні зміни останнього десятиліття, включно з посиленням

уваги до цифровізації КІ, що робить її більш уразливою для нових загроз, також стали важливим фактором (Popescu and Secrieru, 2018). Це обстеження включає не лише детальний аналіз ключових документів, пов'язаних із політикою, які представляють офіційні ідеї щодо викликів, з якими стикається норвезьке суспільство, але й дає додаткові відомості про те, як ці питання обговорювалися національними експертами.

Досліджуючи, як еволюціонував офіційний підхід до захисту КІ, також важливо визначити, як змінилися офіційні норвезькі оцінки загрози, опубліковані установами, відповідальними за безпеку країни, у цей неспокійний період. Ці офіційні уявлення про загрози зіграли важливу роль у роботі над підвищенням готовності системи захисту та управління інфраструктурою до протидії як новим, так і традиційним ризикам і викликам.

Структурні фактори

Є кілька структурних факторів, які вплинули на розвиток поточної системи інфраструктури в Норвегії. Швидкий погляд на карту країни пояснює, чому географічні фактори відіграли важливу роль. Територія Норвегії, 386 975 км^2, включаючи Шпіцберген і Ян-Майен, робить Норвегію однією з найбільших країн Європи. Материкова частина Норвегії, де проживає більшість людей, площею 323 895 км^2 трохи більша за Польщу, але складається з так званого фастленда (301 614 км^2) і кількох тисяч островів (22 280 км^2) з дуже довгою довжиною. берегова лінія. Норвегія також контролює величезну виключну економічну зону (2 385 178 км^2), де розташовані основні природні ресурси країни, включаючи нафту та морські ресурси. Оскільки ці ресурси необхідно розробляти, виробляти, транспортувати та продавати, до існуючої інфраструктури потрібно додати нові елементи, щоб зробити це можливим. Крім того, форма країни та її рельєф зробили процес будівництва фізичної інфраструктури складним завданням. Наприклад, відстань між найпівнічнішою точкою, Kinnarodden у Фіннмарку, та його найпівденнішим місцем у Ліндесні становить 1752 км по прямій. Лише 3,3% території країни визначено як орні землі, 38% займають ліси та рідколісся, тоді як решта – 59 % – займають гори та пустоші, болота та заболочені землі, озера та річки та міські території, де проживає більшість населення. Усі ці суто географічні фактори роблять забезпечення однакового рівня доступу до КІ по всій країні не лише економічним, а й технологічним і політичним викликом.

Майже всі політичні партії в Норвегії погоджуються з тим, що однією з найважливіших політичних цілей є забезпечення базових потреб населення незалежно від того, де люди живуть, і цього можна досягти лише шляхом забезпечення місцевого доступу до ключових елементів КІ та факторингу демографічних даних. У 2021 році населення Норвегії досягло 5,4 мільйона, що робить Норвегію однією з європейських країн з найнижчою щільністю населення. Це робить забезпечення доступу до КІ для всіх жителів країни досить складним і дорогим завданням, не в останню чергу через величезні регіональні відмінності. Наприклад, майже 44% населення країни проживає в Осло та двох сусідніх графствах, Вікен, Вестфолл і Телемарк, які займають лише 13% території країни, тоді як 2 найпівнічніших округи, Нурланн і Тромс, займають понад 34% території країни. територія і розташовані частково над полярним колом із суворими кліматичними умовами та містять лише 9% населення. Модель розселення з високим рівнем урбанізації, 82,3% населення у 2020 році, створює різні виклики. Забезпечення доступу до інфраструктури та послуг є відносно легким у густонаселених міських районах і більш складним у віддалених і іноді ізольованих сільських районах.

Крім географічних і демографічних факторів, політичні, історичні та економічні фактори відіграли свою роль у процесі побудови КІ в Норвегії. Політичні рішення, прийняті владою після відновлення незалежної державності в 1905 році, сформували рамкові політичні умови для економічної діяльності та відносини країни з іншими суб'єктами. Було кілька переломних подій, які вплинули на рішення щодо КІ в Норвегії. Ще до відновлення норвезької незалежної державності в 1905 році процес швидкої індустріалізації зробив великий внесок у формування національної інфраструктури (про особливий норвезький підхід до індустріалізації див. Slagstad, 1998, стор. 134–162). Швидка індустріалізація Норвегії була б неможливою без національної гідроенергетичної інфраструктури та електромережі, які сьогодні є наріжними каменями національної інфраструктури. Той факт, що Норвегія вже була важливим гравцем у міжнародному судноплавстві, також відіграв свою роль у розвитку деяких елементів національної транспортної та морської інфраструктури (докладніше про це див. у Government.no, 2021; Міністерство торгівлі, промисловості та рибальства, 2021 для поточного підходу до морських аспектів).

Досвід німецької окупації під час Другої світової війни був найбільшою національною травмою, а також був одним із факторів, які вплинули на рішення Норвегії в 1949 році приєднатися до НАТО, яке вважалося вирішальним для стримування нової радянської загрози. Бути членом альянсу у геополітично важливому місці також відіграло роль у розвитку національної інфраструктури, оскільки країна мала здійснити певні приготування для задоволення потреб союзників і мати можливість отримати їхню підтримку під час кризи (Міністерство закордонних справ справ, 2011).

Відкриття нафтових ресурсів на норвезькому континентальному шельфі стало ще одним фактором, який сприяв розвитку енергетичної та транспортної інфраструктури. Ця інфраструктура з’єднує Норвегію з Європою, і в її будівництві брали участь різні суб'єкти, які мають необхідні технологічні знання, економічні інтереси та фінансові ресурси (див., наприклад, Austvik, 2019; Schiefloe, 2016).

Нарешті, закінчення холодної війни відкрило вікно можливостей для переорієнтації уваги з жорсткої безпеки на інші аспекти безпеки, включаючи соціальну безпеку, роль соціальних служб і служб охорони здоров’я та розбудову норвезької моделі держави добробуту.

Питання соціальної стійкості та ролі інфраструктури також різко актуалізувалося після терористичних нападів на Сполучені Штати у 2001 році та знову актуалізувалося після трагічного терористичного нападу 22 липня 2011 року в Норвегії, який був, мабуть, найбільш травматичним для країни досвід за весь післявоєнний період і виявив деякі серйозні недоліки в національній системі захисту КІ та управління кризовими ситуаціями.

Членство Норвегії в НАТО та партнерство з ЄС через Європейську економічну зону (ЄЕЗ) також мало певні наслідки для національного обговорення та впровадження політики, пов’язаної із захистом елементів національної КІ (додаткову інформацію про підхід ЄС до КІ див. див. Європейська комісія, 2005, 2013; Європейська рада, 2008). Норвегія постачає енергію багатьом союзникам по НАТО та партнерам з ЄС і, реалізуючи свою політику щодо КІ, повинна враховувати інтереси цих двох організацій у цій сфері (Muller et al., 2018). Наприклад, однією з підстав для проведення навчань Trident Juncture у 2018 році було перевірити здатність Норвегії отримати підтримку НАТО у випадку великого конфлікту за участю великої регіональної держави. Конфлікт 2014 року в Україні та його наслідки призвели до більшої уваги до захисту КІ від різних гібридних загроз, включаючи

кібератаки та цифрові атаки на її важливі елементи та спроби деяких іноземних суб'єктів отримати доступ до елементів національної КІ та можливий контроль над ними. через інвестиції (Hallberg, 2019).

Політичні рішення також мали вирішальне значення для створення норвезького варіанту скандинавської моделі соціальної держави з певними особливостями (Frelle-Petersen та ін., 2020). Ці особливості включають широкий і універсальний доступ до послуг і істотну підтримку для створення добре функціонуючих мереж безпеки, щоб допомогти громадянам справлятися з ринковими провалами. Функціонування моделі також сприяє високий рівень довіри до людей та інституцій у скандинавських країнах (Grimen and Skirbekk, 2012; Houston et al., 2016; Saltkjel and Malmberg-Heimonen, 2014). Оскільки однією з головних функцій цієї моделі є забезпечення безперешкодного широкого та універсального доступу до тих елементів інфраструктури, які необхідні для задоволення основних соціальних, економічних і політичних потреб, створення та підтримка національної інфраструктури має першочергове значення для загального визнання цього специфічного скандинавського підходу.

Нарешті, рішення щодо створення національної системи КІ та найкращих способів її захисту від різноманітних викликів, ризиків і загроз також ґрунтувалися на зміні сприйняття загроз, питання, яке буде обговорено більш детально в одному з наступних розділів.

Що потрібно захищати – критична інфраструктура в Норвегії

Норвезький підхід до КІ не відрізняється від підходів, прийнятих в інших країнах. Питання КІ було на порядку денному норвезької громадськості протягом багатьох десятиліть. На його розвиток вплинули різні фактори, коротко розглянуті в попередньому розділі. Наприклад, у дослідженні 2000 року про вразливість суспільства в Норвегії було представлено те, що на той час вважалося ключовим елементом національної КІ (Міністерство юстиції та громадської безпеки, 2000). Цей інтерес до КІ також було чітко відображено в Білій книзі про захист КІ. У цьому документі КІ визначена як «споруди та системи, які мають важливе значення для підтримки найважливіших функцій суспільства, які з часом захищають основні потреби суспільства та відчуття безпеки та захищеності у широких кіл» (Міністерство юстиції та громадської безпеки 2006). Подібний підхід було прийнято в дослідженні DSB, опублікованому через 6 років (DSB, Норвезька дирекція цивільного захисту, 2012). Більше деталей також надано в інших офіційних документах (Міністерство юстиції та громадської безпеки, 2006, 2008), тоді як інші документи приділяли більше уваги основним ризикам, з якими може зіткнутися національна КІ (Міністерство юстиції та громадської безпеки, 2016).

Дослідження, опубліковане в 2007 році, розділило елементи інфраструктури на 3 основні категорії, 14 секторів, 61 підсектор тощо (Henriksen et al., 2007). У цьому дослідженні електроенергія та електронні комунікації описані як елементи базової КІ, тоді як вода та каналізація, нафта та газ, транспорт, банк і фінанси визначені як інші елементи КІ. Постачання продуктів харчування, утилізація відходів, охорона здоров’я та соціальні послуги, поліція та рятувальники, політичне керівництво, ЗМІ, важливі галузі з високим ризиком та національні символи були визначені як елементи, які мають вирішальне значення для інших функцій суспільства.

Чим можна пояснити центральну роль у системі КІ, яку відведено електроенергії та електронному зв’язку? Міністерство нафти та енергетики стверджує, що безперебійне

функціонування всієї країни залежить від безперебійного функціонування інфраструктури сектору виробництва електроенергії (Міністерство паливенерго та енергетики, 2017). Що робить ситуацію ще складнішою – і пояснює, чому електронний зв'язок також зазначений як базовий елемент КІ – це оцифрування сектора, що робить його більш вразливим до зловмисних дій у цифровому просторі.

У 2017 році DSB опублікував детальне дослідження (DSB Норвезька дирекція цивільного захисту, 2017) про те, які елементи КІ важливі для задоволення основних особистих і суспільних потреб. Детальний огляд цих основних потреб і елементів КІ, які є важливими в цьому контексті, представлено в таблиці 1.

До цих питань підходять з функціональної точки зору. КІ відіграє важливу роль у допомозі суспільству забезпечити його життєво важливі функції, оскільки вона надає громадянам доступ до різноманітних критично важливих послуг, які, у свою чергу, дозволяють їм задовольняти свої основні потреби. Таким чином, будь-який елемент інфраструктури можна визначити як дуже критичний, критичний або важливий, залежно від тяжкості наслідків, з якими може зіткнутися суспільство, якщо такий елемент буде знищено або зроблено непридатним для використання внаслідок зловмисних дій або стихійного лиха.

Цей функціональний підхід також відображено в новому Законі про безпеку, який набув чинності 1 січня 2019 року (Міністерство оборони, 2017; Stortinget, 2018). Закон розглядає елементи інфраструктури як такі, що заслуговують на захист, якщо основним національним функціям може бути завдано шкоди, якщо їхня функціональність зменшена або вони піддадуться вандалізму, пошкодженню чи незаконному захопленню (Stortinget, 2018, розділ 7.1).

Бруннер і Сатер (2009, с. 308) оцінюють критичність елементів інфраструктури за 3 критеріями: залежність, коли функціонування елемента інфраструктури залежить від належного функціонування інших елементів інфраструктури; відсутність альтернативи для опису ситуації, коли елемент інфраструктури не може бути замінений іншими елементами; тісний зв'язок, що означає, що міцні зв'язки та залежність від інших елементів інфраструктури передбачають більш високу критичність. Цей підхід також відображено в новому Законі про безпеку, в якому в розділі 4.2 про оцінку ризиків зазначено, що «кожне підприємство має визначити інші підприємства, від яких воно залежить для належного функціонування» (Stortinget, 2018).

Таблиця 1. Фундаментальні потреби та КІ

ФУНДАМЕНТАЛЬНІ ПОТРЕБИ		
Керованість і суверенітет	Безпека населення	Соціальна функціональність
Управління та антикризовий менеджмент **Оборона**	Правопорядок Здоров'я і турбота Аварійні служби Безпека ІКТ Природа і навколишнє середовище	Безпека постачання Вода та каналізація Фінансові послуги Блок живлення Електронні комунікаційні мережі та послуги Транспорт Супутникові послуги

Норвезьке сприйняття загроз і вразливостей

Оцінюючи фактичні та потенційні загрози для КІ, суб'єкти повинні, відповідно до чинної версії Закону про безпеку (Stortinget, 2018, розділ 7.2), робити оцінки потенційної шкоди, намагаючись виміряти, як фундаментальні національні функції, що підтримуються об'єктом, або інфраструктура може постраждати. Будь-яка оцінка загрози та ризику повинна розглядати 2 аспекти – можливий вплив події та її ймовірність. Такий підхід не є виключно норвезьким, оскільки він широко використовується на міжнародному рівні, коли досліджуються потенційний вплив і ймовірність різних ризиків і загроз (див. Всесвітній економічний форум, 2021 рік, і попередні видання).

У Норвегії є кілька офіційних виробників загальнодоступних оцінок загроз. Цей короткий огляд того, які загрози для КІ в Норвегії були виявлені в період після 2014 року, розділений на 3 частини. У І-ій частині перераховано основних постачальників оцінки загроз у Норвегії та описано їхню роль у цьому процесі. ІІ-га частина містить детальний аналіз того, які загрози КІ були виявлені цими офіційними установами. У ІІІ-ій частині наведено кілька прикладів для визначення вразливостей у норвезькому суспільстві, які виявили певні останні події.

Служба поліцейської безпеки (PST) — це служба внутрішньої безпеки Норвегії. PST розслідує та запобігає серйозним загрозам національній безпеці та публікує щорічні оцінки загроз, у яких виявлено різні загрози КІ.

Норвезька розвідувальна служба (NIS) або E-tjenesten — це служба зовнішньої військової розвідки Норвегії. Одним із його завдань є визначення того, як загрози, що виходять з міжнародного середовища, можуть вплинути на ситуацію в країні. Як і PST, служба публікує щорічні оцінки загроз, які також розглядають питання, важливі для захисту КІ в Норвегії.

Робота над превентивною національною безпекою є основним обов'язком Управління національної безпеки Норвегії (NSM). У своєму звіті Risiko NSM оцінює різні типи ризиків і загроз, з якими може зіткнутися норвезьке суспільство, включаючи шпигунство, диверсії, терористичні акти та інші. серйозні інциденти (докладніше про роль NSM див. Arnøy, 2020).

Управління цивільного захисту та планування на випадок надзвичайних ситуацій (DSB), яке займається питаннями ризиків і вразливостей у норвезькому суспільстві, публікує власні оцінки загроз і ризиків, які зосереджуються на ризиках великих інцидентів у Норвегії, приділяючи особливу увагу природним явищам, великим аваріям і навмисним діям, які також можуть мати негативний вплив на національну інфраструктуру.

Оскільки концепція тотальної оборони відіграє важливу роль у політиці безпеки Норвегії (Endregard, 2019, 2020), а Міністерство оборони є основним органом, відповідальним за національну безпеку, зрозуміло, що МО також надає деякі оцінки загроз (Міністерство оборони , 2016a).

Які загрози та вразливості, пов'язані з інфраструктурою, визначені в оцінках ризиків і загроз, проведених цими установами? Щоб дослідити це питання, ми розглянемо те, що можна назвати «змінною моделлю сприйняття загрози», знайденої в наборі офіційних оцінок загроз, опублікованих між 2014 і 2021 роками.

DSB у 2011 році опублікував аналізи ризику та майбутні сценарії, що зосереджуються на ризиках, пов'язаних з катастрофічними подіями, такими як стихійні лиха, основні нещасні випадки та навмисні дії, які можуть вплинути на норвезьке суспільство. Найновіше доступне вивчення можливих ризиків та криз було опубліковано в 2020 році та містить детальний перелік типів проблем, з якими може стикатися суспільство, яке також може мати негативний вплив на КІ та життєво важливі суспільні функції (DSB, Норвезький Управління цивільного захисту , 2020b). До них відноситься весь спектр природних та техногенних криз, що тягнуться від проблем, спричинених екстремальною погодою та затопленням, через проблеми, пов’язані зі здоров’ям, пожежі, сейсмічну діяльність, різні види нещасних випадків та інцидентів, порушення ціннісних ланцюгів, політичне насильство, включаючи тероризм, агресію іноземними державами та різними типами кібератак.

Таблиця 2. Офіційне сприйняття загроз, пов’язаних з КІ (2014-2021 рр.)

Рік	Документ	Загрози КІ
2015	PTS 2015	ворожі операції в кіберпросторі
2015	NIS Focus 2015	проведення диверсійних дій у кіберпросторі щодо елементів КІ з метою впливу на їх функціонування
2015	NIS Focus 2015	діяльність ворожих іноземних розвідувальних служб, які прагнуть отримати доступ до конфіденційної інформації для використання її проти КІ в конфліктній ситуації
2016	PTS 2016	зловмисну діяльність іноземних спецслужб, які прагнуть отримати доступ до інформації про КІ, щоб її саботувати
2016	PTS 2016	цифрові атаки на інфраструктуру Норвегії з боку іноземних спецслужб
2016	NIS Focus 2016	картографування вразливостей КІ в Норвегії іноземними спецслужбами
2017	PTS 2017	операції китайських та російських спецслужб, спрямовані на елементи КІ (найбільш викриті – сектор виробництва та розподілу електроенергії та послуги електронного зв’язку)
2019	NMS 2019	загрози, пов'язані з операціями іноземних спецслужб
2019	NMS 2019	мережевих операцій та інших цифрових загроз
2019	NMS 2019	інсайдерів, розміщених на ключових посадах, які можуть бути завербовані іноземними службами
2019	NMS 2019	операції впливу
2019	NMS 2019	картографування інфраструктури
2019	NMS 2019	глушіння та інші електронні операції
2019	NMS 2019	тероризм
2020	PTS 2020	цифрове картографування та диверсії проти КІ
2020	NIS Focus 2020	загрози критичній інфраструктурі через більш точні російські ракети з більшою дальністю
2020	NIS Focus 2020	Китай намагається отримати доступ до національної КІ через інвестиції в цифрову інфраструктуру
2020	NIS Focus 2020	розширене дослідницьке співробітництво з іншими державами, що може надати їм доступ до

		елементів інфраструктури в Норвегії
2020	NIS Focus 2020	Операції російських розвідувальних служб у Норвегії спрямовані на отримання розуміння створення нової військової інфраструктури
2020	NMS 2020	Зростаюча залежність суспільства від електронних комунікацій та супутникових послуг
2020	NMS 2020	залежність від виробництва електроенергії та енергетичної інфраструктури
2020	NMS 2020	зростаюча залежність від цифрової інфраструктури та ланцюжків створення вартості, які виходять за межі країни
2020	NMS 2020	стратегічні придбання, інвестиції або операції впливу
2021	PTS 2021	картографування інфраструктури Норвегії іноземними спецслужбами (рос.), включно з вербуванням норвезького персоналу для отримання інформації про елементи КІ (електропостачання, рух, водопостачання та каналізація виділені як найважливіші сектори)
2021	PTS 2021	загрози доступності КІ, спричинені іноземними інвестиціями
2021	NIS Focus 2021	мережеві операції, спрямовані на норвезьку цифрову інфраструктуру
2021	NIS Focus 2021	загрози західним і норвезьким підводним установкам
2021	NMS 2021	Іноземна власність на елементи інфраструктури може мати негативний вплив на безпеку
2021	NMS 2021	вплив національної цифрової інфраструктури на дії державних і недержавних суб’єктів
2021	NMS 2021	використання різними суб'єктами людських і цифрових вразливостей, що може мати негативні наслідки для захисту інфраструктури

Як згадувалося раніше, МО поділило деякі ідеї щодо важливості КІ. 2 нещодавно опубліковані документи заслуговують на більш детальний контроль. У документі 2016 року про довгострокові цілі та засоби в оборонній політиці (МО, 2016b) КІ згадується 7 разів. Документ стверджує, що напад на КІ може покалічити здатність збройних сил діяти, а особлива увага приділяється загрозам, спричиненим наступальними кібер -операціями (стор. 35).

У 2020 році був запущений новий довгостроковий план оборонного сектору (МО, 2020). Цей документ містить 12 згадок про термін «КІ» та перераховує загрози, створені внаслідок діяльності іноземних розвідувальних послуг ті.

Оскільки норвезька держава та суспільство беруть участь у міжнародному економічному співробітництві, питання, що стосуються захисту національної КІ, також розглядаються в ключових документах щодо зовнішньої політики. Роль країни як головного постачальника енергетичних ресурсів для Європи також зробила Норвегію важливою в міжнародному контексті.

Таким чином, Європа є найважливішим ринком норвезької енергетики та захисту норвезької енергетичної КІне тільки в національному, але й міжнародному контексті. Хоча Норвегія не є членом ЄС, країна працює в регуляторному просторі ЄС, коли мова йде про енергію та захист КІ (Міністерство закордонних справ, 2012a).

За останнє десятиліття було опубліковано кілька детальних оцінок норвезької зовнішньої політики, але вони мають справу з питаннями, пов'язаними з інфраструктурою, лише незначно. Біла книга 2015 року про зовнішню політику, яка зосереджується на нових проблемах глобальної безпеки (МЗС, 2015 р.). Зазначає КІ лише раз, визначення загрози електронних та цифрових операцій може створити національну інфраструктуру. Біла книга, опублікована в 2017 році (МЗС, 2017), містила лише 1 згадку про термін "критична інфраструктура" та перелічила різні види загроз, що виникають у копалинному просторі як основна проблема.

Які з можливих загроз та вразливостей, визначених у досліджених вище документах, виявилися реальними в норвезькому контексті? Що стосується історичного виміру, Løsnegård (2013) забезпечує популярний, але цікавий огляд основних природних та техногенних аварій та катастроф, з якими довелося боротися норвезькому суспільству. Більш систематичний та детальний огляд фактичних несприятливих подій з різних частин спектру загрози, які повідомили норвезьке мислення про ЗКІ, наведено у фонових розділах дослідження, що обговорюють фактори ризику, опубліковані англійською мовою DSB у 2020 році (DSB, Норвезький директор з цивільного захисту, 2020b). З моменту публікації цього детального звіту, Норвегія зазнала декількох трагічних подій, які виявили деякі недоліки та вразливість. Сюди входили терористичний напад, проведений правою крилкою на мечеті в серпні 2019 року, спалах глобальної пандемії навесні 2020 року, масовий зсув, черезх який загинуло 10 людей на околиці Осло в грудні, кілька нападів на норвезьку цифрову інфраструктуру , включаючи масштабну кібератаку на парламенті в 2020 році, та масове вбивство в Конгсберзі в жовтні 2021 року, яке забрало життя п’яти людей. Цей короткий перелік подій, що охоплюють лише останні 2 роки, показує, що захист КІ та забезпечення життєво важливих функцій у норвезькому суспільстві все ще заслуговує та привертає багато уваги громадськості. Офіційне уявлення про ризики, загрози та вразливості та фактичні несприятливі події змусили розробників політики усвідомити, наскільки важливим є питання захисту КІ в норвезькій соціальності. Такі ж несприятливі події та зміни в міжнародному середовищі також повідомили про роботу про створення національного підходу до ЗКІ.

Норвезька система управління та захисту критичної інфраструктури

У розвитку нинішнього норвезького підходу до КІ було кілька фаз. Вже в 90-х роках дослідницька організація (FFI) розпочала свою І-шу BAS (Beskyttelse AV Samfunnet або захист Товариства). Дискусія завершилася публікацією дослідницької роботи FFI про те, як зрозуміти концепцію КІ (Hagen and Fridheim 2005), і лише через рік Мін юст та громадської безпеки опублікувало свій насінний звіт про ЗКІ (Міністерство Справедливості та громадської безпеки, 2006 р.), що викликало національну дискусію з цих питань і призвело до опублікування нового Закону про безпеку у 2018 році.

Суб'єкти та обов'язки

Поточна система ЗКІ в Норвегії виникла з впровадженням нового національного закону про безпеку, що набуває чинності.

1 січня 2019 року (Stortinget, 2018) та замінив Закон про безпеку з 1998 року. Було кілька причин перегляду старого закону про безпеку з 1998 року.

І-ою причиною стала зростаюча напруга в міжнародному середовищі, спричиненому російською агресією проти України в 2014 році, яка вплинула на безпосередньо відносини між Заходом та росією, важливим сусідом Норвегії на Сході, і виявив здатність росії діяти за всіма масштабами ескалації конфлікту (Див. Jonsson and Seely, 2015).

ІІ-ою важливою причиною були технологічні зміни, особливо значно вищий рівень оцифрування в норвезькому суспільстві, що зробило як суспільство, так і національну КІ, більш піддані цифровим та кіберзагробам та ризикам. Це викликало усвідомлення того факту, що ЗКІ слід розглядати як проблему безпеки, оскільки "взаємопов'язаний характер цифрових систем робить ризик пошкодження та непередбачуваних наслідків серйозною проблемою" (Gjesvik, 2019, p. 11). Це пояснює, чому Закон про безпеку 2019 року розглядався в детальних питаннях, пов'язаних з інформаційною інфраструктурою (розділ 2.4 та глави 5 та 6 закону про безпеку).

Нарешті, зіткнувшись із більш складним набором проблем із безпекою, спричиненими змінами міжнародного середовища та технології, норвезькі особи, які приймають рішення, зрозуміли, що необхідний більш міжгалузевий, загальний та менш розділений підхід до управління та ЗКІ.

Поточна система управління та ЗКІ в Норвегії може бути описана наступним чином. Норвезький парламент, Стортінгет, після того, як проконсультувався з рішеннями з різними держ органами та експертним середовищем, надає політичні вказівки щодо політики ЗКІ в Норвегії, беручи до уваги норвезькі міжнародні зобов'язання. Політика, визначена парламентом, реалізується виконавчою владою.

Мін юст та громадської безпеки несе загальну відповідальність за управління питаннями, пов'язаними з цивільною безпекою, включаючи захист ключових об'єктів та елементів інфраструктури. Міністерство оборони відповідає за безпеку власних інфраструктурних систем.

Цей Закон несе відповідальність за захисну безпеку у конкретних сферах у відповідних секторальних міністерствах, які повинні співпрацювати з іншими державними установами та іншими державними та приватними суб'єктами, які контролюють елементи КІ. Ці міністерства повинні визначити та підтримувати огляд основних національних функцій, визначити та підтримувати огляд підприємств, що мають матеріальне значення для фундаментальних національних функцій та приймати рішення відповідно до розділу 1-3 І-ий пункт нового Закону про безпеку. Списки підприємств, які обробляють класифіковану інформацію, контрольну інформацію, інформаційні системи, об'єкти чи інфраструктуру, які мають життєво важливе значення для основних національних функцій, а також займаються діяльністю, яка має життєво важливе значення для основних національних функцій.

Також є 2 спеціалізовані установи, які безпосередньо стосуються питань, що стосуються ЗКІ. Норвезьке Управління з національної безпеки, який структурно розмістився під

Міністерством юстиції та громадської безпеки та під Міністерством оборони, несе відповідальність за профілактичну національну безпеку, консультує та контролює захист інформації, ОКІ національної значущості. NSM також несе національну відповідальність за виявлення, попередження та координацію відповідей на серйозні напади ІКТ. NSM також несе міжгалузеву відповідальність за закриття цих підприємств, які виконують захисну безпеку відповідно до нового закону про безпеку. Це дає право НСМ запропонувати міністерству приймати відповідне рішення щодо захисної роботи, включаючи ЗКІ, та подати це питання до міністерства, яка несе загальну відповідальність за захисну роботу в цивільному секторі або міністерство, що несе загальну відповідальність за захисну безпеку в секторі оборони за остаточне рішення

Дирекція з питань цивільного захисту та планування надзвичайних ситуацій (DSB), яка розміщується безпосередньо під Міністерством юстиції та громадської безпеки, відповідає за підтримку огляду ризиків та вразливості в норвезькому суспільстві.

ЗКІ також делегується двома норвезькими організаціями розвідки, Службою поліцейської безпеки (PST), відповідальними за внутрішню безпеку та норвезьку розвідувальну службу (NIS), яка відповідає за виявлення загроз, що виникають з-за кордону. NIS співпрацює з послугами інших країн НАТО та допомагає політичним рішенням у вирішенні питань, важливих для національної спільноти, включаючи ЗКІ проти злоякісних дій, що походять з-за кордону.

Існує 4 основні та всебічні принципи для організації роботи з захисту та управління КІ щодня та в кризі (Міністерство юстиції та громадської безпеки, 2016). Це:

• відповідальність, що означає, що суб'єкти, відповідальні за елементи КІ в нормальній ситуації, відповідають за функціонування одних і тих же елементів інфраструктури в кризі;

• схожість, що означає, що при боротьбі з кризою організації повинні організувати свою роботу так само, як і в періоди, що не є кризами;

• близькість, що означає, що будь -яка криза повинна боротися на найнижчому можливому рівні;

• співпраця, що означає, що всі органи влади та суб'єкти, відповідальні за елементи КІ, важливі для забезпечення різних функцій у суспільстві, повинні координувати свою роботу як у звичайні часи, так і під час різних видів кризи.

Огляд галузевих обов'язків, заснованих на дослідженні 1 з останніх пропозицій державного бюджету, наведено в таблиці 3, де обов'язки в деяких ключових секторах більш детально відображаються.

Оскільки основна мета політики - забезпечити безперебійне функціонування норвезького суспільства шляхом забезпечення доступу до різних життєво важливих або критичних функцій, цей функціональний підхід також використовується при призначенні інституційних обов'язків. Теоретично, 1 галузева міні-спроба несе основну відповідальність за вирішення питань, пов'язаних з "його" сектором, але інші державні установи та суб'єкти, включаючи інші міністерства з принципом співпраці.

Однак на практиці все ще існують серйозні проблеми з міжнародною координацією політики, як це стосується випадків двигунів Берген, в якому Міністерство торгівлі було готовим продати цю стратегічно важливу компанію, яка обробляє деяку конфіденційну інформацію для російських інтересів та операції було зупинено Міністерством юстиції та

громадською безпекою лише після втручання, яке висловило глибоку стурбованість впливом запланованого продажу на національну безпеку та безпеку союзників Норвегії, які використовували експертизу компанії.

Таблиця 3. Норвегія 2020: Інституційні обов'язки щодо забезпечення різних елементів інфраструктури та критичних функцій у суспільстві (на основі Міністерства юстиції та громадської безпеки, 2019, с. 34–36).

Критичні функції та області	**Відповідальне міністерство**	**Відповідальні організації, що підтримують**	**Інші відповідальні міністерства**
Електронна комунікація та послуги	Міністерство транспорту	Норвезьке управління комунікацій (NKOM), Nødnett (DNK), Збройні сили, компанії з цього сектору	Міністерство юстиції, Міністерство оборони
Захист ІКТ в цивільному секторі	Міністерство юстиції	Норвезька Управління національної безпеки (NSM), Норвезький Центр інформаційної безпеки (NORSIS), Норвезький орган захисту даних (DataTilsynet), Норвезький орган зв'язку (NKOM), Управління цивільного захисту та планування надзвичайних ситуацій (DSB), власників критично важливих систем даних , цифрові регістри та архіви, норвезьке агентство з цифрової цифрової діяльності (DIFI)	Міністерство транспорту, Міністерство місцевого самоврядування та модернізації, інші міністерства
Супутникове спілкування та навігація	Міністерство транспорту	Норвезьке космічне агентство, Норвезька прибережна адміністрація, Норвезька Управління з питань зв'язку (NKOM), Норвезьке управління картографування	Міністерство юстиції, Міністерство торгівлі, промисловості та рибного господарства, Міністерство місцевого самоврядування та модернізація
Енергетичний сектор	Міністерство нафти та енергетики	Норвезька Управління з водних ресурсів та енергетики (NVE), Норвезьке агентство з електропостачання (KBO), Statnett SF, Statkraft, районні опалення, енергетичні та сітчасті компанії, DSB, Метеорологічний інститут	Міністерство юстиції, Міністерство освіти та досліджень

Заключні зауваження

У цій статті вивчено, які фактори впливають на розвиток існуючої системи захисту КІ в Норвегії. Він також мав на меті вивчити, які елементи національної інфраструктури визначаються сьогодні як критичні, і дізнатися більше про те, до яких загроз та ризиків ця національна інфраструктура може бути піддана. Оскільки ми припустили, що сприйняття загрози, що розвиваються, також відіграють вирішальну роль у еволюції офіційного підходу до КІ в Норвегії, у статті також розглядається, як офіційні сприйняття загрози розвивалися між 2014 та 2021 роками.

В останньому розділі було вивчено форму поточної національної системи ЗКІ, з новим законом про безпеку як юридичної основи для її функціонування. Ця експертиза демонструє, що на створення існуючої системи дійсно сильно вплинуло всі перераховані вище фактори. Процес створення норвезької системи ЗКІ був поінформований функціональним підходом до КІ. Такий підхід означає, що це не насамперед захист фізичних елементів КІ, що є головною метою політики, а скоріше питання про те, як забезпечити функціонування суспільства в ситуації, коли деякі елементи інфраструктури знаходяться ризик або інвалід.

Коли сучасні суспільства - і норвезьке суспільство тут не є винятком - повинні боротися з наслідками несприятливих подій, що впливають на їх здатність задовольнити різні потреби населення, головним викликом, з яким вони стикаються, є той факт, що ці наслідки скорочуються в різних сферах відповідальності, що ускладнює управління кризою. Крім того, різні функції в сучасному суспільстві настільки сильно переплетені, що якщо одна важлива функція буде виконана з дій, проблеми можуть легко перерости та перекинутися на інші сфери (DSB, Норвезький директор з питань цивільного захисту, 2020b). Наприклад, можна уявити, який вплив важлива і тривалий провал національної системи електроенергії та розподілу може мати на норвезьке суспільство, якщо це сталося в середині суворої зими без альтернативних джерел електроенергії, щоб забезпечити Опалення та доступ до здоров'я та інших послуг. Основна невдача норвезької системи транспортування газу до ЄС, яка є частиною як національної, так і міжнародної КІ, з іншого боку, матиме відносно незначні наслідки для норвезького суспільства, але дуже серйозні наслідки для споживачів газу в ЄС які залежать від запасів норвезького газу, щоб покрити свої енергетичні потреби. Останній приклад - це хороша ілюстрація транснаціональної природи викликів, пов’язаних із ЗКІ, яка ще більш помітна в Норвегії, яка добре інтегрована на міжнародному рівні та відіграє основну роль як головний постачальник енергії в ЄС.

Таким чином, на норвезьку політику щодо ЗКІ сильно впливає рішення інших суб'єктів, що стосуються тих самих питань. Країна була членом-засновником НАТО в 1949 році, і її безпека залежить від здатності та готовності інших членів НАТО надати допомогу. Щоб мати можливість отримати цю допомогу, Норвегії довелося розробити адекватну інфраструктуру. Приналежність Норвегії до ЄС через її член в рамках ЄЕП також відіграла роль у розробці інфраструктури та роботи над національними правилами, пов'язаними з інфраструктурою. Тому деякі елементи норвезької національної інфраструктури, особливо енергетичної інфраструктури, а також морська та транспортна інфраструктура, мають вирішальне значення не лише для громадян Норвегії, але і для країн, які покладаються на постачання енергії чи інших товарів з Норвегії. Ці сильні інституційні зв'язки як з НАТО, так і з ЄС також мали певний вплив на еволюцію норвезької системи управління та ЗКІ (див. Міністерство закордонних справ, 2012b).

Однак еволюція цієї системи була зумовлена здебільшого внутрішніми факторами та міркуваннями. Ідея надання доступу до життєво важливих функцій для всіх мешканців, які можуть таким чином задовольнити різні суспільні, економічні, політичні та інші потреби, незалежно від того, де вони живуть на території країни, є однією з ідей, що керують розвитком Північна модель стану добробуту. Тому не повинно бути дуже дивним, коли бачить, що ця ідея також була однією з головних ідей, що керують роботою над новою системою для розробки КІ, яка виникла внаслідок введення нового закону про безпеку 1 січня 2019 року . Ця система повинна зробити Норвегію кращою підготовленою для впорання з новими проблемами, що виникають, випливаючи з міжнародного середовища, де такі актори, як Росія чи Шин цілий спектр ескалації конфліктів. Поява та розповсюдження нових технологій, особливо зростаючий рівень оцифрування, також було фактором, що змушує норвезьких осіб, які приймають рішення, прийняти більш всебічний підхід до питання про ЗКІ, яка чітко відображається в останній офіційній оцінці викликів, з якими стикається норвезьке суспільство (Міністерство юстиції та громадської безпеки, 2020).

Фінансування

Проект монет, проведений у NUPI, що фінансується Радою досліджень Норвегії RCN.

Заява про наявність даних

Не застосовується.

Заява про розголошення

Автор не повідомляв про потенційний конфлікт інтересів.

Автор прочитав і погодився з опублікованою версією рукопису.

Посилання

Арной, М.С. (2020) "Nasjonal Sikkerhetsmyndighet: ролик OG Ansvar I Krisehåndtering", в А.К. Ларссен і G.L. Dyndal (ред.), Strateceisk Ledelse I Krise OG Krig. DET NORSKE Systemet. Осло: Universitetsforlaget, стор. 167–182.

Оствік, О.Г. (2019) «Норвегія: мала держава у великій європейській енергетичній грі», у Дж. CHAM: Palgrave Macmillan, С. 139–164.

Brunner, E.M. and Suter, M. (2009) "Міжнародний посібник CIIP 2008 /2009", в інвентаризації 25 національних та 7 міжнародних політики захисту критичної інформаційної інфраструктури. Цюріх: Центр досліджень безпеки ETH. Доступно за адресою: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-forsecurities-studies/pdfs/ ciip-hb-08-09.pdf (доступ: 10 Липень 2021 р.).

Collier, S.J. та Лакофф, А. (2021) Уряд надзвичайних ситуацій: життєво важливі системи, досвід та політика безпеки. Принстон, штат Нью -Джерсі: Princeton University Press.

DSB Норвезька Управління цивільного захисту (2012 р.) Sikkerhet I Kritisk Infrastruktur OG Kritiske Sam- Funnsfunksjoner- Modell для Risikostyring Overordnet (безпека в критичній інфраструктурі та критичних соціальних функціях- модель загального управління

ризиками). Tønsberg: DSB. Доступно за адресою: https://www.dsb.no/globalassets/dokumenter/ rapporter/sikkerhet-i-kritisk-infrastruktur.pdf (доступ: 28 вересня 2020).

DSB Норвезька Управління цивільного захисту (2017) Життєві функції в суспільстві. Які функціональні можливості повинні підтримувати суспільство у будь-який час? Tønsberg: Норвезький директор DSB з цивільного захисту. Доступно за адресою: https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-ii_english_version.pdf (доступ: 26 вересня 2020).

DSB Норвезький директор з питань цивільного захисту (2020a) Risikostyring I Digitale Verdikjeder. Раппорт FRA en arbeidsgruppe Ledet av професор Олав Лісне (управління ризиками в цифрових ланцюгах вартості). Tønsberg: DSB. Норвезька управління цивільного захисту. Доступно за адресою: https://www.dsb.no/globalassets/dokumenter/ rapporter/risikostyring-i-digitale-verdikjeder.pdf (доступ: 23 травня 2021).

DSB Норвезький директор з питань цивільного захисту (2020b) Аналізи кризових сценаріїв 2019. Tønsberg: Норвезький директор DSB з цивільного захисту. Доступно за адресою: https://www.dsb.no/globalassets/dokumenter/ rapporter/p2001636_aks_2019_eng.pdf (доступ: 15 жовтня 2021).

Endregard, M. (2019) "Totalforsvaret I et sivilt perspektiv", у P. norheim-martinsen (ред.), Det Nye TotalForsvaret. Осло: Гілдендал, с. 62–80.

Endregard, M. (2020) "TotalForsVaret - Samfunnet I Væpnet Konflikt", в A.K. Ларссен та Г. Л. Діндал (ред.),

Стратегісіска Ledelse I Krise OG Krig. DET NORSKE Systemet. Осло: Universitetsforlaget, с. 406–434.

Європейська комісія (2005) Зелений документ про європейську програму критичної інфраструктурної захисту, COM (2005) 576 фінал. Брюссель: Європейська комісія. Доступно за адресою: https://op.europa.eu/en/publication- detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/мова-ен (доступ: 13 жовтня 2021).

Співробітники Комісії Європейської Комісії (2013), що працюють з новим підходом до Європейської програми щодо критичної інфраструктури, що робить європейську критичну інфраструктуру більш безпечною. Брюссель: Європейська комісія. Доступно за адресою:
https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_ korting_document.pdf (доступ: 23 вересня 2021).

Європейська рада (2008) Директива Ради 2008/114/ЄК від 8 грудня 2008 р. Про ідентифікацію та розробку європейської критичної інфраструктури та оцінки необхідності поліпшення їх захисту. Брюссель: Європейська рада.

Frele-Petersen, C., Hein, A. and Cristansen, M. (2020) «Модель Північної соціального забезпечення. Уроки реформи », Deloitte Insights. Копенгаген: Делойт. Доступно за адресою: https://info.deloitte.no/rs/777-lhw-455/images/ the-nordic-social-welfare-model-report.pdf (доступ: 20 жовтня 2021).

Gjesvik, L. (2019) Порівняння кібербезпеки. Захист критичної інфраструктури в Норвегії, Великобританії та Фінляндії.

Осло: Нупі. Доступно за адресою: http://hdl.handle.net/11250/2598280 (доступ: 14 жовтня 2021).

Уряд. Ні (2021 р.) Океанська нація Норвегії. Доступно за адресою: https://www.regjeringen.no/en/topics/havet/ the-ocean-nation-of-norway/id2609341/(доступ: 23 жовтня 2021).

Grimen, H. and Skirbekk, H. (ред.) (2012) Tillit I Norge (довіра до Норвегії). Осло: res publica.

Hagen, J. та Fridheim H. (2005) 'HVA er Kritisk Infrastruktur? (Що таке критична інфраструктура) ', FFI/NOTAT- 2005/00363. Kjeller: Forsvartes forskningsinstitutt. Доступно за адресою: https://www.regjeringen.no/no/dokumenter/ nou-2006-6/id157408/sec4 (доступ: 22 жовтня 2021).

Haemmerli, B., Renda, A. та Центр досліджень європейської політики (2010), що захищає критичну інфраструктуру в ЄС. Звіт про цільову групу CEPS. Доступно за адресою: https://www.ceps.eu/download/publication/?id=6906&pdf= Critical%20Infrastructure%20 - захист%20Final%20A4.pdf (доступ: 22 вересня 2021).

Hallberg, J. (2019) Інвестиційний скринінг у чотирьох північних країнах - огляд. Доступно за адресою: https: // www. kommerskollegium.se/contentassets/2781b31214234afabd749e170c77c8ff/investment-screening-in-four- Northern-Countries.pdf (доступ: 12 вересня 2021).

Henriksen, S., Sørli, K. and Bogen, L. (2007) Метода для ідентифікації OG Rangering Av Kriticke Samfunns- Funksjoner. Kjeller: Forsvarets forskningsinstitutt. Доступно за адресою: https://publications.ffi.no/nb/item/asset/ dspace: 3325/07-00874.pdf (доступ: 12 червня 2021).

Х'юстон, Д. Дж., Айталіне, Н., Морлолок, А.Л. та Шультс, С.А. (2016) «Довіра громадян до державних службовців: міжнаціональний іспит», Міжнародний журнал державного управління, 39 (14), стор. 1203–1214. doi: 10.1080/01900692.2016.1156696.

Jonsson, O. and Seely, R. (2015) «Російський конфлікт у повному спектрі: оцінка після України», Журнал слов'янських військових досліджень, 28 (1), стор. 1–22. Доступно за адресою: https://doi.org/10.1080/13518046.2015.998118 (доступ: 15 травня 2021).

Løsnegård, G. (2013) Norske Ulykkar OG Katastrofar (Норвезькі аварії та катастрофи). Осло: Скальд.

Міністерство оборони (2016a) Самандлінг для Sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid (діє разом для безпеки. Захист основних суспільних функцій у зміну часу). Осло: Міністерство оборони. Доступно за адресою: https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/ (доступ: 20 жовтня 2020).

Міністерство оборони (2016b) проп. 151 с (2015–2016). Kampkraft OG Bærekraft. Langtidsplan для Forsvarssektoren (бойова влада та стійкість. Довгостроковий план оборонного сектору). Осло: Міністерство оборони. Доступно за адресою: https://forsvaret.no/forsvarsmateriell/forsvaretdocuments/kampkraft%20og%20b%C3%A6Rekraft.pdf (доступ: 19 травня 2021).

Міністерство оборони (2017) Пред. 153 L. Пропозиція Lov OM Nasjonal Sikkerhet (Sikkerhetsloven). Осло: Міністерство оборони. Доступно за адресою: https://www.regjeringen.no/contentassets/0fceee45affd24280896b-88b5413a00aa/no/pdfs/prp201620153000dddpdfs.pdf (доступ: 19 травня 2021).

Міністерство оборони (2020 р.) Пред. 62 S 21 VILJE TIL BERERDSKAP- EVNE TIL FORSVAR- LANGTIDSPLAN для Forsvarssektoren (готовність бути підготовленою- здатність захищати- довгостроковий план оборонного сектору). Осло: Міністерство оборони. Доступно за адресою: https://www.regjeringen.no/contentassets/b43ae5a187034670adc96a83fbf79651/no/ pdfs/prp201920200062000dddpdfs.pdf (доступ: 19 травня 2021).

Міністерство закордонних справ (2011) Meld. St. 24 2010–2011 Samarbeidet I NATO I 2010 (співпраця в НАТО в 2010 році). Осло: Міністерство закордонних справ. Доступно за адресою: https://www.regjeringen.no/contentassets/9da57b- b221a247e3aff26f54d8f6fef8/nn-no/pdfs/stm20101010024000dddpdfs.pdf (доступ: 10 жовтня 2020).

Міністерство закордонних справ (2012a) Utenfor OG Innenfor: Norges Avtaler Med Eu (зовні та всередині: Угоди Норвегії з ЄС). Осло: Міністерство закордонних справ. Доступно за адресою: http://www.regjeringen.no/ сторінки/36797426/pdfs/nou201220120002000dddpdfs.pdf (доступ: 13 липня 2021).

Міністерство закордонних справ (2012b) Пред. 130 S (2011–2012) Пропозиція Samtykke til Godk-Jenning av eøs-komiteens, що не піддається nr. 101/2012 AV 30. Квітень 2012 р. OM Innlemmelse I Eøs-Avtalen AV ECIP Direktiv 2008/114/EF (згода на затвердження рішення Комітету ЄЕА № 101/2012 від 30 квітня 2012 року про включення до Угоди ЄЕА до Директиви ECIP 2008/114 / EF). Осло: Міністерство закордонних справ. Доступно за адресою:
https://www.regjeringen.no/contentassets/1a7d9c8a19624cf4ba7543589dd4f885/no/pdfs/prp 201120130000dddpdfs.pdf (доступ: 13 вересня 2020).

Міністерство закордонних справ (2015) Meld. Св. 37 (2014–2015) Мелдінг Тіль Стортінгет. Globale sikkerhetsutfor- dringer i utenrikspolitikken. Тероризм, orgenisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digi-tale rom (глобальні проблеми безпеки у зовнішній політиці Норвегії- тероризм, організована злочинність, піратство та кібер-загрози). Осло: Міністерство закордонних справ. Доступно за адресою: https://www.regjeringen.no/contentassets/bdf4bd40d57d4dc-
79409de87419a2217/no/pdfs/stm201420150037000dddpdfs.pdf (доступ: 13 вересня 2020)

Міністерство закордонних справ (2017) Meld. St. 36 (2016 - 2017) Melding Til Stortinget. Veivalg I Norsk Utenriks- og sikkerhetspolitikk (встановлення курсу норвезької іноземної політики та політики безпеки). Осло: Міністерство закордонних справ. Доступно за адресою:
https://www.regjeringen.no/contentassets/0688496c2b764f029955cc6e2f2799c/no/pdfs/ stm20162017003000dddpdfs.pdf (доступ: 10 листопада 2020).

Міністерство юстиції та громадської безпеки (2000) та Сербарт Самфунн- Утфордрінгер для Sikkerhets- og Bedskapsar- Beidet I Samfunnet (вразливе суспільство- виклики для роботи над безпекою та громадською безпекою в суспільстві). Осло: Міністерство юстиції та громадської безпеки. Доступно за адресою: https://www.regjeringen.no/no/dokumenter/nou-2000-24/ id143248/(доступ: 13 вересня 2020 р.).

Міністерство юстиції та громадської безпеки (2006) Нір Сіккерхетен Ектігст. Beskyttelse AV-ландететів Kritiske Infras-TrukTerure OG Kritiske Samfunnsfunksjoner (коли безпека є найважливішою. Захист критичних інфрачервоних структур країни та критичних соціальних функцій). Осло: Міністерство юстиції та громадської безпеки. Доступно за

адресою: https: // www. regjeringen.no/no/dokumenter/nou-2006-6/id157408/ (доступ: 23 вересня 2020).

Міністерство юстиції та громадської безпеки (2008) St.Meld. nr. 22 (2007–2008) Samfunnssikkerhet. Samvirke OG Samordning (безпека суспільства. Взаємодія та координація). Осло: Міністерство юстиції та громадської безпеки. Доступно за адресою: https://www.regjeringen.no/contentassets/ff6481eba7bf495f8532c2eeb603c379/no/pdfs/stm20072008002000dddpdfs.pdf (доступ: 23 вересня 2020).

Міністерство юстиції та громадської безпеки (2016) Meld. St. 10 (2016–2017) Risiko I et Trygt Samfunn - Samfunnssikkerhet (ризик у безпечному суспільстві - соціальне забезпечення). Осло: Міністерство юстиції та громадської безпеки. Доступно за адресою: https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm2012010010000dddpdfs.pdf (доступ: 23 вересня 2020).

Міністерство юстиції та громадської безпеки (2019) Пред. 1 S (2019 - 2020) Пропозиція Осло: Міністерство юстиції та громадської безпеки. Доступно за адресою: https://www.regjeringen.no/contentassets/218e2d95e8e54cf685d3aaeba909ef44/no/pdfs/prp2019202001kuddddpdfs.pdf (доступ: 23 Вересня 2020 р.).

Міністерство юстиції та громадської безпеки (2020) Meld. St. 5 (2020 - 2021) Samfunnssikkerhet I en usikker verden (соціальне забезпечення в небезпечному світі). Осло: Міністерство юстиції та громадської безпеки. Доступно за адресою: https: // www. regjeringen.no/no/dokumenter/meld.st.-5-20202021/id2770928/ (доступ: 23 січня 2021).

Міністерство нафти та енергетики (2017) за Budsjettåret 2018. (Prop. 1 S (2017–2018) (за бюджетний рік 2018). Осло: Міністерство нафти та енергетики. Доступно за адресою: https://www.regjeringen.no/ContentAssets/EC4BA37A7736466A9D04BA8F8B27F0D6/NO/PDFS/PRP201720180001OEDDDPDFS.PDF (доступ: 23 вересня 2020).

Міністерство торгівлі, промисловості та рибного господарства (2021) Блакитний океан, Зелене майбутнє. Прихильність уряду до океанської та океанської промисловості. Осло: Міністерство торгівлі, промисловості та рибальства.

Muller, L.P., Gjesvik, L. and Friis, K. (2018) Кіберблематики в міжнародній політиці. Можлива диверсія проти норвезького нафтового сектору. Осло: Нупі. Доступно за адресою: https://nupi.brage.unit.no/nupi-xmlui/bitstream/ручка/11250/2486814/nupi_report_2018-3.pdf? Sequence = 1 & isalle = y (доступ: 30 січня 2021).

Popescu, N. and Secrieru, S. (ред.) (2018) Хакки, витоки та збої. Російські кібер -стратегії, статті Chaillot. Париж: Інститут досліджень безпеки Європейського Союзу.

Saltkjel, T. та Malmberg-Heimonen, I. (2014) "Соціальні нерівності, соціальна довіра та участь громадян-справа Норвегії", Європейський журнал соціальної роботи, 17 (1), стор. 118–134. doi: 10.1080/13691457.2013.789004.

Schiefloe, P.M. (2016) "Norge og oljen", в I. frønes та L. Kjølsrød (ред.), Det Norske Samfunn. 7. Utgave. Осло: Gyldendal Akademisk, с. 139–167.

Slagstad, R. (1998) De Nasjonale Strateger. Осло: Pax forlag.

Stortinget (2018) Lov Om Nasjonal Sikkerhet (Sikkerhetsloven) (закон про національну безпеку). Осло: Сторінгет. Доступно за адресою: https://lovdata.no/dokument/nl/lov/2018-06-01-24 (доступ: 23 вересня 2020).

Управління ООН з питань боротьби з тероризмом та Радою Безпеки Організації Об'єднаних Націй (2018) Захист критичної інфраструктури від терактів: збірник хороших практик. Нью -Йорк, Нью -Йорк. Доступно за адресою: https: // www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021 /jan/compen- dium_of_good_practices_eng.pdf (доступ: 24 вересня 2021 .).

Всесвітній економічний форум (2021) Звіт про глобальні ризики 2021, 16 -е видання. Глобальні звіти про ризик. КОЛОГ, Женева: Всесвітній економічний форум.