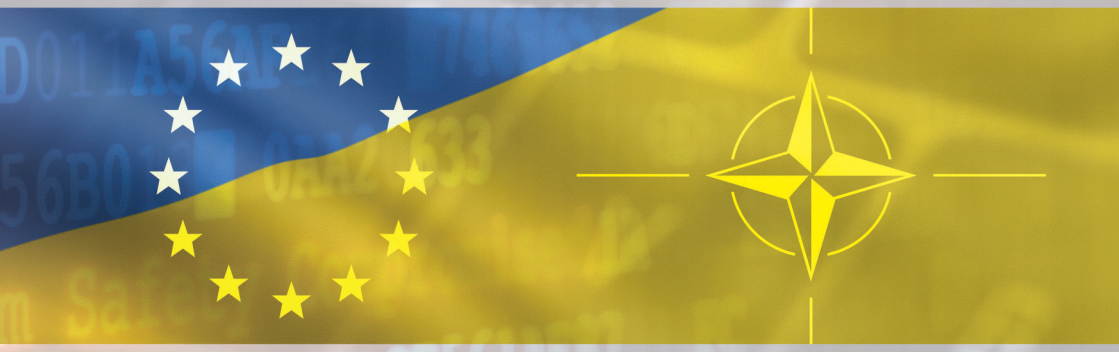
KONRAD ADENAUER STIFTUNG

Strategy XXI Стратегія

SYNERGING ENERGIES
Centre for Global Studies / Центр Глобалістики

Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері



Київ, 2019

KONRAD ADENAUER STIFTUNG

Strategy XXI Стратегія

SYNERGING ENERGIES
Centre for Global Studies / Центр Глобалістики

Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері

Київ
2019

Співробітництво Україна – ЄС – НАТО
з протидії гібридним загрозам у кіберсфері

В аналітичному документі зроблено порівняльний аналіз нормативно-правової бази, інституційних можливостей та рівня активності із протидії гібридним загрозам в ЄС, НАТО й Україні у кіберсфері, а також оцінку поточного стану співпраці між ЄС і НАТО та обох організацій з Україною у сфері кібербезпеки. На основі аналізу поточних викликів і загроз у кіберсфері та прогнозу їх трансформації з врахуванням подальших агресивних намірів РФ у контексті проведення президентських і парламентських виборів в Україні та виборів до Європейського Парламенту, описані формати можливого розвитку співпраці України з ЄС і НАТО у сфері кібербезпеки.

Аналітичний документ підготовлено Михайлом Гончаром, президентом Центру глобалістики «Стратегія XXI» та Віталієм Мартинюком, виконавчим директором організації на основі попередніх напрацювань Центру за кібер-напрямком досліджень, за підтримки та у співпраці з Представництвом Фонду Конрада Аденауера в Україні. Його зміст є виключно відповідальністю Центру глобалістики «Стратегія XXI» і не обов'язково відображає точку зору Фонду Конрада Аденауера.

ЗМІСТ

Вступ

Сучасні загрози в Європі, які з'явились після початку російської агресії проти України у 2014 році, є актуальними не лише для України, але й для інших країн, що є членами ЄС і НАТО, або ж взяли курс на набуття членства в цих організаціях. Про це свідчать заключні декларації самітів НАТО, починаючи з Уельського, та Глобальна стратегія ЄС й інші стратегічні документи, якими була введена дефініція «гібридні загрози». Серед таких загроз першочергово виділяються дезінформаційні кампанії, які спрямовані на внесення розколу в країнах та союзах, і втручання в інформаційні та комп'ютерні системи.

Україна та ЄС і НАТО опинились в певному взаємозв'язку, коли Україна не може самостійно протистояти поточним загрозам з боку Росії без міжнародної підтримки, а ЄС і НАТО – зацікавлені в просторі миру і стабільності в межах української території, що гарантуватиме їхню власну безпеку. Це створює підґрунтя для тристороннього безпекового партнерства з метою зміцнення стабільності у Європі в контексті гарантування безпеки в та навколо України з довгостроковою метою забезпечення регіональної стабільності, миру та процвітання.

Україна вже має певний досвід протистояння гібридним загрозам. Саме в Україні Кремль випробовує нові методи і засоби ведення гібридної війни. Однак, відсутність достатніх ресурсів та засобів для самостійного відбиття агресії Росії посилює важливість не тільки політичного сприяння на міжнародній арені з боку ЄС і НАТО, але й практичної допомоги у розвитку здатності України протистояти цим сучасним загрозам. У цьому контексті кібербезпека опинилась у центрі взаємодії Україна-НАТО-ЄС. Вона увійшла до переліку семи ключових напрямків безпекової співпраці НАТО-ЄС, визначених у Спільній декларації про співробітництво НАТО і ЄС, стала пріоритетом для обох організацій у наданні ними допомоги з посилення українських можливостей гарантувати власну безпеку.

Сфера кібербезпеки яскраво демонструє безпекову взаємозалежність України, ЄС і НАТО. Технічно Україна потребує допомоги та підтримки з боку обох організацій, але й українські інституції, які відповідають за цей напрям, отримують унікальний досвід протидії новим загрозам, який є цікавим для євроатлантичних партнерів. Україна стала для Росії полігоном для випробування нових засобів і способів ведення кібер-війни. Російська кібердіяльність активізується в період президентських і парламентських виборів в Україні. Не виключено, що окремі технології, «обкатані» на українських виборах, будуть застосовані на виборах до Європейського Парламенту. Тож така тристороння співпраця набуває особливої актуальності.

І. Нормативно-правовий та інституційний базис кібербезпеки в ЄС, НАТО й Україні

Європейський Союз не є безпековим альянсом, хоча й має власну Спільну політику безпеки та оборони, адже створювався як економічний союз, а отже безпека для нього має переважно внутрішній і невійськовий вимір, і протидія гібридним загрозам набуває там особливої актуальності. Тому кібербезпека поміщена на одне з перших місць сьогоднішньої безпекової політики ЄС й була виведена в пріоритетні сфери набагато раніше, ніж у термінології ЄС з'явилось визначення «протидія гібридним загрозам», особливо враховуючи активний розвиток цифрового ринку та перспективи створення «Цифрового союзу ЄС».

Ще у 2001 році Європейська Комісія прийняла Комунікацію «Безпека мережі та інформації» (Network and Information Security (NIS): Proposal for A European Policy Approach). Пізніше, в липні 2016 року, ЄС схвалив Директиву з безпеки мереж та інформаційних систем (NIS directive - Directive (EU) 2016/1148). Відповідно до неї, країни-члени ЄС повинні були схвалити відповідні національні закони до 9 травня 2018 року і визначити операторів основних послуг у цій сфері до 9 листопада 2018 року.

Хоча в Європейській стратегії безпеки 2003 року кіберзагрози не увійшли до переліку загроз безпеці ЄС, але у звітах про її імплементацію кібербезпеці приділяється все більше уваги. В якості концептуального документу ЄС у 2006 році була схвалена Стратегія безпечного інформаційного суспільства (Strategy for a Secure Information Society).[1] В подальшому кібербезпека стає невід'ємною складовою безпекових документів Євросоюзу. У 2009 році була схвалена Комунікація «Захист критичної інформаційної інфраструктури» (Communication on Critical Information Infrastructure Protection, CIIP), а у лютому 2013 року - Кібер-стратегія ЄС. Глобальна стратегія із зовнішньої і безпекової політики ЄС, схвалена в червні 2016 року, стала основою для розробки інших секторальних та оперативних документів. У ній кібербезпека виведена в окрему безпекову сферу, яка включає розвиток технологічних можливостей для протидії кіберзагрозам, скорочення кіберзлочинності, посилення стійкості критичної інфраструктури, мереж і сервісів.[2]

Кібер-стратегія ЄС «Відкритий, надійний і безпечний кіберпростір» (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)[3] визначає такі стратегічні пріоритети ЄС: кіберстійкість, зменшення кіберзлочинності, розвиток можливостей і політики кіберзахисту, ін-

1 http://ec.europa.eu/information_society/doc/com2006251.pdf

2 87% європейців вважають кіберзлочинність важливим викликом внутрішній безпеці ЄС, а в 2016 році 80% європейських компаній мали щонайменше по одному випадку кібератак.

3 https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

дустріальних і технологічних ресурсів кібербезпеки, послідовної міжнародної політики з кіберпростору. У вересні 2017 року ЄС доповнив цю Стратегію, схваливши Спільну комунікацію Європейської служби зовнішньої дії і Єврокомісії з розбудови належної кібербезпеки ЄС.[4] Цей документ визначив пакет додаткових заходів, спрямованих, перш за все, на посилення Агентства кібербезпеки ЄС (ENISA), створення загальної для ЄС схеми сертифікації з кібербезпеки, розвиток Плану відповіді на масштабні кібератаки і кризи, посилення досліджень.

Наприкінці 2017 року в ЄС було запущено Постійне Структуроване Співробітництво (Permanent Structured Cooperation on Defence, PESCO), до якого приєдналися 25 із 29 країн-членів Євросоюзу. Одним із напрямків цієї співпраці стала кібербезпека, зокрема, розпочалось створення Груп швидкого реагування на кіберзагрози (Cyber Rapid Response Teams). Позитивним для України рішенням є те, що треті країни можуть запрошуватись до участі в окремих проектах PESCO, включаючи сферу кіберзахисту.

В грудні 2018 року Європейський Парламент, Європейська Рада і Європейська Комісія досягли політичної згоди щодо Акту з кібербезпеки (Cybersecurity Act)[5], який також посилює мандат Європейського Агентства Мережевої та Інформаційної Безпеки (European Network and Information Security Agency (ENISA), встановлює рамки для сертифікації з кібербезпеки, прискорює розвиток онлайн сервісів з кібербезпеки.

Слід окреслити інституційний вимір кібербезпеки ЄС. У 2004 році Європейська Комісія схвалила рішення про створення Агентства ENISA, яке планується перетворити в Агентство кібербезпеки ЄС (EU Cybersecurity Agency) для надавання допомоги країнам-членам ЄС в протидії кібератакам. Відповідну пропозицію 13 вересня 2017 року озвучив Президент Єврокомісії Жан-Клод Юнкер: «*Європа все ще не оснащена належним чином, коли мова йде про кібератаки. Ось чому сьогодні Комісія пропонує нові інструменти, включаючи Європейське агентство кібербезпеки, щоб допомогти нашому захисту проти таких атак*».[6] Агентство має проводити щорічні пан-європейські навчання з кібербезпеки та обмін розвідувальною інформацією щодо кіберзагроз шляхом створення Центрів обміну інформацією та аналізу (Information Sharing and Analyses Centres). Ще однією важливою функцією Агентства визначено сертифікацію програмних продуктів на відповідність вимогам кібербезпеки в ЄС.

Одночасно, Єврокомісія запропонувала створити Фонд реагування на надзвичайні ситуації з кібербезпеки (Cybersecurity Emergency Response Fund), до яко-

4 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN
5 https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en
6 http://europa.eu/rapid/press-release_IP-17-3193_en.htm

го можуть приєднатися країни-члени ЄС за бажанням. Однак, започаткований наприкінці 2017 року в рамках безпекової ініціативи PESCO Європейський оборонний фонд (European Defence Fund), який серед іншого акумулював фінансові засоби й для проектів з кібероборони, фактично відсунув на другий план потребу створення окремого кібер-фонду ЄС.

У 2012 році в ЄС була створена Група з питань реагування на інциденти в галузі комп'ютерної безпеки (Computer Emergency Response Team, CERT-EU), відповідальна за безпеку інформаційних систем інституцій ЄС. Директивою 2016/1148/ЄС була створена Група співробітництва NIS, на яку покладені функції забезпечення стратегічного співробітництва та обміну інформацією між країнами-членами з питань кібербезпеки. Група здійснює безпосередню координацію мережі Груп реагування на інциденти комп'ютерної безпеки (Network of Computer Security Incident Response Teams).

У вересні 2018 року Єврокомісія схвалила рішення про створення мережі центрів компетентності в країнах-членах за координації Європейського центру досліджень і компетентності з кібербезпеки, яка сприятиме розвитку знарядь і технологій для протидії кіберзагрозам. З метою більшого залучення приватного сектору до протидії кіберзагрозам, в ЄС була створена Європейська платформа публічно-приватного партнерства стійкості (European Public-Private Partnership for Resilience). В рамках агентства Європол діє Європейський Центр протидії кібер-злочинності (European Cybercrime Centre, EC3).

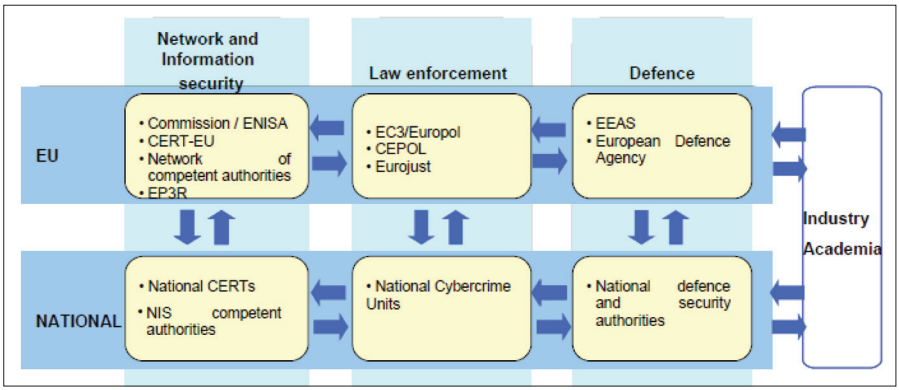


Рис.1. Схема інституцій ЄС у сфері кібербезпеки.

Окрім суто специфічних агентств ЄС, за питання кібербезпеки також відповідають вже згаданий Європол, Євроюст (Eurojust), Європейський поліцейський коледж, Європейська служба зовнішньої дії, Європейське оборонне агентство (EDA), які розробляють та координують спільні для країн-членів ЄС заходи.

«*Жодна країна не може протистояти викликам кібербезпеки самостійно. Наші ініціативи посилюють співпрацю так, що країни ЄС можуть подолати ці виклики разом*», - ці слова Віце-Президента з Єдиного цифрового ринку Андруса Ансіпа демонструють, що офіційний Брюссель все більше колективних зусиль спрямовує на протидію кіберзагрозам. [7]

На відміну від ЄС, в **НАТО** протидія кіберзагрозам визначена поняттям «кібероборона»[8], яка входить до переліку головних цілей колективної оборони, що підкреслює його безпеково-оборонну спрямованість, а не внутрішньо-безпекову, як у випадку ЄС. Генеральний секретар НАТО Йенс Столтенберг чітко окреслив три напрямки у цій сфері: «*Сьогодні НАТО відіграє три ключові ролі у кіберпросторі. Просуває прогрес в усьому Альянсі. Відіграє роль хаба для обміну інформацією, тренувань і досліджень. І захищає наші мережі*».[9] Тому НАТО зосереджується на захисті власних мереж і посиленні внутрішньої стійкості країн-членів, що є актуальним і для України.

Вперше кібероборона була поставлена на політичний порядок денний Альянсу на його Празькому саміті у 2002 році. На Уельському саміті 2014 року НАТО схвалив посилену політику з кібероборони і відповідний план дій з її імплементації. Ця політика визначила діяльність Альянсу за напрямками поінформованості, навчання, тренувань і навчань. Тоді ж протидія кіберзагрозам була введена під дію Статті 5 Північно-Атлантичного Договору[10], що є дуже важливим рішенням, адже кібератака на одну країну викликає відповідь усього НАТО. На Варшавському саміті 2016 року Альянс вже зосередив увагу на посиленні кібероборони національних мереж та промисловості. Тоді ж був підтверджений мандат НАТО на проведення операцій у кіберпросторі, який прирівняли до інших сфер проведення операцій – суші, повітря і моря. На Брюссельському саміті НАТО 2018 року кібератаки віднесені до головних гібридних загроз.[11] НАТО погодило необхідність доведення операцій з кібероборони до рівня операцій в інших трьох сферах як за загальної координації Альянсу, так і в межах окремих груп союзників.

Загальну імплементацію Політики з кібероборони НАТО здійснює Північно-Атлантична Рада. Їй підпорядковується Комітет кібероборони, який здійснює загальне управління політикою кібероборони. На робочому рівні Рада управління з кібероборони (NATO Cyber Defence Management Board, CDMB) відповідає за координацію дій у сфері кібероборони між різними інституціями НАТО та країнами-членами. Цей орган включає вищих посадових осіб з політичних,

7 http://europa.eu/rapid/press-release_IP-17-3193_en.htm
8 https://www.nato.int/cps/en/natohq/topics_78170.htm
9 https://www.nato.int/cps/en/natohq/opinions_154462.htm
10 https://www.nato.int/cps/en/natohq/opinions_145415.htm?selectedLocale=en
11 https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=uk

військових, оперативних і технічних органів Альянсу, які відповідають за кібероборону. В НАТО також діють Рада консультацій, контролю й управління (NATO Consultation, Control and Command (NC3) Board) та інші органи, які відповідають за ті чи інші питання кібероборони.

Операційними органами Альянсу у сфері кібербезпеки є:

- Центр операцій у кіберпросторі (Cyberspace Operations Centre), створений рішенням Брюссельського 2018 року саміту НАТО;

- Центр можливостей з реагування на комп'ютерні інциденти (NATO Computer Incident Response Capability, NCIRC) – виконує завдання із захисту мереж НАТО та надає централізовану цілодобову підтримку комп'ютерним ресурсам Альянсу;

- Групи швидкого реагування у кіберсфері (NATO Cyber Rapid Reaction teams) - перебувають у постійній готовності надати допомогу союзникам.

Важливу роль відіграють Центр передового досвіду із кібероборони (NATO Cooperative Cyber Defence Centre of Excellence, CCD CoE), створений у 2008 році й розташований в Таллінні в Естонії, який здійснює дослідження, проводить навчання і тренування у сфері кібербезпеки, а також Школа НАТО з комунікацій та інформаційних систем (NATO Communications and Information Systems School, NCISS), Школа НАТО в Обераммергау в Німеччині (NATO School in Oberammergau) та Оборонний коледж НАТО в Італії, які виконують функцію підготовки спеціалістів з кібероборони.

Поняття «кібербезпека» примушує Альянс постійно розширювати напрямки і засоби протидії кіберзагрозам, на що вказують рішення НАТО та його органи, залучені до цієї протидії. Зокрема, він все більш тісно взаємодіє з промисловістю та приватним сектором. Для цього розроблена і реалізується програма Кібер-партнерство НАТО з індустрією (NATO Industry Cyber Partnership). Водночас, НАТО розвиває тісну співпрацю з ЄС та країнами-партнерами, включаючи Україну, допомагаючи їм досягати двох зазначених цілей – захисту власних мереж та посилення можливостей з протидії кіберзагрозам.

Україна вибудовує свою кібербезпеку за напрямками захисту комп'ютерних мереж та протидії кіберзлочинності, за зразком ЄС, та зміцнення кібероборони, як в Альянсі. Їх актуальність була підтверджена у 2018 році, коли українські спеціалісти з кібербезпеки змогли заблокувати близько 400 кібератак. Окремі з них, за інформацією СБУ, могли бути за наслідками не менші, ніж вірус Petya-A.[12]

12 https://www.ukrinform.ua/rubric-technology/2638599-v-ukraini-torik-zablokuvali-majze-cotiri-sotni-kiberatak.html

До початку агресії Росії у 2014 році Україна вже мала певну нормативно-правову базу у сфері кібербезпеки. Так Законом України від 7 вересня 2005 року була ратифікована міжнародна Конвенція про кіберзлочинність. З часом Україна стала переглядати та удосконалювати національне законодавство у сфері кібербезпеки. Російська агресія стала прискорювачем цього процесу.

Стратегія національної безпеки України 2015 року містить окремий блок кіберзагроз національній безпеці держави – «Загрози кібербезпеці і безпеці інформаційних ресурсів».[13]

Відповідно до Стратегії, до переліку актуальних загроз, що здійснюються Росією «для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території», віднесено «загрози кібербезпеці і безпеці інформаційних ресурсів:

- уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;

- фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом»[14].

Основні напрями державної політики національної безпеки України передбачають спеціальний розділ «Забезпечення кібербезпеки і безпеки інформаційних ресурсів» Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів визначено:

- розвиток інформаційної інфраструктури держави;

- створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT);

- моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації;

- розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

- забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації;

- реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС;

13 https://zakon.rada.gov.ua/laws/show/287/2015
14 https://zakon.rada.gov.ua/laws/show/287/2015

- створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони;

- розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Керівництво України було послідовним і на початку 2016 року була схвалена Стратегія кібербезпеки України,[15] яка визначила комплекс заходів, пріоритети та напрямки забезпечення кібербезпеки держави. Передбачено створення й оперативну адаптацію державної політики і досягнення сумісності з відповідними стандартами ЄС і НАТО та поглибленої співпраці з ними. У документі проглядаються ті ж підходи, що й у Стратегії кібербезпеки ЄС, зокрема – принципи «відкритості, доступності, стабільності та захищеності кіберпростору». У військовому вимірі кібербезпеки України застосовуються підходи НАТО, зокрема, кіберпростір також визначений сферою проведення операцій.

Схвалений у жовтні 2017 року закон «Про основні засади забезпечення кібербезпеки України»[16] містить термінологію із врахуванням термінології ЄС і НАТО, яка дозволяє чітко розрізнити види й об'єкти діяльності та зафіксувати сфери відповідальності суб'єктів у цій сфері. Наприклад, в законі відображені такі європейські принципи як відкритість, доступність, стабільність і захищеність кіберпростору, а також необхідність взаємодії з приватним сектором і громадянським суспільством у сфері кібербезпеки.

Закон України «Про національну безпеку», введений в дію 21 червня 2018 року, у Статті 19 покладає на Службу безпеки України забезпечення кібербезпеки.[17] Стаття 22 цього ж Закону відзначає особливу роль Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ): «Державна служба спеціального зв'язку та захисту інформації України є державним органом, призначеним для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону». Стаття 31 Закону присвячена Стратегії кібербезпеки України як документу «довгострокового планування, в якому визначаються пріоритети національних інтер-

15 https://zakon.rada.gov.ua/laws/show/96/2016/ed20180509
16 https://zakon.rada.gov.ua/laws/show/2163-19
17 https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2469-VIII

есів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі», пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, а також потреби бюджетного фінансування.

Законом передбачено «Комплексний огляд сектору безпеки і оборони», який проводиться за рішенням Ради національної безпеки і оборони України, що вводиться в дію указом Президента України. Комплексний огляд сектору безпеки і оборони включає проведення, з-поміж інших, «огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури». Кабінет Міністрів України визначає порядок проведення спеціального огляду ДССЗЗІ, стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Воєнною доктриною України, схваленою 24 вересня 2015 року, питання кібероборони фактично обійдені увагою. Згадується лише кіберзахист критичної інфраструктури, як частина компетенції ДССЗЗІ: «забезпечення функціонування урядового зв'язку Верховного Головнокомандувача Збройних Сил України з посадовими особами Збройних Сил України, інших військових формувань, правоохоронних органів спеціального призначення під час їх перебування у пунктах управління, забезпечення кіберзахисту об'єктів критичної інфраструктури».[18]

Згідно із згаданими документами, основу національної системи кібербезпеки складають СБУ, ДССЗЗІ, Міністерство оборони та Генеральний штаб ЗС України, Національна поліція, Національний банк України, розвідувальні органи. Вищим координаційним органом є Національний координаційний центр кібербезпеки як робочий орган РНБО України. Основним завданням Центру є вироблення пропозицій з посилення спроможностей України у боротьбі із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом, кіберзлочинністю та у забезпеченні кіберзахисту інформаційних ресурсів і критичної інфраструктури.

Ще задовго до схвалення Стратегії кібербезпеки в Україні, у 2007 році була створена Команда реагування на комп'ютерні надзвичайні події України (Computer Emergency Response Team of Ukraine, CERT-UA), яка є спеціалізованим структурним підрозділом ДССЗЗІ. Вона виконує роль технічного координатора державних органів, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань запобігання, виявлення та усунення наслідків кіберінцидентів.

18 https://zakon.rada.gov.ua/laws/show/555/2015

CERT-UA діє за такими ж принципами, що й CERT-EU. На цю команду також покладені функції оперативної взаємодії з іноземними партнерами та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST. Хоча у цьому Форумі Україна представлена лише однією командою CERT-UA, тоді як від Польщі там 5 команд, від Німеччини - 31 команда, а від США – аж 90 команд.

У Службі безпеки України функціонує Ситуаційний центр забезпечення кібербезпеки, на який покладено завдання з виявлення, запобігання та нейтралізації акцій кібернетичного характеру проти України. У Національній поліції України діє Національний контактний пункт формату 24/7 щодо реагування та обміну інформацією про комп'ютерні злочини.

Україна знаходиться на передовій протидії кіберзагрозам, а її досвід цінується в світі. Так, на зустрічі щодо ситуації на Близькому Сході 21 лютого 2019 року у Варшаві Міністра закордонних справ України Павла Клімкіна попросили виступити з питань кібербезпеки. "*Наш досвід дуже цінується, оскільки, крім звичайних дискусій і виступів, мене попросили спеціально виступити з питань кібербезпеки та інформаційних війн. Саме наш досвід значною мірою зараз використовується*", - заявив Клімкін перед цим заходом.[19]

Таким чином, Україна адаптувала та продовжує застосовувати європейські і міжнародні стандарти у сфері кібербезпеки, створила і розвиває відповідні органи, які здатні ефективно взаємодіяти з відповідними органами ЄС і НАТО. Однак, через несхвалений до цього часу закон про захист критичної інфраструктури в Україні відсутнє чітке визначення критичної кібер-інфраструктури, що ускладнює роботу державних органів у цій сфері і застосування єдиних стандартів. Між тим, досвід України дозволяє їй бути не тільки реципієнтом допомоги від ЄС і НАТО, але й джерелом нових знань, навичок та способів протидії сучасним кіберзагрозам.

19 https://www.ukrinform.ua/rubric-polytics/2640332-klimkin-govoritime-pro-kiberbezpeku-na-blizkoshidnij-konferencii-u-varsavi.html

ІІ. Співпраця України з ЄС і НАТО з кібербезпеки

Цілі розвитку безпекового **співробітництва ЄС і НАТО** співпадають, і це базується не лише на тому факторі, що 22 країни є одночасно членами і ЄС, і НАТО, але й на бажанні взаємного заповнення поточних прогалин у безпекових можливостях один одного, зокрема у сфері кібербезпеки. Для розвитку такої співпраці, а також взаємодії з іншими акторами, зокрема, Україною, був розроблений Рамковий документ з спільного дипломатичного реагування ЄС на шкідливу кібердіяльність (Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities).

Важливою віхою розвитку співпраці ЄС і НАТО з кібербезпеки стало встановлення Центром передового досвіду НАТО з кібероборони у 2013 році зв'язків з Європейським оборонним агентством для обміну інформацією, проведення спільних навчань і заходів та уникання дублювання досліджень у кіберсфері. Дві структури провели низку спільних навчань, зокрема – вже згадане навчання «Кібер Коаліція» (Cyber Coalition) і навчання «Кібер Європа» (Cyber Europe), які стали платформою для спільних підходів.

Нинішня актуалізація гібридних викликів і загроз, пов'язана з агресією Росії проти України, надає додаткового поштовху поглибленню взаємодії двох організацій. В лютому 2016 року, ще до схвалення Спільної заяви ЄС-НАТО, дві організації підписали Технічну угоду про співпрацю з кібероборони за напрямками обміну інформацією, тренування, досліджень і навчання. В результаті, практична співпраця розвивається між Групою реагування на комп'ютерні надзвичайні ситуації ЄС (CERT-EU) і Центром можливостей з реагування на комп'ютерні інциденти (NCIRC), які й стали підписантами згаданої технічної угоди від імені ЄС і НАТО.

На саміті НАТО 11-12 липня 2018 року у новій штаб-квартирі в Брюсселі розширене співробітництво між ЄС і НАТО відсвяткувало свій другий рік. Співпраця між ЄС і НАТО зросла в усіх сферах, від гібридних загроз та кібербезпеки до морського співробітництва. Кібербезпека постійно присутня в їхніх офіційних документах.

В рамках Розширеної співпраці між ЄС і НАТО із залученням третіх сторін, зокрема, з кібербезпеки, на даний час існують три пілотні країни: Молдова, Туніс та Боснія і Герцеговина. Третій звіт про хід її імплементації, схвалений Радами ЄС та НАТО,[20] визначає, що обмін інформацією, включаючи й між-штабні політичні консультації, також матимуть місце й для України.

20 https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf

Фото 1. Підписання Технічної угоди між ЄС і НАТО 10.02.2016р.
(підписанти – керівник CERT-EU Фредді Дезьор і голова з кібер-безпеки NCIRC Ян Вест)
Джерело - https://www.nato.int/docu/review/2016/also-in-2016/cyber-defense-nato-security-role/en/index.htm

Україна має багато кваліфікованих експертів у кіберсфері. Проте, їм все ще не вистачає міжвідомчої координації та співпраці з міжнародними партнерами. Наприклад, Консультативна місія ЄС в Україні співпрацює з Кіберполіцією України, Службою безпеки України та Національним центром координації кібербезпеки при РНБОУ. Тим часом, належна координація залишається важливою проблемою, оскільки вона не залежить від стратегій чи політик, які вони розробляють. Так само кошти та зусилля донорів залежать від рівня міжвідомчої координації в Україні.

Україна співпрацює з ЄС і НАТО у сфері кібербезпеки поки що сепаратно, хоча в окремих випадках, переважно на рівні практичної допомоги, дві організації здійснюють щонайменше узгодження своїх зусиль, адже ця двостороння допомога має бути скоординована у відповідності до засад співробітництва ЄС-НАТО у сфері кібербезпеки.

В Європейській службі зовнішньої дії вважають, що комплексний характер кіберпростору вимагає спільних зусиль урядів, приватного сектору, експертного середовища, технічної спільноти, користувачів і науковців з протидії сучасним кіберзагрозам. Як повідомив представник Підрозділу координації кіберполітики, попередження конфліктів і політики безпеки Європейської служби зовнішньої дії Елоїз Діволь на міжнародній конференції "Нові формати співпраці НАТО і ЄС з Україною" 30-31 травня 2018 року у Києві,[21] ЄС звертає увагу на необ-

21 https://geostrategy.org.ua/ua/component/k2/item/1473-post-reliz-novi-formati-spivpratsi-nato-i-es-z-ukrayinoyu

хідність адаптації країн-партнерів, включаючи Україну, до правил кібербезпеки ЄС, пріоритетними серед яких є сертифікація програмного забезпечення, процес передачі звітності, впровадження норм відповідальності за дії в кіберпросторі.

На багатосторонньому рівні ЄС керується переважно цілями, визначеними в Спільному робочому документі «Східне Партнерство – 20 очікуваних досягнень до 2020 р.: фокусуючись на головних пріоритетах та реальних результатах», де в розділі «Безпека» три із десяти груп завдань стосуються кібербезпеки, зокрема, щодо створення повноцінних діючих підрозділів боротьби з кіберзлочинністю, розвитку державно-приватного співробітництва та міжнародного співробітництва у сфері кібербезпеки. Ці завдання Україна або вже виконала, або має усі реальні шанси виконати до 2020 року.[22] В Україні схвалена Стратегія кібербезпеки України, імплементується Конвенція про кіберзлочинність і Директива 2008/114/ЄК щодо захисту критичної інфраструктури, створені необхідні інституції, які взаємодіють з ЄС та недержавними інституціями (наприклад, CYS-Centrum і Українськими Кібервійськами).

На двосторонньому рівні Україна-ЄС кібербезпека перебуває у центрі уваги. Так під час п'ятого засідання Ради асоціації 17 грудня 2018 р. в Брюсселі обидві сторони підкреслили необхідність подальшої співпраці у боротьбі з кібер- та гібридними загрозами в інтересах безпеки своїх громадян. У зв'язку з цим Рада асоціації привітала зобов'язання ЄС продовжувати підтримку України в галузі кібербезпеки.[23]

У 2017-2018 роках ЄС здійснив низку заходів в рамках інструменту технічної допомоги TAIEX в трьох сферах: створення відповідної законодавчої бази в Україні; створення державно-приватного партнерства та просування організаційних аспектів національних структур кібербезпеки; підтримка технічних здібностей та навичок у державних органах, відповідальних за кібербезпеку.

ЄС допомагає Україні завдяки своїй Консультативній місії (EU Advisory Mission to Ukraine, EUAM), яка по всій Україні допомагає серед іншого у сфері протидії кіберзагрозам. На різноманітні проекти допомоги Україні у сфері кібербезпеки в КМЄС було виділено більше 2,5 млн євро. Місія сприяє покращенню технічного оснащення українських правоохоронних органів, проводить тренінги, обміни досвідом, дискусійні панелі. До заходів залучаються фахівці Європолу та інших інституцій ЄС.

Кіберсфера є пріоритетною у розвитку співробітництва України з **НАТО**. Зокрема, українські експерти, які взяли участь у міжнародному круглому столі «Україна-НАТО: Невійськова співпраця як спільна відповідь на гібридні загрози»,

22 http://eap-csf.org.ua/wp-content/uploads/2017/10/Report_Ukrainian.pdf

23 https://eu-ua.org/novyny/spilna-zayava-dlya-presy-za-rezultatamy-5-go-zasidannya-rady-asociaciyi-mizh-ukrayinoyu-ta?fbclid=IwAR3m9I-dcxFVi18jxynTEpsuTk0BiZTBoSCzf-NSmFygQ-cc_6gEJxAM5D1Y

організованому Центром глобалістики «Стратегія XXI» і Представництвом Фонду Конрада Аденауера в Україні 9 лютого 2017 року в м.Київ, поставили кібербезпеку на друге місце серед пріоритетних напрямків спільної Україна-НАТО протидії гібридним загрозам.[24]

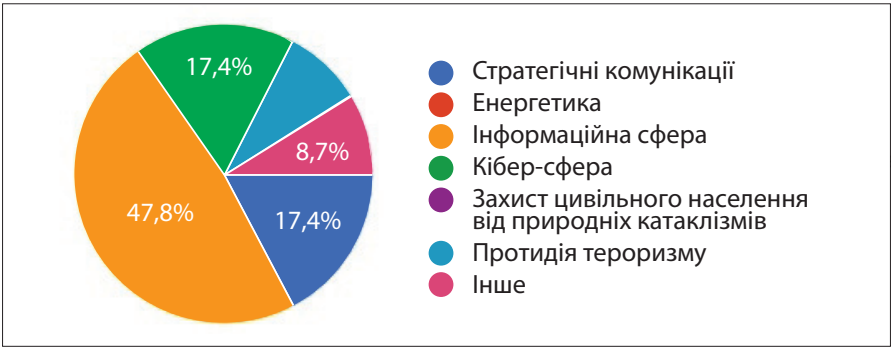


Рис. 2. Ключова сфера спільної Україна-НАТО протидії гібридним загрозам.

Налагоджено кібер-співпрацю між Україною й НАТО, яка щороку прописується в Річних національних програмах під егідою Комісії Україна-НАТО (РНП) в окремому розділі «Кібербезпека».[25] Метою цієї співпраці визначено «удосконалення національної системи кібербезпеки як складової системи забезпечення інформаційної безпеки, її правових концептуальних засад та практичних механізмів протидії агресії РФ у кіберпросторі». Згідно РНП, Україна зміцнює співробітництво державних, у тому числі правоохоронних і спеціальних органів, з приватним ІТ-сектором, що відповідає підходам і ЄС і НАТО у сфері протидії кіберзагрозам.

Співпраці Україна-НАТО сприяє запущений у 2014 році відповідний Трастовий фонд допомоги Альянсу (Trust Fund on Cyber Defence) та Комплексний пакет допомоги НАТО, схвалений 2016 року, де кібербезпека визначена пріоритетним напрямком. Мета очолюваного Румунією Трастового фонду полягає в тому, щоб забезпечити розвиток в Україні власних груп протидії кіберзагрозам та надійних захисних технічних можливостей CSIRT1, включаючи лабораторії для розслідування кіберінцидентів. НАТО надає допомогу Україні із вдосконалення законодавства, розробки стратегії і політик, практичної підтримки у розвитку технічної інфраструктури, підготовки та напрацювання потенціалу кібероборони, що залишатиметься пріоритетом на найближчий час.

У 2014 році розпочато проект із створення ситуаційних центрів реагування на комп'ютерні інциденти для моніторингу подій у сфері кібербезпеки, а також ла-

24 https://www.kas.de/veranstaltungen/detail/-/content/ukraine-nato-nichtmilitaerische-zusammenarbeit-als-gemeinsame-antwort-auf-hybride-bedrohungen
25 https://www.president.gov.ua/documents/892018-23882

бораторій для розслідування інцидентів у кіберпросторі та ліквідації їхніх наслідків. У червні 2017 року українські інституції успішно отримали відповідне обладнання, а в липні 2017 року завершився перший етап Цільового фонду, головними бенефіціарами якого були СБУ та ДССЗЗІ. У січні 2018 року був відкритий Ситуаційний центр забезпечення кібербезпеки СБУ. На цей проект НАТО виділило понад 1 млн. доларів США. Інші українські міністерства, зокрема, МЗС України, також отримують від НАТО обладнання та програмне забезпечення, необхідне для захисту інформаційної інфраструктури.

В рамках підготовки українських фахівців, у 2015 році Естонія, як учасник Трастового фонду, організувала українській стороні п'ять навчальних курсів із реагування на інциденти в галузі кібербезпеки, підготовки на стратегічному рівні (кіберполітика і кіберстратегія) та оперативному рівні кібербезпеки. Розміщений у столиці Естонії Центр передового досвіду НАТО із кібероборони вивчає ситуацію в Україні та співпрацює з українськими акторами, відповідальними за цю проблематику.

Україна є однією з країн-партнерів, які беруть участь у навчальній програмі з кібербезпеки Програми НАТО «Удосконалення військової освіти» (Defence Education Enhancement Programme, DEEP). Так, у вересні 2018 року такий курс був проведений на базі Житомирського військового інституту імені Сергія Корольова, під час якого були відпрацьовані оборонні і наступальні кібер-операції на підтримку військовій місії.[26]

Щороку українські військові фахівці у сфері кібероборони беруть участь в масштабному багатонаціональному навчанні НАТО «CWIX" (Coalition Warrior Interoperability Exercise), які проводяться у тренувальному центрі в Бидгощі в Польщі. У 2019 році ці навчання тривалістю три тижні заплановані на травень-липень.

В подальшому у сфері кібербезпеки НАТО приділятиме увагу розбудові можливостей України, наданні необхідного обладнання і підготовці персоналу, в результаті чого Україна повинна набути здатності захищати свою інфраструктуру від кібератак. Одночасно, важливим напрямком залишатиметься протидія і припинення діяльності осіб, які проживають на території країн-членів НАТО і ЄС та надають різного роду підтримку терористичній й екстремістській діяльності, зокрема, діяльності т.зв. «ДНР» і «ЛНР», та громадян Росії й інших країн, які причетні до агресії проти України.

У майбутньому розвитку співпраці між ЄС і НАТО у сфері кібербезпеки Україна може бути в центрі уваги, якщо українське керівництво буде підтримувати темпи реформ та покращить рівень міжвідомчої координації.

26 https://www.nato.int/cps/en/natohq/news_159840.htm?selectedLocale=en

III. Нові виклики і кіберзагрози

Російська активність в кіберпросторі є головним викликом для України у сфері забезпечення кібербезпеки. Росія використовує кіберпростір як простір нових можливостей для здійснення не тільки розвідувальної діяльності проти України, але й проведення спеціальних операцій з прихованого проникнення в кібер-мережі органів державного управління та встановлення дистанційного контролю над об'єктами критичної інфраструктури з метою отримання переваг та забезпечення своїх інтересів у інформаційній, військово-політичній, фінансово-економічній, енергетичній сферах.

Американська компанія «FireEye», що спеціалізується на проблематиці міжнародної кібербезпеки, ідентифікувала групу хакерів з числа низки груп постійних загроз (Advanced Persistent Threat), яка тривалий час проводила інформаційні операції на замовлення російського уряду. Вона отримала кодову назву APT 28 (відома також як Fancy Bear, Pawnstorm, CyberCaliphate, Cyber Berkut, Tsar Team та ін.), її ідентифікують як кібер-підрозділ ГУ ГШ ЗС РФ. Починаючи з 2007 року, характерною особливістю діяльності APT 28 була спеціалізація у сфері добування інформації з оборонної, військово-політичної та геополітичної тематики. Об'єктами атак були комп'ютерні мережі низки державних установ та організацій країн Центральної і Східної Європи, зокрема, Польщі, Чехії, України, Грузії, а також НАТО та ОБСЄ.

З 2014 року Україна використовується як полігон для тестування російськими спецслужбами та підконтрольними їм групами хакерів нових практик кібератак. Зафіксовано відпрацювання декількох видів атак, спрямованих на інформаційно-психологічний вплив на населення, незаконний збір інформації, паралізацію діяльності центральних органів влади, а також завдання матеріальної шкоди державі та громадянам через виведення з ладу інформаційно-телекомунікаційних систем на об'єктах критичної інфраструктури.

Довідково. *Наявність у Росії серйозного потенціалу для кіберагресії була проявлена в ході відомої атаки на Естонію у 2007 році. Показовим щодо напрямку подальшого нарощування кібер-спроможностей став 2012 рік. 17 жовтня 2012 р. МО РФ спільно з Агентством стратегічних ініціатив, Міністерством освіти і науки РФ та Московським вищим технічним училищем ім. Баумана оголосило всеросійський конкурс науково-дослідних робіт, одна з тем якого – «Методи і засоби обходу антивірусних систем, засобів мережевого захисту, засобів захисту операційних систем».*[27]

27 Российский конкурс научно-исследовательских работ и идей для укрепления обороноспособности страны 13.10.2012. http://inno.nsu.ru/news/2012-10-13.htm

Виходячи з назви теми, російські фахівці оцінили це як відбір проектів та підбір кадрів для розробки бойових наступальних вірусів з метою подолання захисних систем ймовірного противника.[28] На думку російських експертів «подібна постановка питання кардинально розходиться з суто оборонною стратегією в сфері інформаційного протиборства, яка була прописана у Військовій доктрині РФ від 2010 року, а також у зовнішньополітичних російських ініціативах.[29]

Про різкий зсув 2013 року в напрямку підвищення активності в кіберпросторі свідчить указ президента РФ В. Путіна №31с від 15 січня 2013р., яким на ФСБ РФ покладена відповідальність за створення системи кіберзахисту та протидії кібератакам на російську критичну інфраструктуру. Незабаром, 13 лютого, під егідою військового відомства було оголошено про організацію підрозділу інформаційного протиборства в Генштабі ЗС РФ. Лише через 4 роки, 22 лютого 2017 року міністром оборони РФ С. Шойгу на спеціальному засіданні в Державній Думі було визнано створення військ інформаційних операцій. Начальник Генштабу ЗС РФ у 2004-2008 р.р. генерал армії Юрій Балуєвський, коментуючи заяву С. Шойгу, сказав, що перемога в інформаційному протиборстві часто має більше значення, ніж в класичній війні: «*Перемога над противником в цій війні може бути набагато важливіше, ніж перемога в класичному військовому протистоянні, оскільки вона безкровна, а ефект вражаючий - знекровлює і паралізує всі органи влади держави-супротивника*».[30] Не дивлячись на активність російського Міністерства оборони в кіберсфері, ФСБ, ФСО та ФСТЭК мають не менші можливості.

Зізнання С. Шойгу 2017 року є підтвердженням того, що Росія цілеспрямовано готувалась до агресивних дій не тільки на традиційних ТВД, в інформаційно-пропагандистському вимірі, але й у кіберпросторі. Це співпадає у часі з початком агресії гібридного типу проти України, а тепер можна констатувати, що й кібер-проникненням в США, країни ЄС та НАТО, яке почало набувати проявлених форм у 2016 році в ході президентської виборчої кампанії в США. Основні кіберзусилля Росії зосереджені на США. Європа не позбавлена уваги, але, тут основний фронт – інформаційно-пропагандистський. Однак, по мірі проведення виборчих кампаній у низці західноєвропейських країн у 2017-2019 роках, російський кібернаступ на Європу посилюється.

---

28 Минобороны объявило тендер на наступательное кибероружие. Взгляд. 2012, 18 октября. http://vz.ru/news/2012/10/18/603077.html

29 Олег Демидов. «Киберкомандование США: уроки для России». «Индекс безопасности», 2013 г., № 3 (106), Том 193 http://www.perspektivy.info/rus/konturi/kiberkomandovanije_ssha_uroki_dla_rossii_2013-11-15.htm

30 Никита Буранов. Принципиально новые войска. «Expert Online». http://expert.ru/2017/03/1/kibervojna/

Що стосується українського кіберфронту російської гібридної агресії, то у 2014 році група «КіберБеркут» (APT 28) взяла на себе відповідальність за атаки на сайти державних органів і громадських організацій України та низки західних країн. Перші атаки були здійснені в березні 2014 року під час окупації Криму, коли був тимчасово заблокований ряд українських веб-ресурсів і було оголошено про атаку на три інтернет-ресурси НАТО. Значущі акції «КіберБеркуту» в інформаційному і кіберпросторі:

- створення перешкод у роботі ЦВК України напередодні виборів Президента України 23 травня 2014 року;

- блокування роботи сайтів МВС України та Генеральної прокуратури України від 4 квітня 2014 року;

- DDoS-атаки на веб-сайт Кабінету Міністрів України 10 і 14 квітня 2014 року;

- блокування телефонів стільникового зв'язку членів уряду України;

- блокування провідних новинних порталів УНІАН і ЛІГАБізнесІнформ;

- блокування сайту президента України П. Порошенка 29 липня 2014 року.

Таким чином, дані дії синхронізуються в часі з дифузною фазою вторгнення РФ в Україну на Донбасі. Отже, кіберфронт проти України був відкритий одночасно з воєнним компонентом гібридної агресії Росії.

У лютому 2015 року за підтримки російських силових органів була створена ідентична хакерська організація під назвою «СПРУТ» (так звана «Система протидії українському тероризму»). Дана організація проводить атаки на офіційні сайти керівництва обласних державних адміністрацій, Міністерства оборони України, Служби безпеки України, Генерального штабу ЗС України, Головного управління розвідки МО України.

Наприкінці 2015 року для підвищення ефективності інформаційної війни проти України керівництво Генштабу ЗС Російської Федерації створило в складі Центру територіальних військ Південного військового округу РФ Центр інформаційного протиборства (ЦІП) в Новочеркаську. В Донецьк було доставлено потужний програмно-апаратний комплекс, призначений для проведення розподілених кібератак (DDoS-атаки).

29 грудня 2016 року, вперше офіційно і публічно, у спільній заяві американських Міністерства внутрішньої безпеки, Офісу Національної розвідки та Федерального бюро розслідувань Росія була звинувачена в хакерських атаках на США.[31] Дії РФ відображені в Спільній аналітичній доповіді Департаменту внутрішньої безпеки та ФБР. Відзначено, що протягом десяти років росій-

31 «Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity». https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity

ські розвідувальні служби проводити кібер-операції проти урядових структур США, важливої інфраструктури, аналітичних центрів, університетів, політичних організацій і корпорацій.

Таким чином, США та Європі знадобилось майже десятиліття, щоб дійти офіційного висновку про недружні дії Росії в кіберпросторі щодо Заходу. Така млявість та повільність тільки грає на руку російському сценарію кібернетичного Перл-Харбору. Росія працює над тим, щоб в «Час «Ч» створити стан дезінформації, хаосу та дезорганізації системи державного управління, в ідеалі – управління стратегічними ядерними силами США, та отримати вікно можливостей для ядерного шантажу Заходу.

У 2013-2017 роках кібератаки проти України здійснювалися з використанням APT-атак (Snake, Uroboros, Sofacy/APT28, Epic Turla, Black Energy 2 і 3, Armageddon та інші), характерних саме для України[32]. У червні 2017 року Україна зазнала масштабної атаки комп'ютерного вірусу Petya-A. Вірус-шифрувальник проник до низки мереж українських державних і приватних установ, зокрема, сайту Кабміну і ряду міністерств, Пенсійного фонду, КМДА, низки банків, крупних державних і приватних підприємств.[33] Кіберполіції України вдалося зупинити наступну хвилю кібератаки та встановити, що їй передував збір даних про підприємства України. На думку фахівців, саме ця інформація і була справжньою ціллю цієї кібератаки для подальшого ведення кіберрозвідки й акцій підривного характеру.[34] Завдяки попереджувальним заходам уже в жовтні 2017 року українським правоохоронцям вдалося уникнути збитків та масового поширення кібератак на окремі об'єкти, зокрема, Одеський аеропорт, Київський метрополітен, Мінінфраструктури.[35]

Іншою загрозою в контексті російської агресії, є робота найнятих китайських кібер-груп на користь РФ. Окремі українські експерти зробили висновок про те, що російські кібер-групи здійснюють свої операції з використанням технічних можливостей китайських хакерських організацій.[36] Це стало можливим після міжнародно-правової легалізації спільної російсько-китайської діяльнос-

32 Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2016 році». – К. : НІСД, 2016. – 688 с.

33 СБУ встановила причетність спецслужб РФ до атаки вірусу Petya-A, 01.07.2017. https://www.ukrinform.ua/rubric-technology/2257453-sbu-vstanovila-pricetnist-specsluzb-rf-do-ataki-virusu-petyaa.html

34 СБУ попереджає про можливу кібератаку на установи та підприємства, 18.08.2017. https://www.ukrinform.ua/rubric-society/2288607-sbu-poperedzae-pro-mozlivu-kiberataku-na-merezi-ukrainskih-ustanov-ta-pidpriemstv.html

35 Міністр інфраструктури прокоментував наслідки кібератаки, 25.10.2017. https://www.ukrinform.ua/rubric-technology/2331042-ministr-infrastrukturi-prokomentuvav-naslidki-kiberataki.html

36 Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. Р.В. Лук'янчук. Вісник НАДУ. 04.2015. http://visnyk.academy.gov.ua/wp-content/uploads/2016/01/2015_4_8_ukr.pdf

ті у кіберпросторі. Між РФ та КНР у 2015 році на міжурядовому рівні було підписано угоду «Про співробітництво у сфері забезпечення міжнародної інформаційної безпеки». Вказана угода є правовою платформою для співпраці російських та китайських кібер-груп, що підтримуються на державному рівні в обох країнах і є підрозділами відповідних розвідувальних організацій обох країн. Таким чином, залучаючи китайський аутсорсинг, РФ здатна концентрувати потужні кібер-ресурси для ведення кібернетичних війн.

Занепокоєння викликає і факт насичення українського ринку засобами мобільного зв'язку китайського виробництва з відповідним програмним забезпеченням. На тлі резонансних розслідувань у Європі та США щодо прихованих можливостей китайських продуктів для збору інформації, для України важливою є співпраця з НАТО та ЄС із запобігання можливим негативним наслідкам їх масового використання та недопущення появи подібного обладнання і програмного забезпечення в системі державного та воєнного управління.

Аналіз російських джерел вказує на те, що на концептуальному рівні кіберзброя визначається більш розширено, аніж це загально прийнято на Заході. Тобто, не як певний програмний продукт для втручання в роботу комп'ютерів та мереж, а як комплекс дистанційних прихованих впливів на машинну чи людино-машинну систему, що призводить до втрати її функціональності або ж приховане перепрограмування її функцій, яке не дозволяє виконати цільове завдання.[37] Приклади: відмова бортової комп'ютерної системи керування вогнем бойового корабля, невлучання в ціль ракети або її раптова самоліквідація на підльоті до цілі, спуфінг системи GPS, що призводить до критичних відхилень при визначенні координат цілей при веденні вогню тощо. Якісно інший ефект може дати комплексне застосування засобів радіоелектронної розвідки, радіоелектронної боротьби та кіберзброї.

В Росії напрацьовані зразки кіберзброї для нейтралізації критичної інфраструктури противника з метою підвищення ефективності послідуючого першого удару або ж максимального послаблення його спроможностей чинити опір. Характерним є те, що дія такого роду кіберзброї прирівнюється до обезброюючого ядерного удару. Причому, подібна кіберзброя не може мати ніякого потенціалу стримування.

Начальник Генерального штабу ЗС РФ Валерій Герасимов у своєму виступі на щорічних зборах Академії військових наук 2 березня 2019 року вказав на істотне зростання значущості інформаційної сфери протиборства: «*При цьому інформаційні технології становлять, по суті, одним з найбільш перспективних видів зброї. Інформаційна сфера, не маючи чітко окреслених національних*

37 Проблемы классификации кибер-оружия. В.В. Каберник. Вестник МГИМО. №2, 2013. https://cyberleninka.ru/article/v/problemy-klassifikatsii-kiberoruzhiya

кордонів, забезпечує можливості дистанційного, прихованого впливу на критичну важливу інформаційну інфраструктуру, а також на населення країни, безпосередньо впливаючи на стан національної безпеки держави. Саме тому опрацювання питань підготовки та ведення дій інформаційного характеру є важливим завданням військової науки. Цифрові технології, роботи, безпілотні системи, РЕБ – все це повинно бути в порядку денному розвитку воєнної науки, в том числі, воєнної стратегії».[38] Як бачимо, акцент зроблено на комплексне застосування новітніх засобів ведення сучасної війни гібридного типу, але з націленістю на критично важливу інформаційну інфраструктуру. Очевидно, що за задумом ГШ ЗС РФ це має привести до дисфункції або як мінімум паралічу системи державного та воєнного управління противника з подальшою його хаотизацією.

На президентських та парламентських 2019 року виборах в Україні, а також під час виборів до Європейського Парламенту, РФ випробуватиме оновлені технології втручання у виборчий процес. Їх особливість у тому, щоб максимально прибрати демаскуючі ознаки втручання, за якими українські та західні кібер-фахівці ідентифікують російського актора. Найбільш імовірно, що з цією метою відповідні «гнізда» та мережі були створенні на території України та країн-членів ЄС. У свою чергу, українські та європейські вибори мають стати черговим етапом кібер-удосконалення з прицілом на президентські вибори у США 2020 року.

38 Начальник Генерального штаба Вооружённых Сил РФ генерал армии Валерий Герасимов выступил на общем собрании Академии военных наук. 04.03.2019. http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1

IV. Посилення взаємодії України з ЄС і НАТО з протидії кіберзагрозам

В рамках подальшого розвитку співробітництва України з НАТО та ЄС варто, перш за все, враховувати поточні тенденції співпраці між ЄС і НАТО. Подальше співробітництво ЄС-НАТО-Україна у сфері кібербезпеки доцільно зосередити на наступних напрямках:

- завершити створення чіткої робочої системи координації у сфері кібербезпеки для повної імплементації Стратегії кібербезпеки України щоб залучити усіх національних акторів, включаючи неурядові організації, і зробити допомогу НАТО, ЄС та інших організацій більш адресною та ефективною;
- використати досвід та практики ЄС і НАТО для створення широкої національної схеми сертифікації з кібербезпеки, розробки плану, як відповідати на широкомасштабні інциденти і кризи, поглиблювати державно-приватне партнерство і посилювати дослідження;
- ініціювати приєднання України до Центру передового досвіду НАТО з кібероборони, що допоможе Україні імплементувати кращі практики і поглибити співпрацю з Альянсом у цій сфері;
- нарощувати оборонний технічний потенціал України у сфері кібербезпеки за сприяння Трастового фонду НАТО з кібербезпеки та у співпраці з Румунією;
- розвинути співробітництво з посилення кібербезпеки в Україні для попередження і нейтралізації можливого російського втручання під час виборчих кампаній в Україні;
- продовжувати діяльність з визначення критичної інфраструктури та її ключових операційних вразливостей;
- опрацювати загальнонаціональний План реагування на надзвичайні ситуації в кіберпросторі;
- розробити механізм розподілення ризиків через використання захищених хмарних сервісів задля мінімізації можливих втрат у разі кібернападу на інформаційні бази органів державної влади;
- залучити кращі західні практики задля посилення міжвідомчого співробітництва та державно-приватного партнерства з виробленням конкретного дієвого механізму його практичного застосування;
- пропонувати з боку НАТО і ЄС та залучити з боку України більше зовнішньої експертної допомоги;
- спільними зусиллями розробити систему мотивації для фахівців, зайнятих у сфері кібербезпеки та кібероборони.

Паралельно із посиленням захисту українського кіберпростору за сприяння Альянсу, важливим напрямком співпраці Україна-НАТО є протидія і припинення діяльності осіб, які проживають на території країн-членів НАТО та надають різного роду підтримку терористичній й екстремістській діяльності. Також слід покращити рівень співпраці між Україною і країнами НАТО та ЄС з блокування роботи на усіх рівнях, особливо на рівні приватних кампаній (наприклад PayPal), діяльності членів т.зв. «ДНР» і «ЛНР» та громадян Росії й інших країн, які причетні до агресії проти України, особливо тих, які внесені до санкційних списків.

Також важливим напрямком співпраці може стати моніторинг російської та китайської кібер-активності, взаємодії кібер-організацій обох країн. В полі спільної уваги може бути вивчення можливостей Росії використовувати лінії технологічного оптико-волоконного зв'язку безтранзитних газопровідних систем типу «Північний потік», «Північний потік-2», «Турецький потік» та їх продовжень по території країн НАТО та ЄС для вирішення непрофільних завдань, в тому числі, для кібершпигунства.

Заключення

Рішенням Координаційної ради Трастового фонду НАТО у 2017 році подальший напрямок розбудови національної системи кібербезпеки було спрямовано на підвищення технічних можливостей України у сфері кібербезпеки об'єктів критичної інфраструктури шляхом їх оснащення автоматизованими датчиками подій та підключення до національної мережі ситуаційних центрів Держспецзв'язку та СБУ, а також на створення Центрів кібернетичної безпеки у системі Збройних Сил України та Національної поліції з їх подальшим інтегруванням у Національну мережу ситуаційних центрів.[39] Цей напрямок є стратегічно важливим для України з огляду на подальші можливі дії Росії як проти України, так і проти НАТО та ЄС, що є цілком прогнозованим в контексті останніх воєнно-стратегічних новацій Генерального штабу ЗС Росії.

Колишній директор Агентства національної безпеки США і перший директор Кіберкомандування США (USCYBERCOM) Кіт Александер в інтерв'ю ВВС у червні 2018 року заявив: «*Очевидно, що через деякий час Україна, її енергетична і фінансова системи, урядові структури зазнають кібератак. Росія буде намагатися представити Україну територією, де держава існує тільки на папері і не здатна функціонувати*».[40] Після потужних кібернападів на Україну 2015-го, 2016-го та 2017-го років, 2018-й рік був роком відносного затишшя на кіберфронті. Ймовірно, це пояснюється тим, що російські кібер-структури, здійснивши «розвідку боєм» українських інформаційних та комунікаційних мереж, готуються до кібердару, що може бути синхронізований з ескалацією військових дій РФ проти України, коли путінський режим вирішить, що Захід остаточно перевантажився власними проблемами і йому не до України. Затишшя також пояснюється періодом двох виборчих кампаній в Україні, коли пропагандистські та кібер-зусилля з боку РФ зосереджені на хаотизації становища в країні через провокування та розпалювання конфліктів між конкуруючими політичними силами за принципом «війни усіх проти всіх».

Україні, НАТО та ЄС важливо продовжувати співпрацю в кіберсфері. На тлі розширення та поглиблення різнобічної співпраці між Україною та НАТО, Україною та ЄС, зміцнення кіберстійкості України в контексті посилення її загального потенціалу опірності у різних сферах, означатиме закриття ще однієї зони вразливості європейського кіберпростору та появу додаткового щита, що прикриватиме Європу зі Сходу.

---

39 У СБУ відбулася церемонія завершення першого етапу Трастового фонду НАТО зі сприяння Україні в зміцненні кіберзахисту. 04.07.2017. https://www.ssu.gov.ua/ua/news/1/category/2/view/3668#.V3SsDFLC.dpbs

40 Готовьтесь, потому что Россия нанесет кибердар по Украине - эксперт из США. Георгий Эрман. BBC News Украина. 4 июня 2018 https://www.bbc.com/ukrainian/features-russian-44353054

Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері

Підготовлено за результатами досліджень Центру глобалістики «Стратегія XXI» щодо протидії гібридній агресії Російської Федерації та посилення співпраці України з ЄС і НАТО.

За фінансової підтримки Представництва Фонду Конрада Аденауера в Україні.

Окремі думки, висловлені в аналітичному документі, є позицією експертів Центру глобалістики «Стратегія XXI» і не обов'язково відображають точку зору Фонду Конрада Аденауера.

Київ
2019

Співробітництво Україна – ЄС – НАТО
з протидії гібридним загрозам у кіберсфері