Аналітична записка
з питань порівняльного законодавства щодо нормативного забезпечення, особливостей створення та інституційного становлення кібервійськ (кіберсил) країн-членів НАТО*

Анотація. В аналітичній записці досліджено питання нормативного забезпечення, особливостей створення та інституційного становлення кібервійськ (кіберсил). Проаналізовано глобальні ризики та передумови інституційної розбудови кібервійськ, нормативне-правове регулювання створення та функціонування підрозділів кібервійськ, їх завдання та повноваження; з'ясовано типові характеристики кібервійськ (кіберсил), а саме – стратегічні засади їх створення, штатну чисельність підрозділів, структуру органів військового управління та командування. Опрацьовано відповідні стратегічні та концептуальні документи Організації Північноатлантичного договору (НАТО), а також положення національного законодавства таких країн-членів НАТО, як: США, Велика Британія, Франція, Польща.

І. Вступна частина

На сьогодні в більшості країн світу існує стійка тенденція до значного збільшення кількості та розширення спектру кібератак, спрямованих на порушення конфіденційності, цілісності й доступності державних інформаційних ресурсів, зокрема і тих, що забезпечують функціонування об'єктів критичної інфраструктури.

Кібербезпека у країнах НАТО визнана важливою складовою національної безпеки, забезпечення якої здійснюється на підставі єдиної загальнодержавної скоординованої політики в цій сфері, що ґрунтується на засадах поваги до норм і принципів міжнародного права, забезпечення національних пріоритетних інтересів у кіберпросторі, ефективної протидії у кібердомені.

Загальною усталеною практикою цих країн стає чітке доктринальне визначення концептуальних засад державної політики у сфері забезпечення безпеки в кіберпросторі у відповідних документах стратегічного планування.

Україна вже понад рік після початку повномасштабної війни стикається з потужними викликами у сфері кібербезпеки. Хакери, які пов'язані з державою-агресором, на перманентній основі здійснюють цілеспрямовані кібератаки проти України, а також щодо установ та організацій інших країн, які надають допомогу нашій державі. Тільки за 2022 рік українські організації та установи пережили понад 2 тис. кібератак. Понад 300 із них були спрямовані на сектор безпеки і оборони, більш ніж 400 – на цивільні об`єкти, включно з комерційними, енергетичними, фінансовими і телекомунікаційними компаніями, ще понад 500 атак зазнали різні урядові установи[1].

Враховуючи необхідність і доцільність мілітаризації кіберпростору, у країнах НАТО та в багатьох інших країнах світу створено й функціонують спеціальні підрозділи – кібервійська, які використовуються як для військових, так і для розвідувальних цілей. 26 країн світу офіційно мають власні кіберсили або

[1] У 2022 році кількість зареєстрованих кіберінцидентів виросла майже втричі – звіт Держспецзв'язку. URL: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit

перебувають у процесі їх створення (зокрема, США, Австрія, Бельгія, Болгарія, Велика Британія, Німеччина, Франція, Іспанія, Ізраїль, Іран, Китай, Російська Федерація, Нідерланди, Південна Корея, Північна Корея, Канада, Польща, Естонія, Італія, Швеція, Японія, Перу, Бразилія, В'єтнам, Південна Корея, Нігерія)[2].

ІІ. Основна частина

Загальні положення

Термін «кібервійна» визначається, насамперед, як чітко скоординований та спланований оцифрований напад однієї держави або декількох держав, спрямований на проникнення в комп'ютери та інформаційно-комунікаційні мережі іншої держави (держав) з метою завдання суттєвої шкоди або руйнування, виведення з ладу операційних систем та інформаційних і комунікаційних мереж[3]. Кібервійна означає конфлікт, який передбачає використання ворожих, незаконних атак на комп'ютерні мережі з метою руйнування комунікацій та інших елементів інфраструктури як механізму завдання економічної шкоди або підриву системи оборони країни[4]. У Доктрині кібероперацій Повітряних Сил США[5] кібервійна розглядається як збройний конфлікт, в якому повністю або частково використовуються кіберзасоби, військові операції, що проводяться з метою перешкодити супротивникові ефективно використовувати власні кибersистеми та кіберзброю в конфлікті.

Кібервійні властиві окремі визначальні, фундаментальні ознаки, характерні й для класичної війни. Зокрема, масштабне вторгнення на «територію» противника (електронні системи й мережі об'єкта впливу); наявність певного стратегічного плану; використання насильницьких засобів у вигляді шпигунського або шкідливого програмного забезпечення; спричинення значної шкоди цим системам тощо. Водночас кібервійна має низку *специфічних рис,* що суттєво змінюють зміст «класичної» війни:

- *неможливо ідентифікувати «агресора»,* навіть коли причетність до кібератаки державних структур певних країн багатьом здається очевидною. Як правило, географічним джерелом кібератаки є територія іншої «незацікавленої» держави;
- *невидимість впливу.* Ця особливість пов'язана, з одного боку, з основним принципом кібервійни – експлуатацією вразливостей інформаційної інфраструктури супротивника, а з іншого – із непомітністю дій шкідливих програм, які зазвичай не призводять до людських жертв. Як наслідок, надзвичайно складно виявити початок кібератаки (тобто момент вторгнення), застосувати превентивні заходи для попередження таких атак, а також адекватно оцінити рівень загрози і масштаб завданих збитків;

---

[2] Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони: підручник. [Видання друге, перероб. та доп.]. Одеса: ОНАЗ ім. О.С. Попова, 2019. 320 с. URL: https://metod.suitt.edu.ua/download/686

3 Cyber Warfare. URL: https://www.imperva.com/learn/application-security/cyber-warfare

[4] Камчатний М. Заборонені засоби ведення кібервійни. *Підприємництво, господарство і право*. 2017. № 9. С. 211-217. URL: http://pgp-journal.kiev.ua/archive/2017/9/44.pdf

[5] Cyberspace Operations – Air Force Doctrine. URL: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf

– *надзвичайна швидкість проведення кібератак*, коли проміжок часу між початком «агресії» та її наслідками скорочується до мінімуму. До того ж, шкідливі програми мають здатність швидко «розмножуватися» і практично безперешкодно поширюватись у різних напрямах.

У кібервійні домінантним є *наступальний аспект*, оскільки атаку можна реалізувати швидше, легше та дешевше, аніж встановити захист.

Під час кібервійни є зброя, але немає Збройних сил у класичному розумінні. Для кіберзброї *не мають значення державні кордони і відстань*, а також відсутні технологічні, юридичні та інші перешкоди для проникнення в комп'ютерні системи й мережі супротивника та віддаленого управління його ресурсами. Як наслідок, кібератаки важко піддаються контролю з боку державних систем розвідки та безпеки.

На відміну від звичайної зброї, кіберзброя необов'язково знищує об'єкт впливу, а скоріше впроваджує певний набір даних і команд, що *змінюють існуючі алгоритми функціонування системи й активізують потрібні реакції* (від виконання бажаних дій чи невиконання певних функцій аж до самознищення).

Характерними рисами кіберзброї також є:

- *маскування* під конкретні інформаційні системи й мережі;
- *варіативність*, тобто шкідливі програми можуть існувати в різних варіантах і виконувати різні функції або дії залежно від версії;
- *одноразовість використання*. Вторинне використання тієї ж самої програми не буде ефективним, оскільки супротивник може виявити і прибрати або удосконалити вразливості, на які вона була розрахована;
- *націленість на системи і комплекси, що діють за чітко визначеними законами й алгоритмами* тощо.

Важливою особливістю кібервійни є також її *певна незавершеність* або *нескінченність*, оскільки жоден із учасників протистояння не може бути впевненим, що противник припинив атаки. Крім того, кібервійна може проводитись як у мирний час, так і в період звичайної війни. Відносини між країнами, у тому числі офіційні дипломатичні відносини, можуть не піддаватися кардинальним змінам.

Організація Північноатлантичного договору (НАТО) у 2016 році визнала кіберпростір одним із можливих театрів воєнних дій, нарівні з повітрям, сушею та морем. Як наслідок, у НАТО на даний час триває процес створення загальних для всього Альянсу кібервійськ (кіберсил). До їх завдань належить не лише забезпечення кібероборони, захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних та комунікаційних систем, які управляють такими об'єктами, реалізація доктрини когнітивного ефекту, тобто використання методів, які потенційно можуть посіяти недовіру, знизити моральний дух і послабити здатність противника ефективно планувати та проводити свою діяльність у кіберпросторі.

Таким чином, кібероборона (Cyber Defense) є частиною головного завдання НАТО щодо стримування й оборони. У грудні 2016 року НАТО та Європейський Союз узгодили понад 40 заходів, спрямованих на покращення способів спільної

роботи двох структур, зокрема щодо протидії гібридним загрозам, кіберзахисту та підвищення стабільності й безпеки їх спільного сусідства. У лютому 2017 року міністри оборони Альянсу схвалили оновлений План дій щодо кіберзахисту, а також Дорожню карту впровадження кіберпростору як сфери операцій. Це мало збільшити здатність членів Альянсу спільно діяти в цьому напрямі, розвивати можливості та обмінюватися інформацією в режимі реального часу.

На саміті НАТО 2018 року в Брюсселі лідери Альянсу погодилися створити новий Оперативний центр у кіберпросторі як частину командної структури НАТО. Центр забезпечує ситуаційну обізнаність і координує оперативну діяльність НАТО у кіберпросторі. Члени Альянсу узгодили, що НАТО може використовувати національний кіберпотенціал окремих країн-членів для спільних операцій та місій.

У лютому 2019 року міністри оборони країн НАТО схвалили керівні рекомендації НАТО, які містять низку інструментів для подальшого зміцнення здатності НАТО реагувати на значні зловмисні дії у кіберпространстві. Так, зокрема, НАТО має використовувати всі наявні в його розпорядженні інструменти, у тому числі політичні, дипломатичні та військові, щоб протистояти кіберзагрозам, з якими воно стикається. Варіанти реагування, викладені у згаданих рекомендаціях НАТО, допомагають країнам Альянсу та їх союзникам покращити обізнаність про те, що відбувається в кіберпросторі, підвищити стійкість і співпрацювати з партнерами для стримування, захисту та протидії повному спектру кіберзагроз.

На саміті НАТО 2021 року в Брюсселі члени Альянсу схвалили Всеосяжну політику кіберзахисту для підтримки трьох основних завдань НАТО, а також її загальної позиції стримування та оборони. Було заявлено, що НАТО має активно стримувати, захищатися та протидіяти повному спектру кіберзагроз у будь-який час – у мирний час, у кризи та конфлікти – на політичному, військовому та технічному рівнях. Члени Альянсу визнали, що вплив значної зловмисної сукупної кіберактивності за певних обставин може розглядатися як збройний напад. Члени Альянсу також погодилися ширше використовувати НАТО як платформу для політичних консультацій між членами Альянсу, поділяючи занепокоєння щодо зловмисної кіберактивності та обмінюючись національними підходами та відповідями, а також розглядаючи можливі колективні відповіді. У вересні 2021 року Північноатлантична рада призначила першого головного інформаційного директора НАТО (CIO) для сприяння інтеграції, узгодженню та згуртованості систем інформаційно-комунікаційних технологій (ІКТ) в масштабах НАТО.

На саміті НАТО у Вільнюсі 2023 року члени Альянсу схвалили нову концепцію посилення внеску кіберзахисту в загальну систему стримування та оборони НАТО. Концепція додатково інтегрує три рівні кіберзахисту НАТО – політичний, військовий і технічний, забезпечуючи цивільно-військову співпрацю в будь-який час – у мирний час, кризи та конфлікти, – а також взаємодію з приватним сектором, якщо це необхідно. Зміцнення кіберстійкості має ключове значення для того, щоб зробити Альянс більш безпечним і здатним пом’якшувати потенціал значної шкоди від кіберзагроз. При цьому НАТО та його союзники покладаються в реалізації цих завдань на потужну та стійку систему кіберзахисту

для виконання *трьох основних завдань Альянсу*: стримування та оборони, запобігання та врегулювання криз, а також спільної безпеки. Найважливішою із трьох основних задекларованих місій НАТО є стримування та оборона. Ключовими оборонними політичними та військовими процесами і функціями, пов'язаними з підтримкою, розвитком і впровадженням стримування, є оборонне планування на теренах НАТО, успішне виконання спільних оборонних завдань НАТО, у тому числі й проведення результативних операцій у кіберпросторі.

Військово-політичне керівництво Альянсу констатує той факт, що потенційні противники, використовуючи кіберпростір, прагнуть погіршити критично важливу інфраструктуру НАТО, втручатися у роботу урядових служб, отримувати розвіддані, викрадати інтелектуальну власність і перешкоджати військовій діяльності. Росія також активізувала свої гібридні дії проти союзників по НАТО та партнерів, зокрема через деструктивну кібердіяльність. Заявлені амбіції та політика Китаю також кидають виклик інтересам, безпеці та цінностям НАТО. Зловмисні гібридні й кібероперації Китаю, а також конфронтаційна риторика і дезінформація спрямовані проти членів Альянсу та завдають шкоди безпеці країн членів НАТО[6].

З метою захисту своїх інформаційно-комунікаційних мереж та операцій від дедалі складніших кіберзагроз, у НАТО сформульовані *основні концептуальні принципи побудови інтегрованої та максимально ефективної системи спільних дій країн-членів Альянсу* при організації роботи із протидії кіберзагрозам. Зокрема:

- кіберзахист є частиною основного завдання НАТО зі стримування та оборони;
- у центрі уваги НАТО у сфері кіберзахисту – захист власних мереж, діяльність у кіберпросторі (зокрема, через операції та місії Альянсу), допомога членам Альянсу у підвищенні їх національної стійкості та забезпечення платформи для політичних консультацій і колективних дій. У липні 2016 року члени Альянсу підтвердили оборонний мандат НАТО та визнали кіберпростір зоною операцій;
- НАТО є платформою для політичних консультацій членів Альянсу, обміну занепокоєнням щодо зловмисної кіберактивності, обміну національними підходами та відповідями, а також розгляду можливих колективних заходів. Члени Альянсу зобов'язуються покращити обмін інформацією та взаємодопомогу в запобіганні, пом'якшенні наслідків, відновленні та реагуванні на кібератаки;
- члени Альянсу сприяють вільному, відкритому, мирному та безпечному кіберпростору й докладають зусиль для підвищення стабільності та зменшення ризику конфлікту, підтримуючи міжнародне право та добровільні норми відповідальної поведінки держав у кіберпросторі. У 2016 році члени Альянсу погодилися виконати зобов'язання щодо кіберзахисту. У 2023 році члени Альянсу взяли на себе зобов'язання досягти нових цілей щодо зміцнення національного кіберзахисту як пріоритетного питання, включно із критичною інфраструктурою;
- НАТО зміцнює свою кіберспроможність, у тому числі шляхом навчання, тренінгів та спільних тренувань;

[6] NATO's Role in Global Cyber Security. URL: https://www.gmfus.org/news/natos-role-global-cyber-security

- комплексна політика кіберзахисту, проголошена у 2021 році, відображає основні завдання НАТО та загальну позицію стримування та оборони для подальшого підвищення стійкості Альянсу;

- НАТО співпрацює, зокрема, з Європейським Союзом (ЄС), Організацією Об'єднаних Націй (ООН) та Організацією з безпеки та співробітництва в Європі (ОБСЄ) щодо кіберзахисту[7].

На саміті НАТО у Вільнюсі в 2023 році члени Альянсу підтвердили та посилили зобов'язання подальшого зміцнення саме національної системи кіберзахисту кожної країни-члена НАТО як пріоритетного питання, включаючи критичну інфраструктуру. Крім того, схвалено нову концепцію посилення кіберзахисту в загальній позиції стримування та оборони НАТО, а також задіяно можливості НАТО із протидії віртуальним кіберінцидентам (*Virtual Cyber Incident Support Capability (VCISC*). У листопаді 2023 року НАТО заплановано проведення першої загальної конференції НАТО з кіберзахисту в Берліні.

Розвиток можливостей кіберзахисту країн НАТО здійснюється Центром кібербезпеки НАТО (*The NATO Cyber Security Centre (NCSC*)[8], який базується у Верховному штабі Об'єднаних Збройних Сил НАТО в Європі (SHAPE) у Монсі, (Бельгія). Останній захищає власні мережі НАТО, надаючи централізовану та цілодобову підтримку відповідного кіберзахисту, у тому числі допомагає військовим командирам в обізнаності про операції та місії Альянсу. Він також координує оперативну діяльність НАТО в кіберпросторі, забезпечуючи свободу дій у цій сфері та роблячи операції більш стійкими до кіберзагроз.

З метою сприяння спільному підходу до розвитку спроможності кіберзахисту в масштабах Альянсу НАТО визначає цілі щодо реалізації країнами-членами Альянсу національних можливостей кіберзахисту, використовуючи процес оборонного планування НАТО.

НАТО також має та активно використовує низку практичних інструментів для покращення ситуаційної обізнаності та сприяння обміну інформацією, включаючи пункти контакту (бюро) з національними органами кіберзахисту в усіх столицях країн-членів Альянсу. Спеціальний Меморандум про взаєморозуміння (MOU) визначає механізми обміну різноманітною інформацією, пов'язаною з кіберзахистом, та надання допомоги для покращення запобігання кіберінцидентам, стійкості та можливостей реагування на них. Обмін технічною інформацією в рамках Альянсу здійснюється через Платформу обміну інформацією про виявлене зловмисне програмне забезпечення, яке несе загрозу для структур НАТО, що дозволяє швидко обмінюватися індикаторами компрометації між кіберзахисниками Альянсу, забезпечуючи виконання положень загальної оборонної доктрини НАТО.

НАТО планує повністю завершити процедури формування Кіберкомандування до кінця 2023 року. У новому кіберцентрі Альянсу працюватимуть 70 експертів, які оперативно надаватимуть військовій розвідці здобуту інформацію про хакерів, починаючи від ісламістів, і закінчуючи проросійськими організованими злочинними групами, які діють від імені держави.

[7] Кібер захист НАТО «Cyber defence». URL: https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en
[8] Центр кібербезпеки НАТО The NATO Cyber Security Centre *(NCSC*). URL: https://www.ncirc.nato.int/

Питання забезпечення безпеки кіберпростору гостро стоять перед політичним керівництвом України. Починаючи з 2018 року Рада національної безпеки і оборони України (РНБО) опрацьовувала питання щодо створення кібервійськ. Так, Указом Президента України від 26 серпня 2021 року, яким було введено в дію рішення РНБО «Про невідкладні заходи з кібероборони держави»[9], анонсована необхідність створення в системі Міністерства оборони України кібервійськ з метою захисту суверенітету держави, забезпечення її обороноздатності, відсічі збройній агресії у кіберпросторі. План реалізації Стратегії кібербезпеки України, затверджений рішенням РНБО України від 30 грудня 2021 року та введений в дію Указом Президента України від 1 лютого 2022 року[10], чітко регламентує інституційні засади створення в системі Міністерства оборони України кібервійськ (кіберсил) протягом першого півріччя 2023 року. Однак, незважаючи на нормативно встановлені терміни, кібервійська в Україні ще не створено.

З огляду на викладене, вбачається доцільним проаналізувати питання нормативного забезпечення інституційного створення та функціонування кібервійськ на прикладі окремих держав-членів НАТО, а саме: США, Великої Британії, Франції, Польщі.

Сполучені Штати Америки

Кібернетичне командування США (United States Cyber Command) «USCYBERCOM» було створено 23 червня 2009 року відповідно до наказу Міністра оборони США Роберта Гейтса у форматі 11-го військового об'єднаного Командування США. Кібернетичне командування – частина Збройних Сил США, підпорядкована об'єднаному Стратегічному командуванню США (база Повітряних сил США, Оффут, Небраска). При цьому операції в кіберпросторі здійснюються через різні компоненти. До складу USCYBERCOM входять 133 команди Сил Національної Кібермісії (CMF), Штабу об'єднаних сил (JFHQ-DODIN), Сили Національної Кібермісії (CNMF), Об'єднана оперативна група «Ares» та відповідні кіберкомпоненти видів Збройних Сил – Армійського кіберкомандування (ARCYBER), Кіберкомандування Корпусу морської піхоти (MARFORCYBER), Кіберкомандування флоту / Десятий флот (FCC/10F), Кіберкомандування ВПС / 16-та повітряна армія (AFCYBER) і Кіберкомандування берегової охорони (CGCYBER).

Бюджетний запит Міністерства оборони США на 2024 рік для фінансування заходів у кіберпросторі складає $13.5 мільярдів. Станом на 2023 рік загальна штатна чисельність 133 команд Сил Національної Кібермісії складає 9 тис. осіб, із них 15 % – цивільні та резервісти.

Основним завданням Кібернетичного командування є планування та проведення глобальних кібероперацій з метою захисту та просування національних інтересів у співпраці із внутрішніми та міжнародними партнерами в повному спектрі наявної конкуренції та глобальних конфліктів. Державне

[9] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави": Указ Президента України від 26 серпня 2021 року № 446/2021. URL: https://www.president.gov.ua/documents/4462021-40009

[10] Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України": Указ Президента України від 1 лютого 2022 року № 37/2022. URL: https://www.president.gov.ua/documents/372022-41289

фінансування підрозділів Кіберкомандування складає понад 7 млрд доларів США на рік. Комплектування цих підрозділів здійснюється переважно за рахунок хакерів, які поповнюють ряди військових у кіберпросторі. Надійний захист кіберпростору й домінування у світовому масштабі – стратегічне завдання уряду США, що включає і військові дії у кіберпросторі. Політичний вектор, закладений у стратегії національної кібербезпеки США, аргументовано декларує існування системи кіберзагроз, настання яких провокує необхідність проведення спеціальних інформаційних операцій, спрямованих на запобігання цим загрозам та недопущення будь-яких кібератак з боку інших держав. Основними напрямами діяльності кібервійськ є розвідка, у тому числі й промислова, проведення кібератак, спеціальних інформаційних операцій та навіть ведення війни у кіберпросторі. У військових структурах також існує окремий персонал, який залучається для захисту інфраструктури військових кіберсистем. При цьому перемога над противником у цифровій війні розглядається навіть більшим пріоритетом, аніж перемога у класичному військовому протистоянні.

Завданнями Кіберкомандування США є:

1) планування, проведення та координація кібероперацій з метою запобігання зовнішній агресії, забезпечення свободи дій оперативних і сухопутних (берегових, інших) формувань військ (сил) при досягненні переваги у кіберпросторі;

2) забезпечення технічної підтримки, надійності, безпеки та захисту каналів управління, включаючи комп'ютерні та космічні системи в секторі відповідальності;

3) керівництво діяльністю сил і засобів радіоелектронної боротьби, радіоелектронної розвідки та служби дешифрування;

4) проведення спільно з іншими командуваннями кібер-, інформаційних, криптологічних, космічних та інших операцій;

5) приведення глобальної комп'ютерної мережі військ (сил) у відповідність до загальних оперативних потреб кіберзахисту Збройних Сил країни. Вирішення цих питань потребує ретельної комплексної підготовки військ (сил) та високої відповідальності, професійних якостей, навченості особового складу, надійності та ефективності роботи інформаційно-телекомунікаційної складової системи кібербезпеки країни. Для цього в США протягом років створювалася потужна система кібербезпеки держави, яка має спроможності як бойового застосування, так і підготовки та розвитку військ (сил) у мирний час. Система кібербезпеки США складається з різних фахівців – як військових, так і цивільних, які в змозі виконувати складні завдання у сфері забезпечення захисту кіберпростору.

Наприклад, Управління кіберзахисту (оборонних кібероперацій) Військово-морських сил США, яке базується на військово-морській базі Норфолка (штат Віргінія), відповідає за безперебійне функціонування мережі «FORCENET», відбиття кібератак та ліквідацію наслідків після атак у межах військово-морського сегменту кіберпростору, а це розгалужена мережа із 700 тисяч комп'ютерів. Чисельність Командування складає 200 військовослужбовців та цивільних співробітників. Умовно кажучи, за кількісною оцінкою, на кожного фахівця цього управління приходиться 3,5 тисячі комп'ютерів.

Починаючи з 2011 року, кібернетичне Командування США щорічно на регулярній основі проводить навчання «Cyber Flag» у взаємодії з іншими агентствами й відомствами та разом із союзниками по Альянсу НАТО. У них беруть участь сотні фахівців із метою підвищення готовності до реагування на кібератаки, налагодження взаємодії між відомствами, а також союзниками та партнерами. Навчання «Cyber Flag» – це система колективної безпеки у кіберпросторі, створена задля поліпшення можливостей з виявлення, синхронізації та спільного реагування на змодельовані шкідливі дії в кіберпросторі, націлені на критично важливу інфраструктуру та ключові ресурси. Проект створений за ініціативи США із залученням міжнародних партнерів США: Канади, Великої Британії, Данії, Франції, Естонії тощо[11].

Діяльність кіберсил США спрямована на захист інформаційних систем Міністерства оборони від усіх кібератак і вторгнень, передбачає посилення здатності країни протистояти кібератакам і реагувати на них. Кіберкомандування надає варіанти для політиків та використовує свої міжвідомчі й міжнародні зв'язки для виявлення та припинення зловмисної кіберактивності, перш ніж вона загрожуватиме критичній інфраструктурі і ключовим ресурсам країни. Американські кіберсили забезпечують здійснення повного спектра операцій (наступальних та оборонних) у кіберпросторі, щоб допомогти Об'єднаним силам у досягненні цілей їх місії. Кібероперації забезпечують надійний стан безпеки мереж і даних навколо світу, нейтралізують та нівелюють можливості злочинної діяльності хакерів та іноземних держав-супротивників. Першочергово USCYBERCOM створювалися суто як захисні сили та офіційно отримали наступальний мандат лише в 2018 році, коли набув чинності таємний Указ Президента США (National Security Presidential Memoranda) «United States Cyber Operations Policy», який передбачав «Defend forward» (захист на випередження), «Hunt forward» (полювання на випередження), «Persistent engagement» (постійне залучення), та яким відповідальним структурам було надано дозвіл на проведення «підривної діяльності в кіберпросторі» на межі військових дій та на випередження дій потенційних ворогів (концепція превентивного удару)[12]. Аналогічна норма продубльована у Стратегії кібероборони Міністерства оборони США 2018 року, відповідно до якої Сполучені Штати захищатимуться на випередження, щоб зруйнувати джерело зловмисної кіберактивності, включаючи активність, яка є нижчою за рівень збройного конфлікту. Це означає, що якщо пристрій, мережа, організація чи держава-противник ідентифіковані як загроза мережам і установам США, або активно атакують їх у кіберпросторі або через нього, вони можуть очікувати на адекватну відповідь Сполучених Штатів Америки.

На виконання задекларованих завдань 5 листопада 2018 року, напередодні виборів у США, Кіберкомандування США на декілька днів заблокувало роботу російської фабрики тролів – Агентства інтернет-досліджень, розташованого у м. Санкт-Петербурзі. Підставою для цього стали здобуті розвідувальні дані щодо намірів втручання держави-агресора у вибори в США. Це була перша наступальна кібероперація, яку офіційно санкціонувало та публічно визнало

[11] Cyber Flag. URL: https://federalnewsnetwork.com/tag/cyber-flag
[12] National Security Presidential Memoranda. URL: https://irp.fas.org/offdocs/nspm/index.html

політичне керівництво країни. Кіберкомандування США має повноваження не лише проводити кібероперації для захисту своєї країни, але й для захисту країн-союзників, тобто надавати допомогу партнерам при одночасному забезпеченні національних інтересів США.

Із 2018 року в Естонії, Литві, країнах Латинської Америки за сприяння США було створено Інтегрований кіберцентр та Об'єднаний центр операцій (із бюджетом $500 мільйонів). Його метою стало об'єднання військової та розвідувальної спільноти, інших федеральних агенцій, міжнародних партнерів. Наприклад, 15 вересня 2021 року Австралія, Канада, Нова Зеландія, США та Велика Британія утворити розвідувальний альянс «П'ять Очей» з метою оперативного взаємного обміну інформацією та передовими можливостями для ведення кібервійни. Діяльність щодо обміну інформацією в реальному часі передбачає налагодження прямих каналів доступу до оперативної інформації партнерів між собою.

19 грудня 2022 року Міністерство оборони США підвищило статус однієї із структур у складі Кіберкомандування – оперативної групи «Cyber National Mission Force» (CNMF)[13], основними завданнями якої є централізоване проведення кібервійськових операцій та захист військових комп'ютерних мереж. Ця структура складається із 39 об'єднаних кіберкоманд та має у штаті понад 2 тис. військовослужбовців і цивільних осіб, які виконують такі завдання, як забезпечення безпеки виборів, боротьба з кібершпіонажем або програмами-вимагачами тощо. У березні 2023 року Кіберкомандування США анонсувало про створення власного Центру розвідки, адже тривалий час відомство використовувало інші джерела збору інформації. Проект має на меті зміцнити збір даних та розширити спектр можливостей Кіберкомандування США щодо діяльності іноземних держав у кіберсфері, яка постійно та динамічно змінюється та розширюється[14]. До кінця 2023 року в армії США планується створити офіс «Program Manager Cyber and Space», який в рамках компетенції займатиметься розробкою та реалізацією наступальних кібер- та космічних операцій.

2 березня 2023 року була затверджена нова Стратегія національної кібербезпеки США, розроблена після низки великих і потужних кібератак, включаючи напад на трубопровід «ColonialPipeline» у 2021 році й кіберзлам федеральних установ протягом 2019–2020 років[15]. Цей стратегічний документ чітко формулює завдання, вирішення яких надасть приватним особам, державним структурам і бізнесу можливість консолідовано діяти в цифровій сфері з мінімальними ризиками. Стратегія визначає, що Уряд США повинен скоординовано використовувати всі наявні важелі та інструменти для захисту основ національної безпеки, громадської безпеки та загального економічного процвітання. Стратегія спрямована на потужний захист інвестицій у відбудову американської критичної інфраструктури, розвиток сектору відновлювальної енергії та розвиток американських цифрових технологій і виробничої бази.

[13] The Cyber National mission force is the newest military command. URL: https://mybaseguide.com/cyber-national-mission-force

[14] US Army to launch offensive cyber capabilities office. URL: https://www.defensenews.com/electronic-warfare/2022/08/31/us-army-to-launch-offensive-cyber-capabilities-office/

[15] National Cybersecurity Strategy. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Пріоритетними засадами Стратегії є: захист критичної інфраструктури; ліквідація, запобігання та блокування будь-яких кіберзагроз; формування ринкових потужностей цифрової економіки, що гарантують кібербезпеку, інноваційний розвиток безпечних і стійких технологій та інфраструктури наступного покоління; розбудова міжнародного цифрового партнерства. При цьому окремі положення Стратегії присвячені розбудові кібервійськ та удосконаленню їх компетенції у сфері проведення наступальних операцій у кібердомені навколо світу.

Таким чином, у США функціонує Кіберкомандування Сполучених Штатів Америки / United States Cyber Command (USCYBERCOM). Це частина Збройних Сил США, яка була створена ще у 2009 році й підпорядковується об'єднаному Стратегічному командуванню США. У 2020 році було оголошено, що статус «USCYBERCOM» буде підвищений до статусу одного з Об'єднаних Командувань Збройних Сил США / Unified Combatant Command, тобто до рівня одного з функціональних командувань, таких як, наприклад, Командування сил спеціальних операцій або Транспортне Командування. На переконання експертів національної асоціації нинішніх та колишніх військової спеціалістів із цифрової безпеки (Military Cyber Professional Association), цього недостатньо, і залежність Кіберкомандування від інших гілок Збройних Сил США, які делегують «USCYBERCOM» свої ресурси та спеціалістів, створює несистемний та складний підхід до оцінки кіберзагроз й «непотрібний ризик» для національної безпеки США. Тому асоціація закликає Конгрес США створити окремий, сьомий рід військ – Кібервійська / U.S. Cyber Force, і це питання все ще залишається відкритим.

Загалом, перевагами побудови кібервійськ за зразком США є те, що у кожного роду військ своя складова представлена в кіберпросторі, що надає можливості командувачам відповідних родів військ скоротити ланцюг у системі військового оперативного управління із забезпечення дій своїх сил (військ). Недоліком є розпорошеність сил кібервійськ і необхідність створення ще одного органу військового управління у вигляді «кіберкомандування» для управління наявними в усіх Збройних Силах кібервійськами, що призводить до додаткових фінансових витрат, спрямованих на утримання відповідних підрозділів.

Велика Британія

Велика Британія активно нарощує свій потенціал у кіберпросторі з метою протидії ймовірним супротивникам, особливо в умовах збройної військової агресії Російської Федерації проти України. У 2016 році в цій країні створено Національний центр кібербезпеки з метою консультування уряду і громадськості про те, як знизити ризик реальних і потенційних кібератак. У 2018 році Велика Британія анонсувала створення власних кібервійськ на базі Міністерства оборони країни та Центру урядового зв'язку (GCHQ) для організації захисту власного кіберпростору, у першу чергу, від російської інформаційної експансії, із загальним штатом 2 тис. військовослужбовців та із бюджетним фінансуванням у розмірі понад 250 млн фунтів. Передумовами цього рішення стали зростаючі глобальні виклики та загрози світового масштабу. Головна мета – збільшення наступальної складової й кіберборотьба не лише проти окремих кіберзлочинців, але й країн чи угрупувань: як то Росія, Іран, ІДІЛ тощо. У 2020 році такі національні

Кіберсили «National Cyber Force» (NCF)[16] було створено. NCF об'єднує під єдиним командуванням співробітників Агентства розвідки, кібернетики та безпеки (GCHQ), Міністерства оборони, Секретної розвідувальної служби (MI6), Лабораторії оборонної науки і технологій (DSTL), фахівців Центру урядового зв'язку, досвідчених військовослужбовців та профільних учених.

Отже, Кіберсили Великої Британії орієнтовані на виконання наступальних кібероперацій. Кібероперації (Cyberspace operations) пов'язані із використанням можливостей кіберпростору з метою досягнення військових цілей або ефектів в або за допомогою кіберпростору. Кібероперації націлені на технічні об'єкти, реалізуються приховано та здійснюють опосередкований психологічний вплив на осіб, які приймають рішення, та фахівців IT-сфери, задіяних в управлінні об'єктами інформаційної інфраструктури. Усі кібероперації, які проводять національні Кіберсили (NCF), здійснюються із дотриманням нормативів та етики відповідно до національного й міжнародного законодавства. Кібероперації базуються на глибокому розумінні сучасного кіберсередовища, що дозволяє NCF змістовно їх проектувати, визначати час і націлювати їх.

У рамках функціональних завдань кібервійська захищають свої дислокації за кордоном; протидіють зовнішнім іноземним кампаніям у сфері дезінформації; проводять щоденний моніторинг кіберпростору, забезпечують кібероборону країни на перманентній основі, протидіють хакерським угрупуванням та світовим кіберзлочинцям, виробникам і розповсюджувачам дитячої порнографії тощо. Тобто NCF націлені на нівелювання та блокування будь-яких кіберзагроз у режимі реального часу, включаючи іноземні системи протиповітряної оборони й мобільні телефони осіб, яких уряд вважає потенційними злочинцями або терористами.

За оперативним задумом Кіберкомандування Великої Британії, найближчими роками планується збільшити штат цього спеціального підрозділу до 3 тис. співробітників. Центральне місце в діяльності кібервійськ країни посідає «доктрина когнітивного ефекту», яка включає методи, спрямовані на те, щоб посіяти паніку та недовіру, знизити бойовий дух і послабити здатність супротивника планувати й реалізовувати свою діяльність у кіберпросторі.

Сучасна військова доктрина Великої Британії під назвою «Велика Британія в епоху конкуренції»[17] оприлюднена 22 березня 2021 року і розрахована на період до 2030 року. Особлива увага в цьому стратегічному документі приділяється питанням розбудови та оптимізації NCF, їх динамічному розвитку. У грудні 2021 року опублікована оновлена Національна стратегія кібербезпеки Великобританії на 2022–2025 роки[18]. Окремі положення цього програмного документу присвячені питанням удосконалення перспективної діяльності кіберсил та розвитку їх бойових спроможностей, посилення стану кібероборони країни.

---

[16] The National Cyber Force (NCF) is a partnership between defence and intelligence. URL: https://www.gov.uk/government/organisations/national-cyber-force/about

[17] Global Britain in Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy URL: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

[18] National Cyber Security Strategy 2022-2025. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1180089/14.283_CO_National_Cyber_Strategy_Progress_Report_Web_v3.pdf

19 грудня 2022 року Уряд Великої Британії оприлюднив нову «Рамкову програму забезпечення національної стійкості»[19]. Цей програмний документ розроблено відповідно до урядових зобов'язань, визначених у Звіті щодо Комплексного Огляду сектору безпеки, оборони, розвитку пріоритетів зовнішньої політики від 16 березня 2021 року, з урахуванням масштабів поширення загрозливих тенденцій та посилення невизначеності у глобальному безпековому середовищі, та розраховано на період до 2030 року. Рамкова програма містить оновлені концептуальні й методологічні підходи до управління ризиками та планування у цій сфері на всіх рівнях, передбачає посилення комплексної взаємодії, доповнює чинні стратегічні документи, зокрема у сфері кібербезпеки, захисту об'єктів критичної інфраструктури тощо.

У новій доповіді уряду 2023 року «The National Cyber Force: Responsible Cyber Power in Practice»[20] висвітлено форми та методи ведення кібервійни національними Кіберсилами Великої Британії (NCF), які включають, у тому числі, заходи психологічного впливу, що створюватимуть параною серед ворогів, не даючи їм зрозуміти, що результати, з якими вони стикаються, є наслідком проведених успішних кібероперацій. Найбільший ефект досягається при впливі на інформаційні мережі ворога із часом, що викликає «непомітний нахил ігрового поля». Так, наприклад, кібероперації проти терористичного угруповання «ІДІЛ» змусили його оперативників не довіряти відданим наказам зверху та сумніватися щодо них. Отже, метою таємних дій є чинення масштабного психологічного тиску.

Виходячи з масштабів російської та іранської загроз, бюджет на фінансування кібервійськ Великої Британії у 2023 році було збільшено до 400 млн фунтів на рік. 4 квітня 2023 року, за результатами трирічного успішного досвіду функціонування NCF, Уряд Великобританії опублікував Керівництво під назвою: «Відповідальна кібервлада на практиці»[21]. Основним документом, що визначає пріоритети діяльності кібервійськ, є національна кіберпрограма, яка розробляється на планових засадах. Стратегічна діяльність NCF полягає в тому, щоб ускладнити супротивникам використання кіберпростору та цифрових технологій для досягнення своїх цілей. NCF щодня проводить кібероперації, щоб захистити кібердомен Великої Британії від кіберзагроз, розвивати та забезпечувати політику національної безпеки, підтримувати військові операції навколо світу та протидіяти сексуальній експлуатації і насильству над дітьми в мережі Інтернет. Кібероперації NCF проводяться проти державних і недержавних загроз (таких, як тероризм).

На практиці NCF розробляє та застосовує кіберпотенціал для проведення своїх операцій, включаючи блокування й переривання можливості противника використовувати кіберпростір і цифрові технології, впливаючи на свідомість та психіку противника. Виконання кібероперацій є досить складним процесом.

[19] The UK Government Resilience Framework. URL: https://www.gov.uk/government/publications/the-uk-government-resilience-framework

[20] The National Cyber Force: Responsible Cyber Power in Practice. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148278/Responsible_Cyber_Power_in_Practice.pdf

[21] Guidance Responsible Cyber Power in Practice. URL: https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html

Велика Британія як відповідальна демократична кібердержава діє в законний та відповідальний спосіб, узгоджений з етичними правилами. Зважаючи на це, NCF реалізують свою діяльність відповідно до таких основних принципів: *підзвітність* (діяльність здійснюється відповідно до вимог національного та міжнародного законодавства, а також правил етики); *точність* (кібероперації базуються на глибокому розумінні кіберсередовища та розроблені таким чином, щоб їх можна було точно та вірогідно розрахувати за часом і мішенями); *відкаліброваність* (вплив та наслідки операцій ретельно оцінюються з урахуванням ширшого контексту, розглядається широкий спектр факторів, у тому числі ті, які можуть вплинути на процеси ескалації та деескалації).

Реалізація зазначених принципів діяльності NCF має на меті змінити поведінку противників, використовуючи їхню залежність від цифрових технологій, блокувати операційні системи та мережі. Також ці операції спрямовуються на те, щоб усунути здатність противника діяти в кіберпросторі. Інші кібероперації спрямовані на більш широкий вплив на спроможність противника реалізовувати свої наміри в кібердомені. Це досягається різними способами, зокрема впливом на здатність противника здобувати, аналізувати та використовувати інформацію, необхідну для досягнення своїх цілей, тощо. NCF інтегрує власні кібернетичні можливості з іншими військовими підрозділами Великої Британії, щоб організувати ефективний кіберзахист, залучити союзників і стримувати супротивників.

Загалом існує три категорії кібероперацій, що можуть проводитися підрозділами NCF:

- протидія кіберзагрозам, які продукують та поширюють терористи, міжнародні злочинці й держави, які використовують глобальну всесвітню мережу для здійснення протиправних транскордонних операцій, кібератак, що можуть завдати суттєвої шкоди Великій Британії або іншим державам НАТО;
- протидія кіберзагрозам, які підривають конфіденційність, цілісність і доступність інформації та даних, а також ефективне використання пошукових систем користувачами. Це може передбачати проведення кібероперацій разом із низкою інших засобів, включаючи покращену кіберстійкість, скоординовані дії з урядами союзників і плідну співпрацю із приватним ІТ-сектором;
- сприяння оборонним кіберопераціям Великої Британії та допомога в реалізації військових програм зовнішньої політики держави. Кібероперації можуть підтримувати весь спектр оборонної діяльності та мати особливий внесок у підтримку ключових завдань зовнішньої політики та безпеки.

NCF регулярно планує та проводить операції з підтримки та захисту військових операцій навколо світу, а також допомагає убезпечити виконання завдань закордонних місій.

Нормативно-правова база, що регулює операції NCF, включає: Закон про розвідувальні служби 1994 року (ISA)[22], Закон про слідчі повноваження 2016 року (IPA)[23] і Закон про регулювання слідчих повноважень 2000 року (RIPA)[24].

[22] Intelligence Service Act 1994. URL: https://www.legislation.gov.uk/ukpga/1994/13/contents
[23] Investigatory Powers Act 2016. URL: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
[24] Regulation of Investigatory Powers Act 2000. URL: https://www.legislation.gov.uk/ukpga/2000/23/contents

Рішення про схвалення тієї чи іншої кібероперації приймаються на рівні військового Кіберкомандування шляхом проведення юридичних консультацій щодо відповідності вимогам національному та міжнародному праву. Напрями діяльності NCF підлягають обов'язковому затвердженню міністром оборони, судовому нагляду та парламентському контролю, що робить режим управління кібероперaціями Великої Британії одним із надпотужних у світі. Ключовою частиною відповідальних кібероперацій є розробка та використання можливостей у спосіб, який є передбачуваним і контрольованим, і де ризики пропорційні необхідному результату. Кібероперації NCF потребують значної підготовки, що включає відповідну технічну розвідку кіберсередовища, оцінку ризиків тощо. Існує декілька етапів затвердження, на яких розглядаються техніко-економічна доцільність, операційний план, переваги та ризики операції, перш ніж її можна буде дозволити та реалізувати.

Велика Британія є світовим лідером у проведенні наступальних кібероперацій, а NCF має трирічний досвід успішної діяльності і поєднує в собі елементи як розвідувального співтовариства, так і збройних сил. При цьому загальне керівництво кібероборoною здійснюється міністерствами оборони та закордонних справ країни.

Франція

Відповідно до положень «Білої книги з питань національної безпеки і оборони» Французької Республіки інституційне формування системи кіберзахисту у складі Національних Збройних Сил є одним із пріоритетних напрямів військового будівництва, а кіберпростір розглядається як сфера глобального протиборства. З урахуванням викладених у положеннях Воєнної доктрини Франції концептуальних основ, у травні 2017 року було створено Кіберкомандування Збройних Сил Франції. Відповідний Декрет «Про зміни організаційно-штатної структури Збройних Сил»[25] підписав Міністр оборони країни. Загальне керівництво покладено на військову посадову особу в ранзі дивізійного генерала.

До складу Кіберкомандування Франції входять:

– Кіберштаб (м. Париж), при якому функціонує Центр операцій (Centre des operations CYBER);

– Аналітичний Центр кіберзахисту (м. Париж та м. Ренн, Centre d'analyse en lutte informatique defensive);

– Центр контролю та безпеки інформаційних систем (м. Мезон-Лаффіт, Centre d'audit et de sécurité des systèmes d'information);

– Центр оперативної підготовки та резерву кіберзахисту (м. Гер);

– Центр міжвидової сертифікації (м. Париж, Centre des homologations principales interarmées);

– Спеціальні підрозділи кіберзахисту Військово-Морських Сил та Повітряно-Космічних Сил.

Загальна чисельність зазначених регулярних формувань складає 4,2 тис. військовослужбовців, із них резервістів – 400 осіб.

[25]Arrêté du 4 mai 2017 modifiant l'organisation de l'état-major des armées. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000034581382/2021-07-15

Кіберкомандування вирішує такі основні завдання: адміністративне та оперативне керівництво кіберсилами; поточне забезпечення захисту інформаційно-телекомунікаційних систем військового відомства, розробка, планування та проведення військових операцій у кіберпросторі; формування підходів до ведення бойових дій у кіберпросторі у взаємодії з іншими профільними структурами міністерств та відомств країни; узгодження моделі кіберзахисту та її загальна координація (кадрова політика, технічні потреби, розробка доктрини) тощо[26].

Практична діяльність Кіберкомандування здійснюється на підставі: Настанов до оборонних (Lutte informatique defensive, 2018 р.) та наступальних (Lutte informatique offensive, 2019 р.) дій у кіберпросторі, а також Доктрини «Інформаційно-психологічна боротьба» (Lutte informatique d'influence, 2021 р.)[27].

У рамках оборонних дій у кібердомені вирішуються завдання щодо попередження, виявлення та реагування на реальні та потенційні кіберзагрози, а також захисту інформаційно-комунікаційного середовища (ІКС) військового відомства від несанкціонованого доступу до систем військового управління або виведення їх із ладу, запобігання нештатним ситуаціям. Наступальні операції здійснюються кіберсилами у взаємодії із традиційними військовими засобами для кібернетичного впливу на інформаційно-комунікаційні системи ворога з метою максимального досягнення поставлених цілей (порушення та виведення з ладу працездатності операційних систем, отримання доступу до конфіденційної інформації тощо).

Основними завданнями у сфері інформаційно-психологічної боротьби за участю кіберпідрозділів Франції є: інформаційна підтримка збройних сил та військових формувань, у тому числі під час виконання гуманітарних або миротворчих операцій за кордоном; тотальна дискредитація дій супротивника, введення його в оману щодо характеру діяльності власних кіберсил; перманентний моніторинг кіберпростору та інформаційного простору тощо. Операції подібного роду проводяться переважно за кордоном і виключно в рамках обмежених військових кампаній.

Аналітичний центр кіберзахисту (АЦКЗ) є наступним компонентом системи забезпечення безпеки інформаційних систем Міністерства оборони Франції. До його функціональних повноважень відносяться: моніторинг цифрового простору, виявлення та ліквідація кіберзагроз, відбиття кібератак, оперативне поновлення працездатності виведених з ладу вузлів та агрегатів ІКТ. Для вирішення практичних завдань та забезпечення належного рівня безпеки ця структура проводить плідну співпрацю та взаємодію із Групою реагування на кіберінциденти (Groupes d'intervention en cyberdefense) (CERT-FR)[28]. У випадку відсутності можливості усунути наслідки кіберінциденту віддалено, спеціальна група реагування у сфері кіберзахисту направляється до місця з метою фізичного усунення проблеми.

26 Le commandement de la cyberdéfense. URL: https://www.defense.gouv.fr/comcyber

27 Élements Publics de Doctrine Militaire de lute informatique d'influence. URL: https://www.defense.gouv.fr/sites/default/files/ema/doctrine_de_lutte_informatique_dinfluence_l2i.pdf

28 Groupes d'intervention en cyberdefense. URL: https://cert.ssi.gouv.fr

Центр контролю та безпеки інформаційних систем відповідно до функціональних завдань призначений для забезпечення безпеки технічної основи ІС та недопущення витоку конфіденційної та службової інформації навіть через ймовірні випадки побічного випромінювання радіоелектронної апаратури. Функціональні підрозділи цієї структури фізично розташовані у містах: Брест, Орлеан, Тулон, Рен.

Центр оперативної підготовки та резерву кіберзахисту забезпечує взаємодію військових і цивільних спеціалістів, сприяючи обміну досвідом та розвитку їхніх професійних навичок. Ця структура є відповідальною за набір, підготовку та розподіл спеціалістів із кіберзахисту в рамках потреб військового відомства, бере участь в організації національних та міжнародних профільних навчань, у тому числі щорічного стратегічного тренінгу з кібербезпеки «DevNet» Збройних Сил Франції з метою відпрацювання процедур забезпечення стабільного та безперебійного функціонування інформаційної інфраструктури в умовах масованих кібератак. «DevNet» – це інтегрована площадка, яка у навчальних цілях використовується програмістами і допомагає розробникам та фахівцям в IT-галузі розвивати інтеграцію з продуктами, інтерфейсами, надає змогу обмінюватися досвідом і навичками[29]. Також ця площадка надає можливість використовувати віртуальні інструменти для написання й тестування своїх програм і додатків. У підпорядкуванні цього Центру перебуває оперативний резерв кіберзахисту, представники якого за необхідності можуть комплектувати профільні підрозділи Збройних Сил та брати участь у проведенні операцій у кібердомені.

Резервний компонент включає два сегменти. Перший – «резерв реагування» (Réserve d'intervention, головним чином, це співробітники профільних підприємств) служить для здійснення моніторингу кіберпростору та виявлення кіберзагроз на ранній стадії. Другий – «резерв поновлення» (Réserve de reconstruction, переважно студенти вищих навчальних закладів старших курсів) виконує нескладні завдання з метою ліквідації наслідків кібератак.

Центр міжвидової сертифікації відповідальний за контроль виконання програм у сфері інформаційних систем та мереж зв'язку, а також сертифікацію технічних засобів, що використовуютсья у військовому відомстві. В інтересах організації навчання спеціалістів із кіберзахисту у Збройних Силах Франції була створена спеціалізована комісія з питань підготовки у сфері кібербезпеки (Commission d'adaptation à la formation Cybersécurité, CAF Cyber), відповідальна за розробки навчальних програм та визначення нормативів для слухачів за відповідними обліковими спеціальностями. Основним навчальним закладом Збройних Сил Франції є військова школа зв'язку (м. Лаваль), яка має у своїй структурі два центри підготовки. У цьому навчальному закладі готують військовослужбовців і цивільний персонал для підрозділів кіберзахисту. Школа перебуває в оперативному підпорядкуванні командування зв'язку та інформаційних систем Збройних Сил Франції.

Пріоритетними завданнями у сфері розвитку системи кібероборони Збройних Сил Франції до 2025 року є нарощування потенціалу наступальних

[29] DevNet – Faster Ethereum Development. URL: https://devnet.so

операцій інформаційно-технічного впливу в кіберпросторі, системне удосконалення їх проведення, збільшення штатної чисельності до 5 тис. військовослужбовців, залучення висококваліфікованих спеціалістів до лав кібервійська, системна підготовка професійних кадрів, здатність впроваджувати інноваційні технологічні рішення та програми штучного інтелекту в питаннях забезпечення кібербезпеки, розширення кооперації та співпраці з партнерами з НАТО та ЄС. При цьому фінансування діяльності Кіберкомандування Франції планується збільшити у 2024 році до показника 1,6 млрд євро на рік.

Таким чином, у структурі Збройних Сил Франції функціонує Командування кіберзахисту (COMCYBER), яке безпосередньо підпорядковане Начальнику Штабу оборони (CEMA) та є оперативним командуванням, яке об'єднує всі сили кіберзахисту Міністерства оборони під спільним керівництвом. Його місія – захист інформаційних систем, а також розробка, планування та проведення військових операцій у кіберпросторі. Для виконання своїх місій COMCYBER має дві структури: Штаб кіберзахисту (EM-CYBER) та армійську групу кіберзахисту (GCA), яка розташована в Ренні та Парижі. Для виконання своєї місії COMCYBER спирається на три цінності: високі стандарти, креативність і дружній колектив.

На відміну від широкомасштабного підходу, який практикується в США та Великій Британії, у Франції саме комбінування кібероперацій з можливостями радіоелектронної розвідки, радіоелектронною протидією створює компактну вузькоспеціалізовану структуру кібервійськ вищого стратегічного рівня. Переваги кібервійськ Франції полягають у зменшеному розмірі сил та, відповідно, у зменшенні фінансових витрат на утримання штату. На цьому фоні недоліком виступає мінімізація сил, що обмежує кількість завдань, що виконуються.

Польща

У 2016 році під час саміту НАТО у Варшаві констатовано, що захист кіберпростору є одним із основних завдань колективної оборони НАТО, а кіберпростір визнано зоною військових операцій[30]. Наприкінці 2017 року Польща як активний член НАТО анонсувала виділення 2 мільярдів злотих (близько 465 млн євро) на створення власного кібервійська.

5 липня 2018 року в Польщі ухвалено закон «Про національну систему кібербезпеки» («*O krajowym systemie cyberbezpieczeństwa» 05.07.2018*)[31], за наслідками реалізації якого в державі створено відповідні структури, основними з яких стали Національний центр кібербезпеки, Національна група реагування на комп'ютерні інциденти, Національний центр безпеки кіберпростору Міністерства оборони Республіки Польща, галузеві структури кіберзахисту тощо.

Прикладом ефективної консолідації сил та засобів для забезпечення кіберзахисту є Національний центр безпеки кіберпростору Міністерства оборони Польщі (*Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni*), створений на базі Національного криптологічного центру (NCK) та IT-інспекції (I2). Ресурси та

[30] Міністерство оборони Польщі. Сили оборони кіберпростору. URL: https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni

[31] Ustawa «O krajowym systemie cyberbezpieczeństwa» 05.07.2018. URL: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/krajowy-system-cyberbezpieczenstwa-18746756

повноваження Міністерства оборони у сферах кібер-, крипто- та ІТ були консолідовані в одній установі, що дозволило поглибити співпрацю між фахівцями, відповідальними за ІКТ-безпеку та криптологічну підтримку, та підрозділами, відповідальними за закупівлю апаратного та програмного забезпечення, а також обслуговування відомчих мереж і систем.

На виконання рекомендацій НАТО у 2019 році розроблено та затверджено Концепцію організації та функціонування Сил оборони кіберпростору (WOC)[32], положення якої спрямовані на підвищення безпеки держави та громадян у кіберпросторі та засновані на чотирьох стратегічних рівнях. Перший – це консолідація та побудова власне структур кібербезпеки; другий – освіта, навчання та тренінги спеціалістів; третій – співпраця та побудова міжнародної позиції із країнами-партнерами; четвертий – підвищення рівня безпеки відомчих і військових мереж та систем Польщі. Одночасно було створено групу формування командування Сил оборони кіберпростору (СОК).

18 березня 2022 року Президент Польщі підписав закон «Про оборону» («*O obronie Ojczyzny» 11.03.2022*)[33], відповідно до якого війська оборони кіберпростору – це спеціалізована компонента Збройних Сил, призначена для виконання повного спектру завдань у кіберпросторі, зокрема не лише реактивних дій, але й проактивного захисту (постійного виявлення інструментів, методів, мотивації і процедур потенційних супротивників) та активної оборони (розпізнавання потенційних небезпек, загроз у кіберпросторі, безпосередніх дій). Стаття 23 вказаного законодавчого акта регламентує повноваження та функціональні завдання польського кібервійська.

Таким чином, у Польщі законодавчо визначені підстави створення нової складової Збройних Сил країни – Сил оборони кіберпростору (*Wojska Obrony Cyberprzestrzeni*). Передбачено, що сили (війська) оборони кіберпростору Польщі є регулярною армією, яка має згідно з компетенцією оборонні можливості, функції виявлення, а також здійснення наступальних дій, якщо буде така потреба. Перед силами кібероборони як новим родом спеціальних військ ставляться досить конкретні завдання – ведення оборонних, наступальних та розвідувальних дій у кіберпросторі. Остаточне формування Сили оборони кіберпростору Польщі планується завершити до 2026 року. Процес створення польських Сил оборони кіберпростору ґрунтується на досвіді створення польських підрозділів спецназу, які на початку також були спеціальним компонентом Збройних Сил Польщі, проте згодом були трансформовані в окремий рід військ. Сили оборони кіберпростору в мирний час підпорядковуватимуться безпосередньо Міністерству оборони, а під час мобілізації та війни – головнокомандувачу, обраному Президентом країни.

Передбачено постійний штат кібервійськ Польщі у кількості 1 тис. осіб. Необхідні фахові оперативні спроможності кіберсил під керівництвом Міністра оборони повинні бути сформовані до кінця 2024 року, та у перспективі будуть передані в підпорядкування начальнику Генерального штабу Збройних Сил Республіки Польща. Водночас війська територіальної оборони Польщі були

[32] Міністерство оборони Польщі Концепція організації та функціонування Сил оборони кіберпростору (CYBER.MIL.PL). URL: https://www.cyber.mil.pl/

[33] Ustawa «O obronie Ojczyzny» 11.03.2022. URL: https://eli.gov.pl/eli/DU/2022/655/ogl

розширені за рахунок кіберкомпонента (*територіальних кібер-груп*), у них були відкриті вакансії для місцевих молодих спеціалістів.

Сили оборони кіберпростору Польщі відповідають за безпеку кіберпростору та здатні проводити повний спектр операцій, включаючи оборону, розвідку та наступ, а також протидію психологічним та інформаційним операціям. Цей підрозділ відповідає за:

- забезпечення кібербезпеки Міністерства оборони;
- планування, організацію та використання кіберпростору;
- проведення оборонних та наступальних операцій у кіберпросторі;
- створення, підтримку та захист критичної інфраструктури та інформації в кіберпросторі;
- забезпечення підтримки військових операцій, що проводяться Збройними Силами Польщі, та операцій, які проводяться в рамках Альянсу;
- координацію з іншими державними установами, відповідальними за оборону;
- проведення досліджень та підготовку інноваційних рішень для виявлення інцидентів у кіберпросторі;
- проектування, створення, впровадження та використання національних криптологічних технологій і рішень для забезпечення інформаційної безпеки;
- розробку нових рішень у сфері сучасних технологій та криптографії;
- проведення освітніх і навчальних заходів;
- нагляд за роботою CSIRT MON, яка відповідає за моніторинг мереж МО 24/7 та захист польського кіберпростору.

У 2022 році Сили оборони кіберпростору Польщі підписали Меморандум про взаєморозуміння з НАТО щодо створення цілодобових контактних пунктів, відповідальних за координацію політики кібербезпеки та технічний аналіз кіберзагроз[34]. Крім того, налагоджено співпрацю із Центром передового досвіду НАТО з питань кіберзахисту, розташованим в Естонії.

Таким чином, Польща демонструє та впроваджує виважену й послідовну державну політику боротьби із сучасними кіберзагрозами у військовій сфері, свідченням чого є сформовані законодавчі та організаційні засади функціонування військ (сил) оборони кіберпростору.

ІІІ. Висновки та пропозиції

Підсумовуючи викладене, варто зазначити, що кожна держава-член НАТО динамічно працює над інституційними засадами створення власних кібервійськ (кіберсил). У досліджених країнах НАТО діє власна модель законодавчого забезпечення та інституційного створення кібервійськ (кіберсил) (Додаток 1). Правові засади створення кібервійськ задекларовано у спеціальних нормативно-правових актах, у тому числі загального, концептуального характеру (стратегіях, концепціях, доктринах, законах), на підставі яких розроблено локальні акти щодо функціонування, компетенції кібервійськ, їх фінансування, підготовки кадрів тощо.

[34] POLISH "CYBERCLAWS". BUILDING OF THE CYBERARMY OF THE RISING MILITARY POWER IN EUROPE. URL: https://pulaski.pl/en/polish-cyberclaws-building-of-the-cyberarmy-of-the-rising-military-power-in-europe/

До типових характеристик кіберсил НАТО у досліджуваних країнах на даний час слід віднести такі: кіберсили здебільшого перебувають у складі Збройних Сил країн-членів НАТО; їх чисельність становить від 0,5 % (США) до 5 % (Франція) від загальної чисельності Збройних Сил країни; грошове забезпечення таких кіберсил на 20–30 % вище, аніж у військовослужбовців інших родів військ; відсутність універсальних структури та підпорядкування.

Заслуговує на увагу апробований у США широкомасштабний підхід створення кібервійськ шляхом формування Кіберкомандування (USCYBERCOM) як частини Збройних Сил, що підпорядковується об'єднаному Стратегічному командуванню США. Кожний рід військ – сухопутні війська, флот, повітряні сили та морська піхота мають власні кіберкоманди. У перспективі планується створення в США окремого, сьомого роду військ – кібервійська (U.S. Cyber Force). Попри наявність чітко структурованого кіберкомандування на державному рівні загальне керівництво кібероборoною здійснюють спільно Директор національної розвідки (Director of National Intelligence, DNI) та Національна рада безпеки (United States National Security Council).

На відміну від широкомасштабного підходу, який практикується у США та Великій Британії, у Франції саме комбінування кібероперацій із можливостями радіоелектронної розвідки, радіоелектронною протидією створює компактну вузькоспеціалізовану структуру кібервійськ вищого стратегічного рівня. Переваги кібервійськ Франції полягають у зменшеному розмірі задіяних сил та, відповідно, у зменшенні фінансових витрат на утримання штату кібервійська. На цьому фоні недоліком виступає мінімізація сил, що обмежує кількість завдань, що виконуються. У структурі Збройних Сил Франції діє Командування кіберзахисту (COMCYBER), яке безпосередньо підпорядковане Начальнику Штабу оборони (CEMA) та є оперативним командуванням, що об'єднує всі сили кіберзахисту Міністерства оборони під спільним керівництвом. Для виконання своїх завдань COMCYBER має дві структури: Штаб кіберзахисту (EM-CYBER) та армійську групу кіберзахисту (GCA).

Польська модель передбачає формат утворення у структурі Збройних Сил нового компоненту – військ оборони кіберпростору, що надає змогу значно посилити оборонний потенціал країни.

З огляду на існуючі загрози, створення спеціальних підрозділів кібервійськ в Україні є важливим та рішучим кроком, спрямованим на запровадження дієвих та ефективних механізмів стримування російської агресії у кібердомені, особливо в умовах триваючої кібервійни.

Згідно з Розділом I Стратегії кібербезпеки України[35] до завдань кіберсил належить «проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами». Тобто бойове застосування кіберсил має забезпечувати превентивні наступальні операції у кіберпросторі та не бути обмеженим територіальним принципом, чітким визначенням противника (агресора) та його дій.

[35] Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

За результатами проведеного дослідження, враховуючи досвід розробки правових засад та інституційного розвитку кібервійськ у проаналізованих країнах НАТО, існує нагальна потреба відповідного законодавчого забезпечення кібервійськ (кіберсил) в Україні, що передбачатиме підготовку Концепції створення кібервійськ та спеціального закону «Про Кібервійська Збройних Сил України».

Для України у цій площині найбільш оптимальним є впровадження власної організаційної моделі кібервійськ (кіберсил) (*Рис. 1*) з урахуванням внутрішньої специфіки та необхідності консолідації зусиль щодо формування єдиного Кіберкомандування, яке входить до системи Міністерства оборони України. Набувають актуальності й питання посиленого захисту та надання особливого правового статусу цивільним особам у складі кібервійськ, які будуть задіяні для проведення спеціальних кібероперацій та забезпечення кібероборони.

Рис. 1. Інфографіка структури Кіберкомандування в Україні

Дослідницька служба
Верховної Ради України

**Цей документ підготовлений Дослідницькою службою Верховної Ради України як довідковий інформаційно-аналітичний матеріал. Інформація та позиції, викладені в документі, не є офіційною позицією Верховної Ради України, її органів або посадових осіб. Цей документ може бути цитований, відтворений та перекладений для некомерційних цілей за умови відповідного посилання на джерело.*

Додаток 1

Інституційні засади кібервійськ окремих країн-членів НАТО

Країна	Законодавче забезпечення	Інституційна модель
США	Стратегія кібероборони МО США (2018) Таємний Указ Президента США (2018) Національна стратегія кібербезпеки (2023)	Кібернетичне командування «USCYBERCOM» включає 133 команди Сил Національної Кібермісії (CMF), Штаб об'єднаних сил (JFHQ-DODIN), Сили Національної Кібермісії (CNMF), Об'єднану оперативну групу «Ares» та відповідні кіберкомпоненти видів Збройних Сил – Армійського кіберкомандування (ARCYBER), Кіберкомандування Корпусу морської піхоти (MARFORCYBER), Кіберкомандування флоту / Десятий флот (FCC/10F), Кіберкомандування ВПС / 16-та повітряна армія (AFCYBER) і Кіберкомандування берегової охорони (CGCYBER) (2009)
Велика Британія	Військова доктрина (2021) Національна стратегія кібербезпеки (2021)	Національні кіберсили (National Cyber Force) (2020)
Франція	Біла книга з питань національної безпеки і оборони (2013) Декрет Міністра оборони «Про зміни організаційно-штатної структури Збройних Сил» (2017)	Командування кіберзахисту (COMCYBER) у складі Збройних Сил (2017)
Польща	Концепція організації та функціонування Сил оборони кіберпростору (2019) Закон «Про оборону» (2022)	Сили оборони кіберпростору у складі Збройних Сил (2019)