Медіафорум : аналітика, прогнози, інформаційний менеджмент : зб. наук. праць. – Чернівці : Чернівецький нац. ун-т, 2018. – Том 6. – С. 71-93

Mediarorum: Analytics, Forecasts, Information Management: Collection of Research Articles. – Chernivtsi: Chernivtsi National University, 2018. – Vol. 6. – pp. 71-93

УДК: 327(1-622НАТО):004.056

©*ОксанаЗвоздецька*[1]

НОВІ ПІДХОДИ ПІВНІЧНОАТЛАНТИЧНОГО АЛЬЯНСУ (НАТО) У СФЕРІ КІБЕРБЕЗПЕКИ В УМОВАХ ЗАГОСТРЕННЯ ІНФОРМАЦІЙНОГО ПРОТИСТОЯННЯ

Стаття присвячена аналізу сучасної політики НАТО в сфері кібербезпеки в умовах загострення інформаційного протистояння. Дослідниця констатує, що гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки залишаються одним із стратегічних завдань діяльності НАТО, оскільки більшість політичних і військових конфліктів відбуваються або віддзеркалюються, сьогодні, саме у віртуальному просторі.

На Лісабонському саміті в 2010 р. кіберзахист був включений до Стратегічної концепції НАТО «Активне залучення, сучасна оборона», в якій нові виклики в галузі безпеки займають центральне місце. Особливо виділені тероризм, кібератаки, поширення зброї масового знищення (ЗМЗ), вразливість галузі енергетики та екологічні обмеження.

***Ключові слова**: Північноатлантичний Альянс (НАТО), кіберпростір, кіберзагрози, кібербезпека, Сили і засоби реагування НАТО на комп'ютерні інциденти.*

NATO's new strategic concept in cybersecurity issues in the context of up-to-the date vulnerability and threat information

The focus of the article revolves around NATO's roadmap of smart defense against cyber attacks as the bedrock of Euro-Atlantic security. The author discloses NATO'S new policy and cutting-edge technical initiatives, aimed at focusing on countering global threats and cyber security challenges. It is stressed out, that new ideas towards a more synergetic approach between all the NATO Cyber Defense agencies should be explored to develop a shared

[1] Кандидат історичних наук, доцент кафедри міжнародної інформації Чернівецького національного університету імені Юрія Федьковича, Україна, E-mail: zvozdecka.o.j@i.ua

framework for cybersecurity that might provide up-to-the date intelligence in order to ensure the development, acquisition and maintenance of the necessary military capabilities.

The research highlights the core aspects of the 2010 Lisbon Summit that adopted NATO's Strategic Concept 'Active Engagement, Modern Defense: Strategic Concept for the Members of the North Atlantic. Treaty Organization', that recognizes Cyber Defense as one of its strategic priorities. In particular, to foster Allied Nations' cooperative efforts to counter terrorism, cyber attacks, prevent the proliferation of nuclear weapons and other weapons of mass destruction (WMD), Reinforce energy security and environmental constraints.

Develop the capacity to contribute to energy security, including protection of critical energy infrastructure and transit areas and lines, cooperation with partners, and consultations among Allies on the basis of strategic assessments and contingency planning;

In July 2011, NATO Defense Ministers adopted revised NATO Policy on Cyber Defense, which highlighted three areas:

• The principles of subsidiarity and proportionality, which involve the assistance provided only upon request, in any other cases, the principle of self-responsibility of sovereign states is applied;

• Avoiding unnecessary duplication of the structures or capabilities and approaches on the international, regional and national levels;

• Collaboration based on trust, with regard to the potential sensitivity and vulnerability of the system, the access to which has to be given.

After the 2014 Wales Summit, in the revised NATO Cyber Defense Policy, cyber threats were identified as a potential prerequisite for collective defense under the Article 5 of the NATO Treaty.

Noteworthy, Cyber Security is responsible for providing the broad spectrum of services in the following specialist security areas: CIS Security, Cyber Defense, Information Assurance, and Computer & Communications Security. Cyber defense is provided by many Alliance bodies: any NATO response concerning collective defense against cyber attacks will be subordinated to the North Atlantic Council (NAC), The Cyber Defense Committee (CDC) – the leading advisory body of the NAC. The executive level is represented by The Cyber Defense Management Board (CDMB), NATO Communications and Information Agency (NCI Agency), Cyber Security incorporates the NATO Computer Incident Response Capability (NCIRC) Technical Centre, providing specialist services to prevent, detect, respond to and recover from cyber

security incidents.

Keywords: *North Atlantic Treaty Organization (NATO), cyberspace, cyber threats, cyber defense, cybersecurity, NATO Computer Incident Response.*

Постановка проблеми. Можливість кібератак розглядається як одна з пріоритетних і ймовірних загроз XXI століття, які зростають як за чисельністю, так і за складністю. Ці загрози посилюється і тим фактом, що потенційний напад може здійснюватися будь-яким актором віртуальної реальності, а наслідки дії можуть призвести до дестабілізації тієї чи іншої країни, втрати здатності до управління та координації дій. Специфічність атак в мережі може мати різний характер та включати, наприклад, інфікування шкідливими програмами, блокування облікових записів електронної пошти, шпигунство, крадіжку даних, блокування телекомунікаційних систем, що може в значній мірі обмежити реальні бойові можливості країни, яка була атакована у віртуальному просторі (Wodnicki 2007, 1(8): 179).

Кіберпростір – це не просто сфера, що розширює зону потенційного конфлікту і дозволяє хактивістам, організованим злочинцям і терористам процвітати. Кіберпростір – це не просто цифровий маршрут здійснення атак. Це також засіб для відмивання злочинними елементами грошей та обміну інформацією тактичного характеру. Крім того, комп'ютерна взаємозалежність між виробниками і споживачами створює поле для промислового і політичного шпигунства на шкоду інтересам держави. Всі ці загрози неможливо відобразити силами лише однієї структури забезпечення безпеки, і цей факт підвищує значущість міжнародного співробітництва у сфері міжнародної інформаційної безпеки. Співпраця означає не тільки обмін технічними знаннями і досвідом, а й формування політики, підвищення рівня обізнаності та координації зусиль. Вирішальне значення для взаєморозуміння мають навчальні програми, обміни передовим досвідом між політиками, розробниками і державними службовцями. Тому гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки залишаються одним із стратегічних завдань діяльності НАТО, оскільки більшість політичних і військових конфліктів відбуваються або віддзеркалюються саме у віртуальному просторі.

Заступник Генерального секретаря НАТО пані Геттемюллер говорила про надзвичайну важливість кіберзахисту, коли, 19 жовтня 2017 р., звернулась до представників цієї галузі на Симпозіумі НАТО

з інформаційного забезпечення (NIAS) в рамках Кіберконференції в м. Монс, Бельгія[1]. Вона відзначила, що «кібератаки – це дуже серйозно, вони потенційно можуть завдати шкоди місіям НАТО у всьому світі і послабити нашу здатність забезпечувати колективну оборону. Саме тому кіберзахист перебуває серед найголовніших пріоритетів НАТО і країн – членів Альянсу» (Заступник Генерального секретаря НАТО, 2017).

Аналіз останніх досліджень і публікацій. З українських дослідників, що висвітлювали окремі аспекти даної проблеми, слід виокремити роботи заавідувача відділу інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень, доктора політичних наук Д.В. Дубова, кандидата історичних наук Т.В. Брежнєвої, кандидата політичних наук Н.Б. Бєлоусова, в яких розглянуто політику НАТО у сфері кіберзахисту до 2012 р. Охарактеризовано основні принципи, шляхи реагування на нові виклики і напрями співпраці як складники політики НАТО з протистояння загрозі кібернападів. Цікавим, на нашу думкує, є аналіз підходів НАТО та ЄС до кібербезпеки який подано у дослідженні Піpет Пернік (Pernik, 2014) наукового співробітника аналітичного центру Естонії «Міжнародний центр оборони та безпеки» (International Centre for Defence and Security (ICDS). Її дослідження зосереджені на політичних та стратегічних аспектах кібербезпеки.

Метою даної статті є аналіз сучасної політики НАТО в сфері кібербезпеки в умовах загострення інформаційного протистояння.

Виклад основного матеріалу. Вперше рішення про необхідність розробки комплексної програми з кіберзахисту було прийнято Альянсом у 2002 р. під час Празького саміту, на якому було прийнято рішення про створення Технічного центру Сил і засобів реагування НАТО на комп'ютерні інциденти (NATO Computer Incident Response Capa bility – NCIRC) як першого етапу Програми. Зусилля НАТО у сфері кіберзахисту були зосереджені на захисті систем зв'язку, що належать і експлуатуються Альянсом.

Три тижні масованих кібернападів на Естонію в 2007 р. продемонстрували, що країни - члени НАТО незахищені на кіберфронті. Лише

[1] Щорічний Кіберсимпозіум НАТО проводить Агентство зв'язку і інформації НАТО. Він надає кіберфахівцям з НАТО і країн-членів, а також представникам галузі можливість обговорити найновіші досягнення у сфері комп'ютерних технологій, а також загрози і виклики, пов'язані з цим.

ці події змусили Альянс радикально переглянути свій підхід до політики кіберзахисту і вивести засоби протидії на новий рівень. Таким чином, Альянс вперше офіційно звернувся до політики кіберзахисту НАТО, в 2008 р. в якій виокремлюють три основні напрями:

- субсидіарність, тобто, допомога надається лише на прохання, в інших випадках застосовується принцип власної відповідальності суверенних держав;
- уникнення зайвого дублювання структур або сил і засобів – на міжнародному, регіональному і національному рівнях;
- співпраця, що ґрунтується на довірі, зважаючи на делікатний характер інформації про систему, до якої має бути наданий доступ, і можливу вразливість (Novi zahrozy, 2011).

Вже 2 квітня 2009 р. штаб-квартира НАТО розповсюдила документ «Рамки для співробітництва у питаннях кібернетичного захисту між НАТО та державами-партнерами». Цей відкритий для держав-партнерів документ став логічним продовженням низки документів доктринального характеру, які визначили політику НАТО щодо кібернетичного захисту, але мали закритий характер.

Мета документу полягає у визначенні рамок для співробітництва між НАТО та країнами-партнерами і міжнародними організаціями у питаннях кібернетичного захисту. У зв'язку з цим, документ визначає завдання, цілі, принципи та потенційні сфери співробітництва, а також механізми та процедури їхньої імплементації.

Згідно з документом, головним елементом політики НАТО у сфері кібернетичного захисту є принцип, що держави – члени Альянсу несуть пряму відповідальність за захист їх національних комунікацій та інформаційних систем, але НАТО повинна мати спроможності для підтримки союзників, які стали жертвою кібернетичних атак національного значення (Framework for cooperation, 2009).

На Лісабонському саміті в 2010 р. кіберзахист був включений до Стратегічної концепції НАТО «Активне залучення, сучасна оборона» (Active Engagement, Modern Defence, 2010), а декларація саміту призвела до оновлення політики в галузі кіберзахисту в 2011 р. та створення додаткового Плану дій в 2012 р. В новій Стратегічній концепції НАТО нові виклики в галузі безпеки займають центральне місце. Особливо виділені тероризм, кібератаки, поширення зброї масового знищення (ЗМЗ), вразливість галузі енергетики та екологічні обмеження. Причина цього не в тому, що ці поняття покрива-

ють весь спектр нових загроз, а те, що в цих сферах потенціал НАТО, військовий за своєю суттю, може істотно підвищити ефективність міжнародних зусиль у цьому напрямку. Стратегічна концепція також закликає НАТО здійснювати моніторинг і аналіз міжнародної обстановки для прогнозування криз з метою їх запобігання.

Стаття 12 Стратегічної концепції зазначає, що «Кібератаки стають все більш частими, більш організованими і більш збитковими для державних установ, підприємств, економіки і, можливо, також транспортній та електричній мережам та інших об'єктів критичної інфраструктури; вони можуть досягти критичного рівня, який загрожує національному та Євроатлантичному процвітанню, безпеці і стабільності. Джерелом таких атак можуть бути іноземні військові та розвідувальні служби, організовані злочинні угруповання, терористичні та/або екстремістські групи» (Стратегічна концепція, 2010).

Для посилення захисту від зазначених загроз, в статті 19, члени Альянсу зобов'язуються «розвивати й надалі наші можливості щодо запобігання, виявлення, захисту і відновлення від кібератак, у тому числі шляхом використання процесу планування НАТО для поліпшення і координації національних можливостей з кіберзахисту, охоплюючи усі органи НАТО централізованим кіберзахистом, а також краще інтегруючи кіберобізнаність, попередження і реагування НАТО з державами-членами Альянсу» (Стратегічна концепція, 2010).

17 вересня 2014 р. НАТО започаткувала офіційну ініціативу щодо значного посилення співпраці з приватним сектором з питань електронних загроз та викликів. Віртуальне партнерство в галузі промисловості «Cyber Partnership» (NICP) було представлено близько 1500 фахівцям з інформаційних технологій на дводенній кіберконференції НАТО в Монсі, Бельгія. NICP було схвалено на саміті НАТО в Уельсі 28 країнами-членами Альянсу. Він визнає важливість співпраці з партнерами у сфері промисловості, для обміну інформацією, досвідом та експертними знаннями для протидії кіберзагрозам. «Технологічні інновації та досвід приватного сектору мають вирішальне значення», – сказав заступник Генерального секретаря НАТО з питань нових викликів безпеці, посол Сорін Дукару в презентації ініціативи «Співпраця з промисловістю через NICP» – це найважливіший спосіб зміцнення нашої кібернетичної спроможності» (NATO launches Industry, 2014).

Важливою датою для НАТО став березень 2015 р., коли Генеральний секретар Альянсу Йенс Столтенберг офіційно визнав, що кіберзагрози визначаються як потенційна причина для колективної оборони відповідно до статті 5 Договору НАТО (Pernik, 2014). Колективна безпека – це складне ключове завдання НАТО, яка підкреслює важливість скоординованих зусиль, встановлення єдиних стандартів і обмін критично важливою інформацією, що стосується спільних загроз.

Варшавський саміт відбувся майже через два роки після саміту Уельсу, 8-9 липня 2016 р., на якому НАТО визнала, що міжнародне право застосовується до кіберпростору, і що кіберзахист є частиною основного завдання колективної оборони НАТО. Згідно з Варшавським комюніке, члени Альянсу взяли на себе зобов'язання «посилити кіберзахист [їх] національних мереж та інфраструктур у першочерговому порядку». Вони покращують свої національні можливості для реагування на кібератаки, в тому числі в гібридних контекстах, і можливості НАТО будуть проходити «безперервну адаптацію» (Minárik, 2017).

Значну увагу було приділено у Варшаві також співпраці між НАТО та ЄС. Сторони підписали Спільну декларацію, в якій чітко визначено основні проблеми кіберзахисту. Ще 10 лютого 2016 р. було підписано Технічну угоду між Технічним центром Сил реагування НАТО на комп'ютерні інциденти (NATO Computer Incident Response Capability NCIRC) та Комп'ютерною командою з реагування на надзвичайні ситуації в Європі (CERT-EU) (її текст не є загальнодоступним). Згідно з новинами Фінляндії «Yle TV», НАТО та ЄС розглядають створення центру захисту від гібридних загроз у квітні 2016 р. Три країни ЄС (Австрія, Фінляндія та Швеція), які не є членами НАТО, вже надають штаб-квартири та ресурси міжнародному Центру передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) м. Таллін, демонструючи, що вони цінують співробітництво в галузі кібероборони з членами НАТО (Гарднер, 2017, 48). Отже, на Варшавському саміті кібернетична оборона була чітко визначена і пов'язана з захистом від гібридних загроз.

Зі 143 проектів НАТО три присвячені кібернетичному захисту:

1. Багатонаціональний проект «Розвиток здатності до кіберзахисту» (Multinational Cyber Defence Capability Development Project MNCD2), спрямований на полегшення обміну конфіденційною ін-

формацією, поліпшення ситуації усвідомлення та здатность виявляти шкідливу активність. П'ять держав-засновниць цієї ініціативи, (Канада, Данія, Норвегія, Румунія та Нідерланди) розробили «Кібер-систему координації інформації та інцидентів» (Cyber Information and Incident Coordination System CIICS). Після завершення першого робочого етапу, що стосувався обміну технічною інформацією про кіберзахист, Рада MN CD2 погодилася запропонувати можливість використання системи CIICS в рамках програми «Cyber Coalition 2014» іншим країнам-членам НАТО (MN CD2 Nations offer, 2014.)

2. Платформа для спільного користування інформацією про шкідливе середовище (The Malware Information Sharing Platform MISP) полегшує обмін про технічні характеристики шкідливого програмного забезпечення в межах довіреної спільноти без необхідності ділитися інформацією про атаки.

3. Трансатлантична оборонно-технологічна та промислова співпраця – це партнерство з промисловістю (Piret , 2014, 7).

Умовно, діяльність НАТО в сфері кібербезпеки можна розподілити на два напрями. Першим, пріоритетним напрямом є захист своїх власних мереж. Це складне завдання, зважаючи на широку присутність Альянсу на різних сайтах і оперативних об'єктах за різноманітних умов – від метрополії Брюсселя до жорсткого середовища пустелі, де НАТО повинна забезпечити захист усіх своїх інформаційно-комунікаційних систем, на які Альянс покладається у своїх операціях і місіях, від кіберзагроз.

Другим пріоритетним напрямом діяльності НАТО є допомога своїм членам з розвитку власних сил і засобів кіберзахисту. Це робиться різними способами, в тому числі через дворічний процес визначення колективних цілей кіберзахисту, які кожен член Альянсу має підтримати, наприклад, розроблення стратегії кіберзахисту. Процес досягнення цих спільно узгоджених цілей регулярно переглядається. На додаток, НАТО пропонує широкий спектр освітніх, тренувальних і навчальних можливостей за допомогою різноманітних освітніх установ, серед яких школа НАТО в Обераммергау і Кіберакадемія, створення якої заплановане в Португалії. Акредитований НАТО Центр передового досвіду з кіберзахисту в Таллінні також відіграє важливу роль в цьому сенсі.

Кібернетична оборона здійснюється цілою низкою органів НАТО. Перш за все, будь-яка реакція НАТО щодо колективної оборони на

кібернетичні напади буде підпорядкована Північноатлантичній раді (North Atlantic Council NAC), яка є верховним органом НАТО, що складається з представників усіх держав-членів та під головуванням Генерального секретаря.

Керівний Комітет з кіберзахисту (The Cyber Defence Committee CDC), до квітня 2014 р., відомий як Комітет оборонної політики та планування (кіберзахист), є провідним дорадчим органом Північноатлантичної ради (NAC) у питаннях кіберзахисту, а також проводить консультації з членами Альянсу та здійснює загальне керівництво внутрішнього кіберзахисту НАТО.

Виконавчий рівень представляє Відомство з управління кіберзахистом (The Cyber Defence Management Board DMB) – головний орган НАТО, що здійснює нагляд за кібербезкою НАТО, відповідає за координацію всієї кібероборони, особливо з огляду на співпрацю між цивільними і військовими установами; здійснює стратегічне планування та керівництво щодо мереж НАТО, також підписує меморандуми про взаєморозуміння з державами-членами для полегшення обміну інформацією та координації допомоги.

Агентство з питань обслуговування систем інформації та зв'язку НАТО (NATO Communications and Information Agency NCIA) створене 1 липня 2012 р. відповідно до мети, викладеної на Лісабонській зустрічі на вищому рівні, шляхом об'єднання 7 агентств НАТО, що займалися проблемами комунікації, інформаційних систем та кібератівності.

Технічний Центр реагування НАТО на комп'ютерні інциденти (NATO Computer Incident Response Capability NCIRC) став мозковим вузлом боротьби Альянсу проти кіберзлочинності. NCIRC відповідає за кіберзахист усіх інформаційних ресурсів НАТО, незалежно від того, належать вони постійним штабам, чи штабам розгорнутим на час операцій чи навчань (Dereń, 2014, 14). На початку 2012 р. НАТО підписала контракт вартістю 67 млн. доларів США з італійською компанією Finmeccanica на розробку, впровадження й обслуговування програми кіберзахисту NCIRC. У рамках угоди італійська компанія забезпечить інформаційну безпеку приблизно 30 важливим об'єктам і штаб-квартирам НАТО у 28 країнах світу (Марков, 2014, 120).

Будь-яка країна-член НАТО, яка постраждала від серйозного кібернападу, зможе звернутися до НАТО по допомогу. Такий запит розгляне Відомство з управління кіберзахистом (CDMB). Прохання

про допомогу, які надходитимуть від країн – не членів НАТО, крім CDMB затверджуватися ще й Північноатлантичною радою. У разі приведення в дію Групи швидкого реагування, НАТО зможе відреагувати на інцидент протягом 24 годин.

Ще однією організацією, яка має акредитацію НАТО і формально не входить до командної структури, однак має величезний вплив на дії Альянсу в сфері кіберзахисту – Центру передового досвіду з кіберзахисту НАТО (NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) в Естонії (м. Таллінн). У Брюсселі 14 травня 2008 р. був підписаний меморандум про створення такого Центру сімома країнами і надання йому статусу міжнародної військової організації. Завдяки його потужностям Естонія стала однією з найбільш захищених від кібератак країною в ЄС. У квітні 2018 р. Португалія вже стала 21 членом цього Центру (Tallinn-based NATO, 2018).

Унікальна специфіка кіберпростору і операцій в цьому середовищі викликають нові складні питання для фахівців: складність у визначенні ініціаторів нападу, відсутність конкретних даних, а також використання кіберпростору в якості середовища, яке в основному використовується для цивільних цілей і управляється цивільними органами для здійснення військових функцій.

Для вирішення цих складних правових питань в 2009 р в Центрі зібралася група з двадцяти дослідників і практиків зі світовим ім'ям з Кембриджського Університету, ряду американських і європейських дослідницьких центрів під керівництвом професора Майкла Шмітта. Ними було розроблено правове керівництво з метою пояснити, як міжнародне право можна застосувати до кібероперацій з найсерйознішими наслідками, даючи можливість для самооборони, а також інших дій, що здійснюються під час збройного конфлікту. Їх робота була опублікована в 2013 р. під назвою «Таллінське керівництво з міжнародного права, що застосовується при веденні кібервійни» («Tallinn Manual on the International Law Applicable to Cyber Warfare»).

Особливу увагу «Таллінн Меньюал» приділяє Jus ad bellum – (норми міжнародного права, що регулюють правомірність застосування сили у міжнародних відносинах), і jus in bello – норми міжнародного права, що регулює поведінку під час збройного конфлікту (також його називають «законом війни», законом про збройний конфлікт або частиною міжнародного гуманітарного права) (Синглтон, 2014, 45).

Згідно з цим документом, кіберпростір – це середовище, створене фізичними та нефізичними компонентами що характеризується використанням комп'ютерів та електромагнітного спектру для зберігання, модифікації та обміну даними за допомогою комп'ютерної мережі (Klimburg, 2012).

Документ отримав різні оцінки. Одні вважають, що «Талліннське керівництво» – не більш ніж експертна праця, яка носить рекомендаційний характер. Інші впевнені, що натівський документ фактично відкриває дорогу широкому використанню інформаційної зброї, обґрунтовуючи необхідність жорсткої відповіді на кібератаки аж до введення економічних ембарго, банківських санкцій і навіть застосування звичайних і ядерних озброєнь для фізичного знищення тих, хто такі атаки зробив (Кранс , 2013). Більше того, розуміючи, що країни стикаються з проблемою того, що кібероперації не досягають рівня збройного нападу, який дає можливість самооборони, центром був ініційований проект під назвою «Таллінн 2.0». Даний проект спрямований на вирішення питань про те, як міжнародне право має розглядати ворожі операції меншого калібру, які, тим не менш, наносять країнам значного збитку. Наприклад, це можуть бути серйозні фінансові втрати, неможливість доступу до життєвоважливих Інтернет-послуг та ін. В рамках проекту також будуть розглянуті зобов'язання, які міжнародне право поширює на держави, а також їх застосування в контексті кіберсфери (Вихул, 2014, 12).

Друге видання «Талліннського керівництва» було опубліковано в лютому 2017 р. та охоплює весь спектр міжнародного права, що застосовується до кібероперацій як в мирний час, так і під час збройного конфлікту. Дає аналіз широкого кола принципів міжнародного права і режими, що регулюють події в кіберпросторі, включають принципи загального міжнародного права, такі як суверенітет та різні підстави для здійснення юрисдикції (Schmitt, 2017).

Катаріна Ціолковська, міністр оборони Німеччини зазначала, що, «з урахуванням ймовірного непрямого і таємного використання в деяких країнах проксі-серверів патріотично налаштованими хакерами (хактивістами), залучити країну до відповіді за кібердіяльність на юридичних підставах в рамках міжнародної юрисдикції і наукових теорій буде дуже складно, мова йде про неможливість перевірити, чи є у такої країни «ефективний» або «повний» контроль над діяльністю її недержавних суб'єктів» (Синглтон, 2014, 45).

Крім курсу з міжнародного права щодо кібероперацій, Центром передового досвіду з кіберзахисту НАТО була розроблена значна програма курсів технічного характеру. Подібні курси стосуються таких питань як моніторинг мережевого трафіку та облік заходів у сфері безпеки, відновлення системи, яка постраждала від шкідливих програм і розгляд того, як системи інформаційних технологій піддаються нападам і як можна знизити збиток від таких нападів. Враховуючи високий рівень зацікавленості такими курсами, пріоритет віддається слухачам з країн-спонсорів Центру. Вільні місця пропонуються слухачам з країн НАТО, а також представникам Австралії, Австрії, Фінляндії, Ірландії, Новій Зеландії, Швеції та Швейцарії (Крутов, 2012, 65).

Щороку в червні Центр організовує велику міжнародну конференцію, присвячену кібербезпеці під назвою «САЙКОН» (CyCon). Конференція покликана обговорювати міждисциплінарні питання, в ній беруть участь більше 500 фахівців в галузі стратегії, права, етики, інформаційних технологій із цивільних та військових відомствах. САЙКОН надає унікальну можливість для обміну професійним досвідом та встановлення контактів. 10 Міжнародна ювілейна конференція з кіберконфлікту CyCon 2018 проходила в Талліні з 30 травня по 1 червня 2018 р., в якій взяло участь близько 700 експертів з кібербезпеки з більше ніж 40 країн, і була присвячена темі посилення впливів в кіберсфері (CyCon 2019 Theme, 2018).

«Зімкнуті щити» («Locked Shields»), навчання з мережевого захисту, яку центр проводить в режимі реального часу, є найбільш очікуваною подією року серед професіоналів з безпеки. Назва навчання «Locked Shields» (Зімкнуті щити) означає стародавній спосіб оборони на полі бою. Якщо тільки один солдат тримає щит, то він захищений тільки з одного боку, пояснив у своєму відеозверненні фахівець з кібербезпеки Центру передових технологій з кібероборони НАТО (CCDCOE) Рейн Оттіс під час навчань 2012 р. Але тісно згуртувавши щити, кілька солдатів можуть захистити вразливі місця кожного з них. «Якщо вас багато, то зімкнуті щити створять непереборну стіну. Саме цю думку ми й хочемо донести до вас - Необхідно працювати разом. Нам треба зімкнути щити і захищати один одного» (Обеспечение безопасности, 2014, 53).

Ще одним кроком у посиленні співпраці НАТО з ЄС є відкриття 2 жовтня 2017 р. у столиці Фінляндії Гельсінкі Європейського цен-

тру протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats). Ця структура покликана допомогти протистояти новим загрозам, спрямованим на дестабілізацію ситуації у європейських державах. Засновниками центру стали 12 країн ЄС і НАТО: Фінляндія, Швеція, Норвегія, США, Франція, ФРН, Великобританія, Іспанія, Польща, Естонія, Латвія і Литва.

Як раніше заявили представники нової структури, її метою є не пряма боротьба проти атак, а дослідницька робота. НАТО і Євросоюз спільно об'єдналися для того, щоб протидіяти гібридним загрозам. Увага під час роботи нового центру буде зосереджена на формуванні адаптивної стійкості щодо загроз, починаючи від «зелених чоловічків» і до протидії гуманітарним катастрофам. Даний центр стане першою подібною установою за участю ЄС, який сформований разом із НАТО, незважаючи на те, що Північноатлантичний альянс має близько двох десятків подібних центрів.

За словами Столтенберга, «гібридною загрозою» є «поєднання воєнних і невоєнних засобів агресії, сукупність відкритих і таємних заходів і кроків від пропаганди і дезінформації і до використання парамілітарних формувань, від твітів до танків» (Новий центр, 2017). Як наслідок, новий Європейський центр протидії гібридним загрозам буде постійно займатися аналізом різноманітних типів атак, які здійснюються проти Європи і США, а також буде вираховувати, як найкраще їм протидіяти.

На семінарі, присвяченому відкриттю центру, зазначалося, що гібридну небезпеку становлять не тільки окремі держави, а й терористичні та кримінальні організації. Однак помічник генерального секретаря НАТО з питань розвідки і безпеки Арндт Фрайтаґ фон Лорінґгофен (Arndt Freytag von Loringhoven) згадав у зв'язку з цим лише одну державу – Росію. «Росія – одна з головних країн, за якою ми спостерігаємо. В якості прикладів можна навести анексію Криму, події в Східній Україні і кібератаки проти Демократичної партії США», – зазначив він (У Гельсінкі відкрили Європейський центр, 2017.).

8 листопада 2017 р. міністри оборони країн-членів Північноатлантичного альянсу схвалили рішення про створення нової структури – Центру кібероперацій. Наразі триває розробка концепції нової командної структури НАТО й в рамках цього процесу було ухвалене відповідне рішення. Пан Столтенберг наголосив, що Центр кібероперацій буде військовою структурою, оскільки кібератаки нині ста-

новлять серйозну загрозу для безпеки країн-членів альянсу. «Я вірю, що надалі в будь-якому військовому конфлікті буде кіберскладова. Через це нам необхідно інтегрувати наші кіберможливості... Ми по винні бути в кіберсфері настільки ж ефективними, як на землі, на морі та в повітрі», –заявив генеральний секретар НАТО («У НАТО затвердили, 2018).

14 лютого 2018 р. Міністри оборони країн-членів НАТО затвердили рішення про створення ще двох нових командних структур, два нових центри планування та управління операціями НАТО. Один з нових командних центрів буде відповідати за перекидання військ і озброєнь по європейському континенту, інший - за операції військово-морських сил в Атлантичному океані. Рішення щодо місцезнаходження нових структур і кількості персоналу буде прийнято в червні.

Три десятки років тому НАТО мав 33 командних центри, де працювали 22 тисячі співробітників. На сьогодні таких центрів є лише сім. Втім, Альянс чудово усвідомлює зростання загрози від Росії і саме через неї змінює свою структуру. В НАТО пояснюють ці зміни необхідністю відповідати на всі сучасні загрози, але виокремлюють ключові – Росію, тероризм та кібератаки.

На тлі подальшого загострення кризи в Україні НАТО поступово збільшила практичну підтримку країни у рамках Особливого партнерства Україна – НАТО, заснованого у 1997 р. Ініціативи, ухвалені Альянсом, передбачають низку невідкладних і короткострокових заходів, спрямованих на те, щоб допомогти Україні впоратися із по точною кризою, а також довгострокових заходів щодо нарощування потенціалу, розбудови оборонних спроможностей й реформування Збройних сил і структур безпеки.

Відповідно, держави – члени Альянсу ухвалили п'ять нових проектів Цільових фондів для розвитку командування, управління, зв'язку і комп'ютеризації (С4), матеріально-технічного забезпечення і стандартизації, захисту від кібернетичних злочинів, соціальної адаптації колишніх військовослужбовців, а також реабілітації військовослужбовців, які зазнали поранень. Ці проекти Цільових фондів запроваджуватимуться на додаток до вже існуючих програм НАТО в Україні, таких як Програма військової освіти, професійного розвитку, управління сектором безпеки і науково-технічного співробітництва з питань безпеки. У 2014 році Україна стала лідером за кількістю грантів, отриманих у рамках програми НАТО «Наука зара-

ди миру і безпеки» (НМБ). На період 2014 – 2017 років було ухвалено 15 нових проектів, загальна вартість яких оцінюється у десять мільйонів євро (Щорічний звіт, 2015, 18-19.). На виконання зазначених ініціатив були розроблені Річні Національні програми співробітництва Україна–НАТО на 2015 р., 2017 р., 2018 р.

На прохання України у червні 2015 р. Альянс погодився започаткувати шостий цільовий фонд для протидії саморобним вибуховим пристроям та розмінування. Один з цих шести фондів покликаний боротися з кіберзлочинністю і спрямований на розвиток систем кібербезпеки відповідно до найпрогресивніших стандартів країн – членів НАТО. Внески в цей фонд здійснюють такі країни як Румунія, Албанія, Естонія, Угорщина, Італія, Португалія, Туреччина, Сполучені Штати.

Проект передбачає допомогти Україні в розробці технічних сил та засобів для протидії кіберзагрозам. Допомога включатиме створення Центру реагування на кіберінциденти для відстеження ситуації в сфері кібербезпеки та лабораторій для розслідування випадків кібернападів. Одним з таких центрів став Ситуаційний центр протидії кіберзагрозам СБУ (СЦПК), створений 25 січня 2018 р. на базі Департаменту контррозвідувального захисту інтересів держави в сфері інформаційної безпеки Служби безпеки України. Україні надано навчальні програми з застосування цих технологій та обладнання, а також практичні рекомендації з розробки належної стратегії. Проект розрахований на 24 місяці з загальним обсягом фі нансування 815 тис. євро. У квітні 2015 р. Естонія виділила на діяльність трастового фонду НАТО для підтримки кібербезпеки в Україні 100 тис. євро, решту – інші країни Альянсу (Підтримка України, 2016).

Висновки. Отже, за останні роки НАТО досяг значних успіхів в розширенні своєї ролі в питаннях протидії новим викликам безпеці. Була прийнята оновлена «Політика кіберзахисту» і пов'язаний з нею «План дій». Технічний центр Сил реагування НАТО на комп'ютерні інциденти NCIRC (NATO Computer Incident Response Capability) став мозковим вузлом боротьби Альянсу проти кіберзлочинності. NCIRC відповідає за кіберзахист усіх інформаційних ресурсів НАТО, незалежно від того, належать вони постійним штабам, чи штабам розгорнутим на час операцій чи навчань.

Дивлячись у майбутнє, Альянс визнає, що кіберзагрози і кібернапади стають дедалі частішими, дедалі складнішими і потенційно

шкідливішими. У намаганні протистояти викликам у галузі кіберзахисту, які дедалі зростають НАТО зосереджує свою увагу на таких аспектах кіберполітики як захист своїх власних мереж, допомога своїм членам з розвитку власних сил і засобів кіберзахисту та запровадження широкого спектру освітніх, тренувальних і навчальних можливостей за допомогою різноманітних освітніх установ Альянсу.

Джерела та література:

1. Бєлоусова, Наталія. 2011. «Основні вимоги НАТО щодо забезпечення безпеки інформаційного простору». Актуальні проблеми міжнародних відносин 102 (ч. 1): 195-202. http://journals.iir.kiev.ua/index.php/apmv/article/view/2165/1928 (accessed April 12, 2018).

2. Брежнєва, Тетяна. 2012. «Політика НАТО з кіберзахисту та співробітництво з партнерами». Стратегічні пріоритети 4 (25): 189-194. http://sp.niss.gov.ua/content/articles/files/28-1440150881.pdf (accessed April 12, 2018).

3. Вихул, Лиис. 2014. «Стремление к передовому опыту в киберсфере». per Concordiam 5 (2): 10-13. http://perconcordiam.com/percon-rus-v5n2/ (accessed April 12, 2018).

4. Гарднер, Джозеф Н. 2017. «Совместная безопасность в НАТО». per Concordiam 8 (1): 46-51. http://perconcordiam.com/perCon_V8N1_RUS.pdf (accessed April 12, 2018).

5. Група швидкого реагування НАТО для боротьби проти кібернападів. 2012. http://www.nato.int/cps/uk/natohq/news_85161.htm?selectedLocale=uk

6. Дубов, Дмитро. 2011. «Сучасні тенденції забезпечення кібербезпеки на міжнародному рівні». Стратегічні пріоритети 4 (21): 5-11. http://sp.niss.gov.ua/content/articles/files/1-1441958808.pdf (accessed April 12, 2018).

7. Замікула, Микола. 2009. «Країни Балтії – НАТО: боротьба з кібертероризмом». Вісник Наукового інформаційно-аналітичного центру НАТО Прикарпатського національного університету імені Василя Стефаника 2: 54-58. http://nato.pu.if.ua/journal/2009/2009-12.pdf (accessed April 12, 2018).

8. Заступник Генерального секретаря НАТО взяла участь в Конференції з кібербезпеки. 2017. https://www.nato.int/cps/uk/natohq/news_147863.htm?selectedLocale=uk (accessed April 12, 2018).

9. Кранс, Максим. Кибероружие в арсенале НАТО Атлантисты открывают возможность для нанесения ядерного удара. 2013. http://

nvo.ng.ru/concepts/2013-06-21/1_cyberweapon.html (accessed April 12, 2018).

10. Крутов, Василь. 2012. «Законодавче забезпечення кібернетичної безпеки окремих зарубіжних країн та міжнародно-правовий досвід у цій сфері» Інформаційна безпека людини, суспільства, держави. 2 (9): 64-69. http://www.nbuv.gov.ua/old_jrn/Soc_Gum/iblsd/2012_2/_private/9kvvitf.pdf (accessed April 12, 2018).

11. Марков, В'ячеслав, і Караченцев, О. 2014. «Напрями діяльності НАТО у справі протидії кіберзлочинності». Право і Безпека 4: 119-123. http://nbuv.gov.ua/UJRN/Pib_2014_4_25. (accessed April 12, 2018).

12. Новий центр буде займатися аналізом гібридних атак і розробкою стратегій щодо їх протидії. 2017, 4 жовтня. https://glavcom.ua/news/u-finlyandiji-vidkrito-centr-nato-i-jes-z-vivchennya-gibridnih-zagroz-441621.html (accessed April 12, 2018).

13. Нові загрози: кібервимір. 2011. НАТО Ревю. http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/UK/index.htm

14. Обеспечение безопасности в Интернете Учения специалистов по кибербезопасности «Locked Shields» в Эстонии. 2014. per Concordiam 4 (4): 50-53. http://perconcordiam.com/percon-rus-v4n4/ (accessed April 12, 2018).

15. Онищенко, Юрій. 2018. «Стратегія опору Росії: які реформи чекають на НАТО». Європейська правда. https://www.eurointegration.com.ua/articles/2018/02/14/7077523/ (accessed April 12, 2018).

16. Підтримка України з боку НАТО. 2016. Бюлетень Організація Північноатлантичного договору. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-nato-ukraine-support-ukr.pdf (accessed April 12, 2018).

17. Синглтон, Дэниел. 2014. «Кибернетическое поле боя». per Concordiam. 5 (2): 40-47. http://perconcordiam.com/percon-rus-v5n2/ (accessed April 12, 2018).

18. Стратегічна концепція оборони та безпеки членів Організації Північноатлантичного договору, прийнята главами держав та урядів у Лісабоні, 2010 /Неофіційний переклад. http://www.nato.int/cps/uk/natohq/official_texts_68580.htm?selectedLocale=uk (accessed April 12, 2018).

19. У Києві розпочав роботу Ситуаційний центр забезпечення кібербезпеки. 26 січня 2018. Media Sapiens http://ms.detector.media/

web/cybersecurity/u_kievi_rozpochav_robotu_situatsiyniy_tsentr_zabezpechennya_kiberbezpeki

20. У НАТО затвердили створення двох нових штабів і центру. 2018. 14 лютого. Європейська правда. https://www.eurointegration.com.ua/news/2018/02/14/7077541/

21. Указ Президента України. (2017). Річна національна програма під егідою Комісії Україна – НАТО на 2017 рік. №103/2017. http://www.president.gov.ua/documents/1032017-21670 (accessed April 12, 2018).

22. Указ Президента України. 2015. Про затвердження Річної національної програми співробітництва Україна - НАТО на 2015 рік. № 238/2015. http://zakon5.rada.gov.ua/laws/show/238/2015 (accessed April 12, 2018).

23. Указ Президента України. 2016. Про річні національні програми під егідою Комісії Україна – НАТО. №547/2016. http://www.president.gov.ua/documents/5472016-20862 (accessed April 12, 2018).

24. Указ Президента України. 2018. Про затвердження Річної національної програми співробітництва Україна - НАТО на 2018 рік. № 89/2018. http://www.president.gov.ua/storage/j-files-storage/00/58/62/bd6cdbcf9328901d1d1d8163ae5348c6_1522256231.pdf (accessed April 12, 2018).

25. Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010. – 40 p. http://www.ccdcoe.org/sites/default/files/documents/NATO-101120-StrategicConcept.pdf (accessed April 12, 2018).

26. Dereń, Jerzy, i Rabiak, Anna. 2014. «NATO a aspekty bezpieczeństwa w cyberprzestrzeni». Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Edition: first, Chapter: NATO a aspekty bezpieczeństwa w cyberprzestrzeni, Publisher: Difin, Warszawa: 202-221. https://www.researchgate.net/profile/Jerzy_Deren2/publication/272818724_NATO_a_aspekty_bezpieczenstwa_w_cyberprzestrzeni/links/56b48d5b08ae8cf9c25b67c0/NATO-a-aspekty-bezpieczenstwa-w-cyberprzestrzeni.pdf

27. Framework for cooperation on cyber defence between NATO and partner nations. EAPC (C) D (2009) 0010. 2 April 2009 http://uan.ua/sites/default/files/41210385dod2.pdf

28. Klimburg, Alexander (Ed.) 2012. National Cyber Security Framework Manual. Tallinn: NATO CCD COE Publication. – 253 p. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (accessed April 12, 2018).

29. Minárik, Tomáš. NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. 2017. International Cyber Developments Review (INCYDER). https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html016

30. MN CD2 Nations offer CCIIS for use in Cyber Coalition. 2014. By MN CD2 Project Office, on 4/30/2014. https://mncd2.ncia.nato.int/news/Pages/MN-CD2-Board-Meeting-04.aspx

31. NATO launches Industry Cyber Partnership By Communication 9/18/2014 https://www.ncia.nato.int/NewsRoom/Pages/140918-NATO-launches-Industry-Cyber-Partnership.aspx

32. North Atlantic Treaty Organisation. Resources Organisations .https://ccdcoe.org/nato.html

33. Piret, Pernik. 2014. «Improving Cyber Security: NATO and the EU» International Centre for Defence Studies. https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf

34. Schmitt, Michael (red.) 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations USA: Cambridge University Press http://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

35. Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence Welcomed Portugal as a New Member. 2018. https://ccdcoe.org/tallinn-based-nato-cooperative-cyber-defence-centre-excellence-welcomed-portugal-new-member.html

36. Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales Press Release (2014) 120 http://www.ccdcoe.org/sites/default/files/documents/NATO-140905-WalesSummitDeclaration.pdf

37. Wodnicki, Jacek. 2017. «Bilans wybranych decyzji podjętych w 2016 roku przez Radę Północnoatlantyc-ką podczas szczytu NATO w Warszawie». Ante Portas – Studia nad Bezpieczeństwem 1(8): 171-188. http://anteportas.pl/wp-content/uploads/2017/09/AP.VIII_Wodnicki.pdf

References:

1. Bielousova, Nataliia. 2011. «Osnovni vymohy NATO shchodo zabezpechennia bezpeky informatsiinoho prostoru». Aktualni problemy

mizhnarodnykh vidnosyn 102 (ch. 1): 195-202. http://journals.iir.kiev.ua/index.php/apmv/article/view/2165/1928

2. Brezhnieva, Tetiana. 2012. «Polityka NATO z kiberzakhystu ta spivrobitnytstvo z partneramy». Stratehichni priorytety 4 (25): 189-194. http://sp.niss.gov.ua/content/articles/files/28-1440150881.pdf

3. Vikhul, Liis. 2014. «Stremlenie k peredovomu opytu v kibersfere». per Concordiam 5 (2): 10-13. http://perconcordiam.com/percon-rus-v5n2/

4. Gardner, Dzhozef N. 2017. «Sovmestnaya bezopasnost v NATO». per Concordiam 8 (1): 46-51. http://perconcordiam.com/perCon_V8N1_RUS.pdf

5. Hrupa shvydkoho reahuvannia NATO dlia borotby proty kibernapadiv. 2012. http://www.nato.int/cps/uk/natohq/news_85161.htm?selectedLocale=uk

6. Dubov, Dmytro. 2011. «Suchasni tendentsii zabezpechennia kiberbezpeky na mizhnarodnomu rivni». Stratehichni priorytety 4 (21): 5-11. http://sp.niss.gov.ua/content/articles/files/1-1441958808.pdf

7. Zamikula, Mykola. 2009. «Krainy Baltii – NATO: borotba z kiberteroryzmom». Visnyk Naukovoho informatsiino-analitychnoho tsentru NATO Prykarpatskoho natsionalnoho universytetu imeni Vasylia Stefanyka 2: 54-58. http://nato.pu.if.ua/journal/2009/2009-12.pdf

8. Zastupnytsia Heneralnoho sekretaria NATO vziala uchast v Konferentsii z kiberbezpeky. 2017. https://www.nato.int/cps/uk/natohq/news_147863.htm?selectedLocale=uk

9. Krans, Maksim. Kiberoruzhie v arsenale NATO Atlantisty otkryvayut vozmozhnost dlya naneseniya yadernogo udara. 2013. http://nvo.ng.ru/concepts/2013-06-21/1_cyberweapon.html

10. Krutov, Vasyl. 2012. «Zakonodavche zabezpechennia kibernetychnoi bezpeky okremykh zarubizhnykh krain ta mizhnarodno-pravovyi dosvid u tsii sferi» Informatsiina bezpeka liudyny, suspilstva, derzhavy. 2 (9): 64-69. http://www.nbuv.gov.ua/old_jrn/Soc_Gum/iblsd/2012_2/_private/9kvvitf.pdf

11. Markov, Viacheslav, i Karachentsev, O. 2014. «Napriamy diialnosti NATO u spravi protydii kiberzlochynnosti». Pravo i Bezpeka 4: 119-123. http://nbuv.gov.ua/UJRN/Pib_2014_4_25.

12. Novi zahrozy: kibervymir. 2011. NATO Reviu. http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/UK/index.htm

13. Novyi tsentr bude zaimatysia analizom hibrydnykh atak i

rozrobkoiu stratehii shchodo yikh protydii. 2017, 4 zhovtnia. https://glavcom.ua/news/u-finlyandiji-vidkrito-centr-nato-i-jes-z-vivchennya-gibridnih-zagroz-441621.html

14. Obespechenie bezopasnosti v Internete Ucheniya spetsialistov po kiberbezopasnosti «Locked Shields» v Estonii. 2014. per Concordiam 4 (4): 50-53. http://perconcordiam.com/percon-rus-v4n4/

15. Onyshchenko, Yurii. 2018. «Stratehiia oporu Rosii: yaki reformy chekaiut na NATO». Yevropeiska pravda. https://www.eurointegration.com.ua/articles/2018/02/14/7077523/

16. Pidtrymka Ukrainy z boku NATO. 2016. Biuleten Orhanizatsiia Pivnichnoatlantychnoho dohovoru. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-nato-ukraine-support-ukr.pdf

17. Synhlton, Dənyel. 2014. «Kybernetycheskoe pole boia». per Concordiam. 5 (2): 40-47. http://perconcordiam.com/percon-rus-v5n2/

18. Stratehichna kontseptsiia oborony ta bezpeky chleniv Orhanizatsii Pivnichnoatlantychnoho dohovoru, pryiniata hlavamy derzhav ta uriadiv u Lisaboni, 2010 /Neofitsiinyi pereklad. http://www.nato.int/cps/uk/natohq/official_texts_68580.htm?selectedLocale=uk (accessed April 12, 2018).

19. U Kyievi rozpochav robotu Sytuatsiinyi tsentr zabezpechennia kiberbezpeky. 26 sichnia 2018. Media Sapiens http://ms.detector.media/web/cybersecurity/u_kievi_rozpochav_robotu_situatsiyniy_tsentr_zabezpechennya_kiberbezpeki

20. U NATO zatverdyly stvorennia dvokh novykh shtabiv i tsentru. 2018. 14 liutoho. Yevropeiska pravda. https://www.eurointegration.com.ua/news/2018/02/14/7077541/

21. Ukaz Prezydenta Ukrainy. (2017). Richna natsionalna prohrama pid ehidoiu Komisii Ukraina – NATO na 2017 rik. №103/2017. http://www.president.gov.ua/documents/1032017-21670 (accessed April 12, 2018).

22. Ukaz Prezydenta Ukrainy. 2015. Pro zatverdzhennia Richnoi natsionalnoi prohramy spivrobitnytstva Ukraina - NATO na 2015 rik. № 238/2015. http://zakon5.rada.gov.ua/laws/show/238/2015 (accessed April 12, 2018).

23. Ukaz Prezydenta Ukrainy. 2016. Pro richni natsionalni prohramy pid ehidoiu Komisii Ukraina – NATO. №547/2016. http://www.president.gov.ua/documents/5472016-20862 (accessed April 12, 2018).

24. Ukaz Prezydenta Ukrainy. 2018. Pro zatverdzhennia Richnoi natsionalnoi prohramy spivrobitnytstva Ukraina - NATO na 2018 rik. № 89/2018. http://www.president.gov.ua/storage/j-files-storage/00/58/62/bd6cdbcf9328901d1d1d8163ae5348c6_1522256231.pdf (accessed April 12, 2018).

25. Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010. – 40 p. http://www.ccdcoe.org/sites/default/files/documents/NATO-101120-StrategicConcept.pdf (accessed April 12, 2018).

26. Dereń, Jerzy, i Rabiak, Anna. 2014. «NATO a aspekty bezpieczeństwa w cyberprzestrzeni». Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku, Edition: first, Chapter: NATO a aspekty bezpieczeństwa w cyberprzestrzeni, Publisher: Difin, Warszawa: 202-221. https://www.researchgate.net/profile/Jerzy_Deren2/publication/272818724_NATO_a_aspekty_bezpieczenstwa_w_cyberprzestrzeni/links/56b48d5b08ae8cf9c25b67c0/NATO-a-aspekty-bezpieczenstwa-w-cyberprzestrzeni.pdf

27. Framework for cooperation on cyber defence between NATO and partner nations. EAPC (C) D (2009) 0010. 2 April 2009 http://uan.ua/sites/default/files/41210385dod2.pdf

28. Klimburg, Alexander (Ed.) 2012. National Cyber Security Framework Manual. Tallinn: NATO CCD COE Publication,. – 253 p. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (accessed April 12, 2018).

29. Minárik, Tomáš. NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. 2017. International Cyber Developments Review (INCYDER). https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html016

30. MN CD2 Nations offer CCIIS for use in Cyber Coalition. 2014. By MN CD2 Project Office, on 4/30/2014. https://mncd2.ncia.nato.int/news/Pages/MN-CD2-Board-Meeting-04.aspx

31. NATO launches Industry Cyber Partnership By Communication 9/18/2014 https://www.ncia.nato.int/NewsRoom/Pages/140918-NATO-launches-Industry-Cyber-Partnership.aspx

32. North Atlantic Treaty Organisation. Resources Organisations .https://ccdcoe.org/nato.html

33. Pernik, Piret, 2014. «Improving Cyber Security: NATO and the EU» International Centre for Defence Studies. https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf

34. Schmitt, Michael (red.) 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations USA: Cambridge University Press http://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

35. Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence Welcomed Portugal as a New Member. 2018. https://ccdcoe.org/tallinn-based-nato-cooperative-cyber-defence-centre-excellence-welcomed-portugal-new-member.html

36. Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales Press Release (2014) 120 http://www.ccdcoe.org/sites/default/files/documents/NATO-140905-WalesSummitDeclaration.pdf

37. Wodnicki, Jacek. 2017. «Bilans wybranych decyzji podjętych w 2016 roku przez Radę Północnoatlantyc-ką podczas szczytu NATO w Warszawie». Ante Portas – Studia nad Bezpieczeństwem 1(8): 171-188. http://anteportas.pl/wp-content/uploads/2017/09/AP.VIII_Wodnicki.pdf