МІЖНАРОДНІ АСПЕКТИ БЕЗПЕКИ КІБЕРПРОСТОРУ

СЕРГІЙ ФЕДОНЮК

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ

Сергій Федонюк

МІЖНАРОДНІ АСПЕКТИ БЕЗПЕКИ КІБЕРПРОСТОРУ

МОНОГРАФІЯ

Електронне видання на CD-ROM

Луцьк
Вежа-Друк
2022

УДК 351.746:004.9.056
Ф 32

Рекомендовано вченою радою
Волинського національного університету імені Лесі Українки
(протокол № 6 від 28 квітня 2022 р.)

Рецензенти:

Карпчук Н. П. − доктор політичних наук, професор, завідувач кафедри міжнародних комунікацій та політичного аналізу Волинського національного університету імені Лесі Українки;

Юськів Б. М. – доктор політичних наук, професор кафедри економіки та управління бізнесом Рівненського державного гуманітарного університету.

Федонюк Сергій
Ф 32 Міжнародні аспекти безпеки кіберпростору : монографія / С. В. Федонюк. – Луцьк : Вежа-Друк, 2022. – 1 електрон. опт. диск (CD-ROM). – Об'єм даних 4,72 Мб.

ISBN 978-966-940-406-0

У книзі розглянуто питання політики щодо забезпечення інформаційної (кібер) безпеки, її витоків і цілей із точки зору міжнародного співробітництва. На основі текстів, опублікованих автором у наукових часописах упродовж 2021-2022 рр., у яких викладено результати досліджень політики й міжнародної діяльності основних міжнародних акторів у сфері інформаційної (кібер) безпеки – США, Росії, Китаю, Європейського Союзу. Для тих, хто цікавиться міжнародними відносинами, студентів, дослідників.

УДК 351.746:004.9.056

ISBN 978-966-940-406-0

ЗМІСТ

ВСТУП 4

Розділ 1. КІБЕРПРОСТІР: ЗАГРОЗИ Й КОНЦЕПЦІЇ БЕЗПЕКИ 10

1.1. Кіберзлочинність і кібертероризм 10

1.2. Інформаційні й кібер-війни 19

1.3. Інформаційна (кібер) безпека 31

1.4. Кібер-війни й міжнародне право 41

Розділ 2. НАЦІОНАЛЬНІ Й РЕГІОНАЛЬНІ ПІДХОДИ ДО БЕЗПЕКИ КІБЕРПРОСТОРУ 51

2.1. Підхід Росії 51

2.2. Підхід Китаю 63

2.3. Підхід США 74

2.4. Підхід ЄС 96

Розділ 3. ВЗАЄМОДІЯ МІЖ ДЕРЖАВАМИ У СФЕРІ ІНФОРМАЦІЙНОЇ (КІБЕР) БЕЗПЕКИ 108

3.1. Міжнародна діяльність Китаю у сфері кібербезпеки 108

3.2. Проблеми взаємодії США й Китаю в сфері кібербезпеки 115

3.3. Взаємодія ЄС і США у сфері кібербезпеки 132

3.4. Взаємодія ЄС із іншими країнами 146

ВИСНОВКИ 153

ДЖЕРЕЛА 157

ВСТУП

Суспільство трансформується в кіберсуспільство. Інтернет стає частиною повсякдення, проникає в усі сфери економіки, освіти, культури, науки, публічного й особистого життя. І це не лише технології, а й спосіб організації відносин між людьми. Комунікація, побудована на персональній участі кожного в створенні, зберіганні й поширенні змісту, дає змогу краще реалізувати персональний потенціал із усіх точок зору. З одного боку — це нові перспективи для підприємництва й розвитку громадянського суспільства, а з іншого — спокуса для потенційних злочинців, терористів і політиків, що мислять категоріями війн і конфліктів. Кіберпростір дає кращі можливості для розвитку особистості, бізнес-проєктів і загалом суспільного прогресу. Але в цих умовах також загострюється конкуренція, серед учасників ринку і на міжнародній арені.

Період становлення моделі суспільних відносин, заснованої на експлуатації переваг глобальної мережі ознаменував собою початок XXI ст. Його характерними рисами стали як стрімкі господарські й технологічні прориви, так і значні економічні, соціальні й політичні потрясіння. І сьогодні на цьому ґрунті відбуваються процеси, що суттєво впливають на політичну сферу й систему міжнародних відносин.

У цій книзі ми розглядаємо ряд безпекових питань зі сфери кіберпростору в аспекті загальних тенденцій у розвитку головних міжнародних акторів сучасності, які загалом, переслідуючи свої цілі, суттєво впливають на розвиток як самого кіберпростору, так і системи міжнародної безпеки. При цьому звертаємо увагу на актуальність поділу світу умовною межею “Схід — Захід”. Виходимо з припущення, що існує й надалі посилюється дихотомія головних концепцій інформаційної (кібер) безпеки, заснованих на глибинних відмінностях між демократичними й авторитарними системами. В основі відмінностей — інтереси, критично важливі для кожної з систем. З одного боку — інтереси демократичних суспільств, засновані на прозорості влади, необхідності збереження свободи інформації й вільної конкуренції, а з іншого (для

авторитарних систем) — це сила, що ґрунтується на тотальному управлінні інформацією та її контролі, домінуюча участь держави в суспільному житті й економіці. На цих підходах базується внутрішня й зовнішня політика держав у сфері інформаційної (кібер) безпеки. Відповідно до своїх інтересів головні міжнародні актори розробляють і просувають на міжнародних майданчиках свої концепції інформаційної (кібер) безпеки. Вони обґрунтовують позиції в сферах державного суверенітету, управління інтернетом, застосування міжнародного права в кіберсфері, доступності інформаційних технологій та ін.

Міжнародна взаємодія у сфері забезпечення інформаційної безпеки, як це й склалося в практиці міжнародної взаємодії на рівні ООН, нами розглядається в аспекті, близькому до проблематики роззброєння й міжнародної безпеки. Такий підхід характерний для представників наукових кіл, що репрезентують як країни з розвинутою демократією (А. Вендт[1], Р. Кьохан і Дж. Най[2]), так і ті, що, як буде показано далі, відстоюють авторитарний підхід до проблеми інформаційної безпеки (О. Зінов'єва[3]). Але відмінності є і вони суттєві. Наприклад у західному академічному дискурсі переважно використовується термін "кібербезпека", визнається наявність терористичних, злочинних загроз і акцентується наявність загроз військово-політичного характеру виключно в галузі технічних засобів упливу, заперечуючи наявність політико-ідеологічного компонента (наприклад А. Венгер[4], Г. Джакомелло[5], М. Хансен[6], Е. Тік-Рінгас[7] та ін.). Репрезентанти іншої точки зору, головним чином російські автори, натомість використовують термін "інформаційна безпека", виходячи з концепції чотирьох головних загроз

[1] Wendt A. (1995). Constructing International Politics. *International Security*. 1(20). P. 71–8.

[2] Keohane R. Nye J. (1998). Power and interdependence in the information age. *Foreign affairs*. P. 81–94.

[3] Зиновьева Е. (2014). Международное сотрудничество по обеспечению информационной безопасности. *Право и управление. XXI век*. № 4.

[4] Wenger A. (2001). The Internet and the Changing Face of International Relations and Security. *Information and Security*. 7. P. 5–11.

[5] Giacomello G. (Ed.) (2014). *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals*. Bloomsbury Publishing USA.

[6] Hansen L., Nissenbaum H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*. 4. P. 1155–1175.

[7] Tikk-Ringas E. (2015). *Evolution of the Cyber Domain: The Implications for National and Global Security*. London. Routledge, for the International Institute for Strategic Studies. 212 p.

міжнародній та національній безпеці в інформаційній сфері: військово-політичної, терористичної, злочинної та загрози порушення громадського порядку й стабільності через уплив на громадську думку в державі (М. Кучерявий[8], А. Смирнов [9], Д. Швець[10] та ін.).

Така ж дихотомія спостерігається й у концепціях управління інтернетом, що відображається в працях науковців із різних країн. Тут також виділяються особливою точкою зору саме представники російських дослідницьких кіл, які вочевидь слідують за державними підходами, характерними для Росії, Китаю й деяких інших країн, суть яких полягає в "суверенізації" управління мережею. Представники ж держав Заходу відстоюють незалежність інтернету від державного контролю на користь моделі багатостороннього управління за участі всіх зацікавлених сторін (порівняйте статті А. Бикова[11], М. Якушева[12] й праці таких авторів, як І. Курбалія[13], Т. Бальзак і М. Данн-Кавелті[14], Д. Маклін[15], Д. Хоффман[16]).

Зважаючи на характер кіберзагроз, тут опрацьовано роботи, що аналізують проблематику інформаційної (кібер) безпеки з правової точки зору, передусім "Таллінський посібник[17]" і "Таллінський посібник 2.0[18]", підготовлені центром Дослідження та моніторингу кібер-загроз НАТО (детальніше розглянуті в розділі

[8] Кучерявый М. М. (2013) Глобальное информационное общество и проблемы безопасности. *Власть*. *Общенациональный научно-политический журнал*. № 9 (сентябрь). С. 89–92.

[9] Смирнов А. И. (ред.) (2011). *Глобальная безопасность: инновационные методы анализа конфликтов.* Москва. Общество «Знание» России. 272 с.

[10] Швец Д. Ю. (2005). *Информационная безопасность Российской Федерации в современных международных отношениях*. Дисс. … кандидата социологических наук. Москва. МГИМО (У) МИД России. 153 с.

[11] Быков А. И. (2008). Управление Интернетом как одна из проблем современных международных отношений. Политэкс. №2 URL: https://cyberleninka.ru/article/n/upravlenie-internetom-kak-odna-iz-problem-sovremennyh-mezhdunarodnyh-otnosheniy (дата обращения: 19.05.2022).

[12] Якушев М. В. (1999). Информационное общество и правовое регулирование: новые проблемы теории и практики. *Информационное общество*. № 1. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/2be96a4e09339699c32568b1003ab653

[13] Kurbalija Jovan (2014). *An Introduction to Internet Governance*. DiploFoundation. 206 p.

[14] Balzacq T., Cavelty M. D. (2016). A theory of actor-network for cyber-security, *European Journal of International Security*. 2. P. 176–198.

[15] MacLean D. (ed.) (2005). *Internet Governance: A Grand Collaboration.* N.Y. UN ICT Task Force Series. 393 p.

[16] Hofmann J. (2005). *Internet Governance: A Regulative Idea in Flux.* Social Science Research Centre. Berlin. URL: http://duplox.wzb.eu/people/jeanette/texte/Internet%20Governance%20english%20version.pdf

[17] Schmitt M. (ed.) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* N.Y. Cambridge University Press. 282 p.

[18] Schmitt M. (ed.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. N.Y. Cambridge University Press. 638 p.

2), а також роботи авторів, що репрезентують два табори з суттєво відмінними поглядами на перспективи міжнародного права в цій сфері. Частина дослідників наполягає на необхідності адаптації права з урахуванням специфіки інформаційного простору, в той час як інші виступають за необхідність вироблення правил застосування вже існуючих норм. До перших належать майже виключно російські автори (такі як А. Коротков [19], О. Крутских [20], А. Федоров [21]), а іншу групу репрезентують представники країн Заходу (наприклад Л. Грінберг, С. Гудман, К. Су Ху[22] та ін). У своєму дослідженні ми дотримуємося домінуючої в репрезентантів країн Заходу позиції, відповідно до якої до інформаційної сфери й забезпечення кібербезпеки застосовуються різні інструменти міжнародного співробітництва. Причому увагу зосереджено передусім на кібербезпеці, проблематику розроблення нормативних основ якої на міжнародній арені висвітлювали такі автори, як Д. Фаррелл[23], М. Фіннемор[24].

Проблематика загроз військово-політичного характеру в інформаційній сфері глибоко досліджена в низці праць, серед яких найбільш відомими є роботи М. Лібіцкі[25], Р. Моландера[26], А. Шафранскі[27] та ін. Потрібно відмітити, що для країн Заходу характерна суто утилітарна концепція використання кіберпростору у військово-політичному контексті. Натомість російські автори наполягають на концепції ”інформаційних війн” у найширшому сенсі (Т. Анічкіна [28],

[19] Коротков А. В., Зиновьева Е. С. (2011). Безопасность критических информационных инфраструктур в международном гуманитарном праве. *Вестник МГИМО-Университета*. № 4. С. 154–162.

[20] Крутских А. В. (2007). К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы*. № 1(5). С. 28–37.

[21] Федоров А.В., Зиновьева Е.С. (2017). *Международная информационная безопасность: политическая теория и дипломатическая практика*. Москва. МГИМО. 360 с.

[22] Greenberg L.T., Goodman S.E., Soo Hoo K.J. (1997). *Information Warfare and International Law.* Washington: National Defense University Press.

[23] Farrell H. (2015). *Promoting Norms for Cyberspace*. New York: Council on Foreign Relations.

[24] Finnemore M. (2011). Cultivating International Cyber Norms. *America's Cyber Future: Security and Prosperity in the Information Age.* Ed. by K. Lord, T. Sharp. Washington, DC. Center for a New American Security. P. 89–101.

[25] Libicki M. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica, CA. RAND Corporation.

[26] Molander R., Riddile A., Wilson P. (1996). *Strategic Information Warfare: A New Face of War*. CA. RAND Corporation. 115 p.

[27] Szafranski R. (1995). A Theory of Information Warfare: Preparing for 2020. *Airpower Journal*. 1.

[28] Аничкина Т. Б. (2007). О некоторых приемах информационной войны США. *США-Канада: экономика, политика, культура*. №7. С. 123–127.

А. Манойло[29], С. Туронок[30]). У цьому дослідженні ми детальніше розглянемо практичні аспекти зазначених підходів.

Серед українських науковців немає одностайності в трактуванні розглянутих вище проблем в аспекті "західного" або "східного" дискурсів, хоча до останнього часу переважали обґрунтування "сильної" позиції держави в питаннях інформаційної безпеки й "інформаційного суверенітету" (О. Солодка[31]), що характерно також для представників російських наукових шкіл, з охопленням сфери, ширшої ніж та, що стосується кіберпростору в "західному" розумінні. Це може стосуватися наприклад питань "культурної експансії", розробки спеціального домена в міжнародному праві в стосунку до інформаційно-безпекових питань (В. Настюк і В. Бєлєвцева[32], О. Кісілевич-Чорнойван[33]), позитивного оцінювання відповідних російських ініціатив на рівні ООН у контексті "режиму міжнародної інформаційної безпеки" (О. Фролова[34,35]). Сучасні публікації провідних науковців у цій сфері частіше розкривають реальний стан справ у балансуванні підходів основних акторів, країн і міжнародних організацій, до політики інформаційної безпеки (М. Копійка[36], Ю. Романчук[37], Є. Макаренко, М. Рижков, М. Ожеван та ін.[38]). Також сьогодні

[29] Манойло А.В. (2003). Объекты и субъекты информационного противоборства. *Пси фактор*. URL: http://psyfactor.org/lib/psywar24.htm

[30] Туронок С. Г. (2003). Информационно-коммуникативная революция и новый спектр военно-политических конфликтов. *Политические исследования*. № 1. С. 24–38.

[31] Солодка О. М. (2020). Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. № 1(32). URL: http://il.ippi.org.ua/article/view/200311

[32] Настюк В.Я., Бєлєвцева В.В. (2014). Правові засади міжнародного співробітництва щодо протидії інформаційним правопорушенням. *Правова інформатика.* № 2(42). URL: http://ippi.org.ua/sites/default/files/14nvypip.pdf

[33] Кісілевич-Чорнойван О. М. (2009). Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика*. № 8. С. 11–18. URL: http://nbuv.gov.ua/UJRN/utp_2009_8_2

[34] Фролова О. М. (2018). Роль ООН в системі міжнародної інформаційної безпеки. *Електронне видання Інституту міжнародних відносин "Міжнародні відносини. Серія: Політичні науки".* №18.

[35] Фролова О. (2019). Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. *Вісник Львівського університету. Серія: Міжнародні відносини*. Вип. 46. с. 123–136. URL: http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_13

[36] Kopiika, M. (2020). Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя.* 1. С. 102–109. URL: https://jpl.donnu.edu.ua/article/view/7967/7967

[37] Романчук Ю. В. (2009). *Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти.* Автореф. дис... канд. політ. наук: 23.00.04. НАН України, Ін-т світ. економіки і міжнар. відносин. Київ. 20 с.

[38] Макаренко Є.А., Рижков М.М., Ожеван М.А., Кучмій О.П., Фролова О.М. (2016). *Міжнародна інформаційна безпека: теорія і практика.* Підручник. Київ. Центр вільної преси. 418 с.

потрібно враховувати зовнішньополітичний досвід України щодо співпраці зі стратегічними партнерами, що відображено в документах стратегічного планування й діяльності на головних міжнародних майданчиках.

Цю книгу створено на основі текстів, опублікованих автором у наукових часописах упродовж 2021–2022 рр., у яких досліджено підходи в реалізації політики й міжнародної діяльності основних міжнародних акторів у сфері інформаційної (кібер) безпеки – США, Росії, Китаю, Європейського Союзу. Із надією допомогти читачеві краще зрозуміти суть цієї політики з точки зору міжнародного співробітництва.

Розділ 1. КІБЕРПРОСТІР: ЗАГРОЗИ Й КОНЦЕПЦІЇ БЕЗПЕКИ

1.1. Кіберзлочинність і кібертероризм

Сьогодні, в третьому десятилітті XXI ст., інформаційне суспільство — це реалія, яка значною мірою стосується всіх народів, держав, організацій та індивідів. Інформація як предмет праці, "робоче тіло", або суттєвий чинник економічної чи соціальної діяльності, глибоко "вкоренилася", по суті, в усіх сферах і галузях, країнах, соціальних групах. А ефективність її використання стала визначальною в аспекті конкуренції.

Після появи ринку гіпертекстових ресурсів і популяризації інформаційних послуг інформаційне суспільство розвивається передусім шляхом "інтернетизації", тобто переведення суспільних відносин на платформу інтернету. Щодня до мережі приєднується близько мільйона нових користувачів. І в 2019 р., за даними Міжнародного телекомунікаційного союзу (ITU), кількість користувачів інтернету перевищила 4 млрд, що становить 51 % від усього населення Землі[39]. До 2030 р. світ досягне показника 7,5 млрд користувачів глобальної мережі. "Інтернетизація" ґрунтується на впровадженні популярних форматів і засобів обробки інформації й телекомунікації в поєднанні з технологічною конвергенцією, завдяки чому активно розвивається ринок ІКТ і масовий ринок послуг, що постачаються цифровим шляхом.

Сучасний ринок — це система попиту й пропозиції в складі товарних позицій, де у вартості кожного товару певну частку складає інформація, — від невеликої дещиці у вигляді штрихового коду GS1 для сканування й обробки в системах рітейлу, до майже 100 відсотків у цифрових послугах, передаванні даних, мультимедійному контенті для комерційного використання. Обсяг світового ринку послуг, що постачаються цифровим способом, у 2019 р. становив 3192586 млн. дол. США, що у 2,65 рази більше порівняно з 2005 р.[40].

[39] ITU estimates that at the end of 2019, a bit more that 51 per cent of the global population, or 4 billion people, are using the Internet. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[40] UNCTADSTAT. International trade in digitally-deliverable services, value, shares and growth, annual. URL: https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=158358)

Світовий ринок ІКТ-послуг за той самий час зріс у 2,55 рази й становив у 2019 р. 635734 млн дол. США[41].

Для такого динамічного ринку характерні просторова неоднорідність і неузгодженість підходів і засобів регулювання — від м'якого спрямовування його операторів у США та Європейському Союзі до тотальних обмежень у Китаї та Росії. Властивою йому рисою є поява й швидкий розвиток нових впливових чинників, які "не встигають" вчасно потрапити в поле національного контролю й міжнародної координації. Прикладом є криптовалюти, які попри скептичне ставлення до них із боку провідних фінансових акторів, суттєво вплинули на перерозподіл капіталів у період коронавірусної кризи з 2020 р. Значні мінливість, невизначеність, складність і неоднозначність суспільних процесів (відомі як VUCA[42]), зокрема процесів на інформаційному ринку, провокують інтересантів із різними мотивами, насамперед економічними й політичними. А їхні методи й засоби не завжди відповідають правовим нормам.

Про випереджаючі темпи розвитку кіберзлочинності опосередковано свідчить зростання світового ринку кібербезпеки, який у 2004 р. оцінювався в 3,5 млрд доларів, у 2011 — в 64, у 2015 — в 78, а в 2017 р. — вже в 120 млрд (приріст у більш як 34 рази)[43]. І ця динаміка стає все виразнішою. У 2020 р. обсяг світового ринку кібербезпеки становив 162,5 млрд доларів із перспективою зростання до понад 418 млрд до 2028[44], що відповідає сукупному середньорічному темпу зростання 12,5 %, і більш як у 10 разів перевищує темпи приросту ринків ІКТ і послуг, що постачаються цифровим способом.

Таке швидке зростання витрат на кібербезпеку — відповідь на все більшу загрозу кіберзлочинності, яка в 2021 р. оцінювалась у близько 6 трлн доларів

[41] UNCTADSTAT. International trade in ICT services, value, shares and growth, annual. URL: https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=158359

[42] U.S. Army Heritage and Education Center (February 16, 2018). "Who first originated the term VUCA (Volatility, Uncertainty, Complexity and Ambiguity)?". *USAHEC Ask Us a Question*. The United States Army War College. URL: https://usawc.libanswers.com/faq/84869

[43] Ross Alec (2016). Want job security? Try online security. *Wired*, 25.04.2016. URL: https://www.wired.co.uk/article/job-security-cybersecurity-alec-ross

[44] Global Cybersecurity Market Size to Grow at a CAGR of 12.5% from 2021 to 2028. *Quince Market Insights.* March 17, 2021. URL: https://www.globenewswire.com/en/news-release/2021/03/17/2194254/0/en/Global-Cybersecurity-Market-Size-to-Grow-at-a-CAGR-of-12-5-from-2021-to-2028.html

США, збільшившись удвічі з 2015 р., а до 2025 р. досягне 10,3 трлн дол. за рік, що більше за збитки, заподіяні стихійними лихами, й перевищить масштаби глобальної торгівлі всіма основними незаконними наркотиками разом [45]. Мільярдер і меценат Уоррен Баффет називає кіберзлочинність проблемою номер один для людства, а кібератаки — більшою загрозою, ніж ядерна зброя [46]. Сьогодні кібератака може потенційно вивести з ладу інформаційну систему компанії, економіку міста чи цілої країни.

За останні роки відбулися наймасштабніші в історії кібератаки. Кіберзагрози стали ще більш актуальними з початком пандемії SARS-CoV-2 у 2020 р., в зв'язку з масовою перебудовою комунікацій у всіх сферах суспільного життя й суттєвим збільшенням попиту на цифрові й IT-послуги. 2020 рік був рекордним за кількістю кібер-нападів і обсягом втрачених даних. Зростає й складність кіберзагроз, що пояснюється застосуванням нових технологій, таких як машинне навчання й штучний інтелект, а також посиленням тактичної співпраці між хакерськими групами й державними акторами. Фіксується різке збільшення масштабів активності зловмисних груп, що фінансуються державами й організованою злочинністю[47]. Безпосередніми наслідками кіберзлочинності є пошкодження й знищення даних, викрадення грошей, втрата продуктивності, крадіжка інтелектуальної власності й персональних та фінансових даних, шахрайство, загроза бізнес-комунікаціям і діловій репутації та ін.

У травні 2021 р. через атаку шкідливого програмного забезпечення зупинено роботу найбільшої американської трубопровідної системи Colonial Pipeline, в результаті чого президент США Джозеф Байден оголосив надзвичайний стан, а компанія заплатила хакерам 4,4 млн дол. у криптовалюті за відновлення роботи. Ймовірно, атаку проведено хакерською групою DarkSide, з

[45] Morgan Steve (2021) *2021 Report: Cyberwarfare in the C-Suite, Cybersecurity Ventures.* URL: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

[46] Oyedele Akin (2017). BUFFETT: This is 'the number one problem with mankind'. *INSIDER.* May 6, 2017. URL: https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5

[47] Morgan Steve (2021) *2021 Report: Cyberwarfare in the C-Suite, Cybersecurity Ventures.* URL: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

приводу чого Байден заявив, що хоча не було доказів того, що російський уряд відповідальний за напад, є дані про те, що група DarkSide знаходиться в Росії, й що російська влада “має певну відповідальність за це”[48].

Кіберзлочинність, відповідно до українського законодавства, — це сукупність кіберзлочинів, тобто суспільно небезпечних винних діянь у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. У свою чергу кіберпростором вважається “середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем і забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних[49]”. Натомість Конвенція Ради Європи про кіберзлочинність ("Будапештська конвенція”), прийнята в 2001 р., яку Україна ратифікувала в 2005 р., не містить прямого визначення кіберзлочинності, але встановлює певні стандарти для держав — учасниць, зокрема у сфері матеріального кримінального права впроваджено поділ на[50]: правопорушення проти конфіденційності, цілісності й доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями); правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами, і шахрайство, пов'язане з комп'ютерами); правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією); правопорушення, пов'язані з порушенням авторських і суміжних прав. Крім того в документі представлено відповідні стандарти в сферах процедурного права і юрисдикції. Але одним з головних досягнень Конвенції

[48] "Biden Says Russia Has 'Some Responsibility' In Pipeline Ransomware Attack". *Radio Free Europe*. May 10, 2021. Archived from the original on May 12, 2021.URL: https://web.archive.org/web/20210512233023/https:/www.rferl.org/a/fbi-confirms-darkside-hacker-group-pipeline-cyberattack-russia/31248174.html

[49] Закон України Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

[50] *Конвенція про кіберзлочинність*. Офіційний переклад. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

стало встановлення порядку міжнародного співробітництва з метою розслідування, або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами й даними, або з метою збирання доказів у електронній формі, які стосуються кримінальних правопорушень. Загалом Будапештську конвенцію позитивно сприйнято в світі, але окремі держави вже більше двадцяти років протидіють її утвердженню в якості глобального стандарту, що пов'язано з особливостями їхніх концепцій інформаційної безпеки. Про це йтиметься в наступних параграфах.

Окрім суто економічних цілей кібернападники можуть мати й політичні, атакуючи ресурси політичних партій і об'єкти критичної інфраструктури під проголошення політичних вимог чи декларацій. За допомогою таких атак робляться спроби впливу на перебіг демократичних процесів, які мають найбільше значення. Такого рівня вплив мала кібератака на Національний комітет Демократичної партії США, про яку стало відомо широкому загалу в червні 2016 р. Інформаційну систему комітету зламали два угрупування російських хакерів — Cozy Bear і Fancy Bear, які викрали скриньки електронної пошти, а також зібраний компромат на конкурента демократів на виборах президента — Дональда Трампа. Згодом викрадені матеріали використано в передвиборчій боротьбі, наприклад опубліковано на сайті організації Вікілікс, засновник якої, Джуліан Ассанж, визнав, що цим витоком намагався зашкодити претендентці від Демократичної партії Гіларі Клінтон виграти вибори [51]. У підсумку переможцем виборів став, ймовірно, більш вигідний для російського керівництва Дональд Трамп. Хоча російський уряд і заперечував причетність до цих кібератак, згодом видання The Wall Street Journal повідомило, що міністерство юстиції США змогло встановити особи шістьох російських високопосадовців, причетних до хакерської атаки на комітет Демократичної

[51] CHARLIE SAVAGE (JULY 26, 2016). Assange. Avowed Foe of Clinton, Timed Email Release for Democratic Convention. *New York Times*. URL: https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html?_r=0

парті [52] . У липні 2021 р. ті ж хакерські об'єднання атакували сервери Республіканської партії США[53].

У 2020 р. оголошено про атаку на важливі урядові структури США, здійснену через продукти американської компанії SolarWinds, яка розробляє промислове програмне забезпечення для управління мережами, системами й інфраструктурою. Через програмний комплекс Orion розробки SolarWinds зламано кілька урядових агентств США, зокрема Міністерство фінансів, Національне управління з телекомунікацій та інформації, Міністерство торгівлі, Міністерство внутрішньої безпеки. Існують підозри в незаконному проникненні в інформаційні системи НАТО, Європейського парламенту, Центру урядового зв'язку Великобританії та ін. Хакери помістили шкідливий код в оновлення програмних засобів Orion, які дають змогу зловмиснику отримати віддалений доступ до інформаційного середовища жертви атаки. Згодом газета Washington Post повідомила про те, що за атакою 2020 р. стояла хакерська група, відома як PT29 (вона ж Cozy Bear), що працює на Службу зовнішньої розвідки Росії[54].

Наприкінці червня 2021 р. зафіксовано атаку на критичну інфраструктуру Німеччини. Хакери напали на постачальника IT-послуг банків Volksbank та Raiffeisenbank, що підтвердило Федеральне управління з питань інформаційної безпеки (BSI). Згідно з інформацією журналу BILD, із західних джерел розвідки стало відомо, що за нападом стояли державні російські хакери з групи "Fancy Bear", які в такий спосіб помстилися за політику санкцій проти Росії, зробили спробу запобігти жорстким санкціям проти Білорусі та її очільника Олександра

[52] Aruna Viswanatha, Del Quentin Wilber (2.11.2017). U.S. Prosecutors Consider Charging Russian Officials in DNC Hacking Case. *The Wall Street Journal*. URL: https://www.wsj.com/articles/prosecutors-consider-bringing-charges-in-dnc-hacking-case-1509618203

[53] Turton Williams, Jacobs Jennifer (2021). Russia 'Cozy Bear' Breached GOP as Ransomware Attack. *Bloomberg*, 7 Jul. 2021. Hit. URL: https://www.bloomberg.com/news/articles/2021-07-06/russian-state-hackers-breached-republican-national-committee

[54] Nakashima Ellen, Timberg Craig (2020). Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce, *The Washington Post*, Dec. 14, 2020. URL: https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

Лукашенка [55]. Російські хакери неодноразово атакували об'єкти німецької критичної інфраструктури. Зламувались інформаційні системи Бундестагу й викрадались дані про політиків.

Є достатньо підстав стверджувати, що суттєво зростає кількість і масштаб кібератак, які можна віднести до терористичних. Сам термін "кібертероризм" досить поширений, але досі немає його однозначного трактування. У НАТО визначають кібертероризм як "кібератаку, що використовує чи експлуатує комп'ютерні чи комунікаційні мережі, щоб спричинити достатнє руйнування чи порушення, щоб викликати страх або залякати суспільство з ідеологічною метою"[56]. Американське Федеральне бюро розслідувань (ФБР) дає визначення кібертероризму як "використання кіберінструментів для виведення з ладу критично важливих національних інфраструктур (таких як енергетика, транспорт, урядові операції) з метою примушення чи залякування уряду чи цивільного населення" [57]. ФБР визначає кібертерористичну атаку як явно призначену для заподіяння фізичної шкоди людям. Комісія США з питань захисту критичної інфраструктури визначає можливими кібертерористичними цілями банківську галузь, військові об'єкти, електростанції, центри управління повітряним рухом і водні системи.

У праці "Кібервійна й кібертероризм" (ред. Л. Янчевскі й А. Коларик) дається таке визначення: "Кібертероризм — це політично мотивовані атаки, що здійснюються суб-національними групами, або таємними агентами, або окремими індивідами проти інформаційних і комп'ютерних систем, комп'ютерних програм або даних, результатом яких є насильство проти некомбатантів" [58]. Це визначення містить два ключові компоненти, які

[55] Tiede Peter (2021). Neuer Hacker-Angriff aus Russland! *BILD*, 30.06.2021. URL: https://www.bild.de/politik/inland/politik-inland/riesen-hacker-angriff-aus-russland-banken-und-kritische-infrastruktur-im-visier-76930232.bild.html

[56] Centre of Excellence Defence Against Terrorism, ed. (2008). *Responses to Cyber Terrorism*. NATO science for peace and security series. Sub-series E: Human and societal dynamics. Amsterdam: IOS Press.

[57] *Terrorism 2002-2005.* U.S. Department of Justice. Federal Bureau of Investigation. URL: https://www.fbi.gov/stats-services/publications/terrorism-2002-2005

[58] Janczewski Lech J., Colarik Andrew M. (eds.) (2008). *Cyber Warfare and Cyber Terrorism*. Hershey, PA. Information Science Reference. P. 13.

допомагають відокремити кібертероризм від інших форм кіберзлочинів — доведену політичну мотивацію й трактування з точки зору міжнародного гуманітарного права (МГП) — спрямування проти осіб, які не входять до складу збройних сил воюючих держав (згідно з визначенням IV Гаазької конвенції некомбатанти не можуть бути безпосереднім об'єктом збройного нападу супротивника, оскільки, на відміну від комбатантів, не є суб'єктами застосування насильства у військовому конфлікті).

У російських джерелах переважає дещо інший підхід до визначення кібертероризму, під яким розуміється "сукупність протиправних дій, пов'язаних із загрозами безпеці особистості, суспільства й держави, деструктивними діями щодо матеріальних об'єктів, спотворенням об'єктивної інформації, або іншими діями з метою отримання переваги при вирішенні політичних, економічних, або соціальних завдань"[59]. Помітна відмінність у російському підході в порівнянні зі сприйняттям кібертероризму в західних країнах. Якщо на Заході трактують кібертероризм як загрозу інформаційним системам, передусім пов'язаним із критичною інфраструктурою, то в Росії розглядають кібертероризм у числі комплексних загроз особі, суспільству й, що важливо, державі.

Такого підходу дотримується й китайська влада, здійснюючи контроль інтернету через державну систему "Золотий щит". Із 2006 р. будь-який інтернет-користувач, що знаходиться на території Китаю, не може отримати доступ до сайтів, що розповсюджують терористичні відомості або заклики, як і до будь-якої іншої інформації, яку ідентифіковано як таку, що має протерористичне спрямування. Ця система забезпечує державним структурам поряд із боротьбою з тероризмом, також комплексне обмеження доступу до антиурядової, аморальної й злочинної інформації, й також має перешкоджати формуванню антисоціальних установок у користувачів інтернету[60]. Але водночас така система

[59] Иванов Станислав, Томилов Олег (2013). Кибертерроризм: угроза национальной и международной безопасности. *ИА "Оружие России".* 14.03.2013. URL: https://bit.ly/2UFEJl6

[60] Дремлюга Роман Игоревич, Коробеев Александр Иванович, & Федоров Александр Вячеславович (2017). Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты. *Всероссийский криминологический журнал,* 11 (3), 607-614. URL: http://cj.bgu.ru/reader/article.aspx?id=21722

дає владі широкі можливості для контролю й суттєво обмежує свободу інформації.

Кібертероризм має два основні прояви — це, по-перше, застосування специфічних методів і засобів упливу на критичну інфраструктуру й інформаційні системи для виведення їх із ладу чи порушення нормального режиму функціонування й, по-друге, — використання анонімності, яку надає кіберпростір, щоб погрожувати особам, певним соціальним групам або громадам. Тобто в другому випадку мова йде про "звичайний" тероризм за допомогою сучасних ІКТ і рішень, таких як соціальні мережі, даркнет.

Також, як окремий випадок, можна розглядати використання кіберзлочинних дій на користь "звичайного" тероризму. Саме на цій основі в 2016 р. висунуто перше в історії США звинувачення в кібертероризмі — Ардіту Ферізі, — у тому, що він зламав військовий веб-сайт, викрав імена, адреси й іншу особисту інформацію державного значення [61]. Хоча випадки використання інформаційних технологій при здійсненні терористичних актів відомі давно, — Рамзі Юзеф, який організував вибух Всесвітнього торгового центру в Нью-Йорку 11 вересня 2001 р., отримував зашифровані інструкції від лідера Аль-Каїди Усами бен Ладена по інтернету.

Характерною рисою кібертероризму є те, що формально до нього відносять тільки дії індивідів, незалежних груп або організацій. Натомість кібератаки, організовані урядовими й іншими державними організаціями, є проявом кібервійни. Хоча в дійсності встановити реальних організаторів і замовників терористичних кібератак складно. Не виключено, що серед них можуть бути кола, близькі до урядів окремих держав.

[61] Blake Andrew (2016). "Ardit Ferizi, hacker who aided Islamic State, sentenced for helping terror group with 'kill list'". *The Washington Times*. Sept. 24.2016. URL: https://www.washingtontimes.com/news/2016/sep/24/ardit-ferizi-hacker-who-aided-islamic-state-senten/

1.2. Інформаційні й кібер-війни

Окрім розглянутих вище кіберзлочинності й кібертероризму можна виокремити й інші сфери загроз, пов'язаних із інформаційною діяльністю й кіберпростором, зокрема військово-політичну. Причому варто виділяти два різні аспекти загроз такого виду. По-перше, це загрози інформаційно-технічного характеру, явно пов'язані з силовим протиборством, де, щоправда, окрім типових для війн упливів руйнівного характеру, також можуть мати місце й такі, що не пов'язані з фізичним пошкодженням або виведенням із ладу якихось матеріальних об'єктів. По-друге, це — інформаційно-психологічні впливи, які можуть здійснюватись як у рамках воєнних стратегій (спеціальні інформаційні операції, військові комунікації), так і реалізуватись у рамках стратегічних комунікацій системного характеру, що залучають також цивільні сфери зв'язків із громадськістю й публічної дипломатії. Останній напрям отримує розвиток у часи загострення протистоянь геополітичного масштабу, як це мало місце в період "холодної війни" між СРСР і США, а також спостерігається сьогодні в постаті "гібридної війни".

Мас-медійні й соціально-медійні стратегічні комунікації здійснюються переважно в рамках правового поля й зазвичай на умовах вільної конкуренції, як наприклад діяльність російських телевізійних медіа-проєктів RT і Sputnik, або активність спонсорованих російськими державними фондами суб'єктів у громадській сфері в різних країнах світу. Цілеспрямований тривалий інформаційний уплив може створювати потенційні загрози для соціально-політичних процесів та явищ методами пропаганди, дезінформації, пост-правди, але їм складно протиставити конкретні засоби, не ризикуючи порушенням свободи слова. Натомість більш явні загрозливі інформаційні впливи, які піддаються ідентифікації, можуть мати наслідком застосування щодо їх виконавців, учасників чи ініціаторів певних легальних інструментів і засобів протидії. Тому сьогодні спостерігається розділення позицій із приводу міжнародно-правового регулювання інформаційної (кібер) безпеки. Одна точка зору полягає в можливості й необхідності застосування існуючих правових норм

і підходів, а друга — в необхідності вироблення спеціального правового режиму щодо цієї сфери. Ймовірно, прихильники першої концепції воліють легально забезпечити себе від усіх існуючих і потенційних інформаційних (кібер) загроз в усіх сферах, а другі намагаються відгородити частину загроз такого характеру, залишивши собі свободу дій в інших, не охоплених обмеженнями міжнародного права, сферах. Очевидно, що ці сфери стосуватимуться саме таких загроз, як пропаганда, пост-правда, витончена дезінформація й маніпуляція. А послідовниками цього підходу, звісно, є ті, хто вже практикує ці речі й почувається у виграшній позиції перед своїми конкурентами.

У цьому параграфі розглянемо більш конкретизовані виклики, пов'язані з кіберпростором, які можуть розглядатись у практичній площині міжнародних відносин і зовнішньої політики.

Між провідними акторами на міжнародній арені постійно відбувається боротьба з приводу відстоювання своїх інтересів. І спеціальним полем такої конкуренції є використання доступних їм інструментів і засобів із точки зору застосування сили. США, Китай і Росія, як такі, що володіють найбільшими можливостями у сфері ІКТ, намагаються в якийсь спосіб використати свої переваги, або навпаки, — нівелювати відставання. Специфіка інструментів і засобів, потенційно доступних із точки зору силового впливу в кіберпросторі чи у зв'язку із кіберпростором така, що викликає різнозначні трактування. Це пов'язано з властивостями інформації та комунікації в мережі, а також екстериторіальністю самого кіберпростору й динамікою технологічного розвитку в цій сфері, яка випереджає процеси стандартизації й легалізації.

Із точки зору використання кіберпростору з метою здійснення силового впливу потрібно враховувати, що інформація чи програмне забезпечення безпосередньо не можуть спричиняти жодних руйнувань або пошкоджень фізичних об'єктів і не можуть завдавати шкоди людям. Але, будучи компонентами зброї, вони здатні значно посилити її дію. Також ІКТ застосовуються для нівелювання оборонних можливостей протидіючої сторони. Сьогодні широко відомі приклади застосування інструментів і засобів

шкідливого кібер-впливу на інформаційні системи. Натомість випадки руйнівного впливу ІКТ поки що поодинокі.

У зв'язку з цим можна розглянути приклад Stuxnet — комп'ютерного хробака, орієнтованого на програмовані логічні контролери в автоматизованих електромеханічних системах. Під упливом цієї програми в 2010 р. отримали неадекватні керуючі сигнали й зазнали фізичного руйнування газові центрифуги для відділення ядерного матеріалу в Ірані[62]. Це була перша масштабна кібер-атака на фізичну інфраструктуру, що призвела до вагомих наслідків і в політичному плані, вплинувши на реалізацію ядерної програми Ірану. Про спеціальну розробку Stuxnet як кібер-зброї свідчить його прецизійне цільове спрямування й уплив на пристрої моніторингу з метою маскування від обслуговуючого персоналу. Були припущення, що його розроблено в рамках спецоперації відповідних служб Ізраїлю та США[63].

З іншого боку, вже відомі випадки застосування кінетичної зброї проти кібер-засобів, що призвело до руйнування інфраструктури й загибелі людей, наприклад коли в травні 2019 р. Сили оборони Ізраїлю зруйнували будівлю, пов'язану з триваючою кібератакою[64]. З цього приводу Сили оборони Ізраїлю опублікували твіт: "Ми зірвали спробу кібернаступу ХАМАС проти ізраїльських цілей. Після нашої успішної операції з кіберзахисту ми націлилися на будівлю, де працюють кібер-оперативники ХАМАС"[65].

Як бачимо, впливи кібер-засобами можуть бути пов'язані з фізичним пошкодженням і руйнуванням певних об'єктів і, потенційно, загибеллю людей, причому за участі офіційних збройних сил, що дає підстави розглядати їх із позиції міжнародного права, що діє у сфері війни. У цьому аспекті важливими є

[62] Kelley Michael B (2013). The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. *Business Insider*. 20 November 2013. URL: https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11

[63] Broad, William J.; Markoff, John; Sanger, David E. (2011). Israel Tests on Worm Called Crucial in Iran Nuclear Delay. *New York Times*. 15 January 2011. URL: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all

[64] Newman, Lily Hay (2019). What Israel's Strike on Hamas Hackers Means For Cyberwar. *Wired*. 6 May 2019. URL: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

[65] @IDF. URL: https://twitter.com/IDF/status/1125066395010699264

саме стратегічні питання, сформульовані в процесі розробки державами концепцій інформаційної безпеки. Розглянемо особливості різних концептуальних підходів до інформаційної (кібер) безпеки у військово-політичному сенсі.

Існують різні підходи до трактування інформаційних- і кібернападів. Поширеним є вживання термінів "інформаційна війна" й "кібер-війна", що характерно також і для мас-медійного дискурсу. В журналістській практиці й популярному сегменті соціальних комунікацій терміни "кібернапад", або "кібервійна" вживаються, маючи на увазі незаконний збір інформації, або інші кіберзлочини, а "інформаційна війна" — щодо пропагандистського впливу телеканалів і спільнот у соціальних мережах. Звісно, зв'язки з громадськістю, публічна дипломатія й психологічні операції, що здійснюються в стосунку до масової громадської аудиторії в зазначеному контексті, можуть здійснюватись у рамках стратегічних комунікацій, але якщо це безпосередньо не стосується таких предметних сфер, як наприклад збройні конфлікти, то очевидно не підлягають нормативно-правовому регулюванню в сенсі їх обмеження, хоча й містять в назві такі слова, як "війна", "напад", або "атака".

Поняття "інформаційної війни" сьогодні частіше використовується в практиці послідовників східного підходу. Наприклад, в Угоді між урядами держав — членів ШОС про співробітництво в галузі забезпечення міжнародної інформаційної безпеки вона визначена як "протиборство між двома або більше державами в інформаційному просторі з метою завдання шкоди інформаційним системам, процесам і ресурсам, критично важливим та іншим структурам, підриву політичної, економічної й соціальної систем, масованої психологічної обробки населення для дестабілізації суспільства й держави, а також примусу держави до прийняття рішень в інтересах протиборчої сторони[66]".

[66] СОГЛАШЕНИЕ между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (2012). URL: https://docs.cntd.ru/document/902289626

У західній концепції поняття “інформаційна війна”, як таке, в офіційних документах не поширене. Натомість у 1990-х — на початку 2000-х рр. розвивалася концепція “інформаційного протиборства” (Information Warfare), що реалізується через інформаційні операції. У звіті “Стратегічне інформаційне протиборство. Нове обличчя війни” американської “фабрики думки” RAND (1996 р.) вперше з’являється термін “стратегічне інформаційне протиборство”, як “використання державами глобального інформаційного простору й інфраструктури для проведення стратегічних військових операцій і зменшення дії на власний інформаційний ресурс[67]“. А вже за два роки вийшов новий звіт ”Розвиток стратегічного інформаційного протиборства“, в якому наведено поділ інформаційного протиборства на перше й друге покоління. Перше покоління — це “класичні“ інформаційні й психологічні операції з арсеналу військових, більш орієнтовані на дезорганізацію діяльності систем управління, які проводяться швидше для забезпечення дій традиційними силами й засобами. Натомість друге покоління визначено як ”принципово новий тип стратегічного протиборства, покликаний до життя інформаційною революцією, що вводить у коло можливих сфер протиборства інформаційний простір і ряд інших областей (перш за все економіку), й що триває довгий час: тижні, місяці й роки[68]“. Того ж 1998 р. Міністерством оборони США опубліковано “Об’єднану доктрину інформаційних операцій”, де пояснено терміни ”інформаційні операції“ (ІО) та “інформаційне протиборство“. Відповідно до цього документа ІО — це дії, вжиті для впливу на інформацію й інформаційні системи супротивника при захисті власної інформації й інформаційних систем, які застосовуються в усьому діапазоні військових операцій та на всіх рівнях війни. А “інформаційне протиборство” (“information warfare”) — це ІО, проведена під час кризи або конфлікту (включаючи війну) для досягнення або просування конкретних цілей над конкретним противником або противниками. Тобто американські військові

[67] Molander Roger C., Riddile Andrew, Wilson Peter A. (1996). Strategic Information Warfare. A New Face of War. RAND. MR-661-OSD. URL: https://www.rand.org/pubs/monograph_reports/MR661.html

[68] Molander Roger C., Wilson Peter A., Mussington B. David, Mesic Richard (1998). Strategic Information Warfare Rising. RAND. MR-964-OSD. URL: https://www.rand.org/pubs/monograph_reports/MR964.html

чітко визначають можливість застосування інформаційних засобів у рамках, охоплених міжнародним гуманітарним правом.

Загалом спостерігається певна еволюція в західній концепції інформаційних упливів з політичною чи військово-політичною метою. У період становлення сучасної моделі інформаційного суспільства й кіберпростору, в 1990-х рр. XX ст., військові доктрини містили поняття "інформаційне протиборство", яке включало не тільки кібернетичні й спеціальні психологічні засоби, а й певну ширшу область засобів інформаційного впливу в рамках інформаційних операцій на всіх етапах конфлікту. Тобто, по-суті, ця позиція загалом не надто відрізнялася від тієї, що наявна в російській концепції "інформаційних війн" (інтегрального інформаційного впливу військово-політичними й цивільними засобами). Натомість вже у спільній публікації родів військ США "Інформаційні операції" від 2006 р.[69] (згодом заміненій версією від 2012 р.) взагалі вилучено поняття "інформаційне протиборство", а отже ІО розглядаються як варіант військових операцій. До того ж, відповідно до тексту документа, припинено використання термінів "наступальні ІО" й "захисні ІО", а натомість роз'яснено, що ІО застосовуються для досягнення як наступальних, так і оборонних цілей. А самі ІО чітко класифіковано з суто військової точки зору: електронне протиборство, операції в комп'ютерній мережі, психологічні операції, безпека операцій та оперативне маскування й пов'язані з ними допоміжні й супутні можливості"[70]. Також у цьому документі пов'язано оборонну підтримку й публічну дипломатію та вказано на адаптацію державних справ і цивільних військових операцій відповідно до можливостей ІО, додано опис інформаційного середовища й обговорено його стосунок до ІО й інших військових операцій, встановлено взаємозв'язок ІО й стратегічних комунікацій.

Що стосується НАТО, то країни — члени організації використовують свої внутрішні визначення інформаційного протиборства, але вже у звіті "Information

[69] "Joint Publication 3-13, Information Operations. 13 February 2006. URL: https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf

[70] Там само.

Warfare and International Security" Комітету Альянсу з науки і технологій, прийнятому в 1999 р., термін Information Warfare пояснюється як "наступальне й оборонне застосування інформації й інформаційних систем для використання, пошкодження або знищення інформації й інформаційних систем супротивника при захисті своїх власних. Такі дії застосовуються для досягнення військової або економічної переваги над супротивником" [71]. А в англійсько-російському словнику сил спеціального призначення НАТО (2006 р.) термін Information Warfare, який часто перекладається українською мовою як "інформаційна війна", подається як інформаційне протиборство ("информационное противоборство — одна из задач сил специальных операций)". У тому ж словнику міститься термін psychological operations — психологічні операції (здійснення впливу на установки й поведінку іноземних цільових груп через різні засоби інформаційного протиборства)[72].

Щодо актуального стану справ, то розглянута вище концепція інформаційних операцій США загалом застосовується і в НАТО. У результаті розширення застосування "м'якої сили" для розв'язання політичних і військових завдань при врегулюванні кризових ситуацій у різних регіонах світу продемонстровано високу ефективність цілеспрямованого інформаційно-психологічного впливу на активних і опосередкованих учасників збройних конфліктів. Також події "Арабської весни" (2010—2011 рр.), української "Революції гідності" (2013—2014 рр.) та інших масових протестів другого десятиліття XXI ст. показали, що масоване використання інформаційних ресурсів дає змогу управляти громадською думкою й спричиняти революційні зміни в суспільствах.

Відтак у цей період в НАТО формується сучасна концепція стратегічних комунікацій (Strategic Communications), яка подібно до розглянутої вище

[71] *NATO, Information Warfare and International Security.* NATO Parliamentary Assembly Science and Technology Committee, Brussels, 6th October, 1999.

[72] NRC WORKING GROUP ON DEFENCE REFORM AND COOPERATION SPECIAL OPERATIONS FORCES GLOSSARY RUSSIAN-ENGLISH .NRC WGDRC SOF GLOSSARY (E-R) 08.12.06. URL: https://www.nato.int/docu/other/ru/2006/pdf/SOFglossary(R-E).pdf

американської доктрини, передбачає перехід від відокремленого застосування військових і цивільних інформаційно-пропагандистських структур до координації їх діяльності при підготовці й проведенні операцій із врегулювання криз. Стратегічні комунікації розглядаються як поєднання публічної дипломатії, громадських справ, військових справ та інформаційних операцій і психологічних операцій на підтримку політики Альянсу, його операцій, діяльності й для досягнення стратегічних цілей НАТО. Таке стратегічне протиборство здатне розв'язувати конфлікти без застосування (або з мінімальним використанням) збройних сил. Окрім "конвенційних" інформаційних операцій ключовим елементом системи стратегічних комунікацій є психологічні операції, визначені як планова діяльність із використання інформаційних та інших інструментів психологічного впливу на цільові аудиторії в інтересах формування необхідного світогляду й поведінки людей для досягнення політичних і військових цілей Альянсу[73].

Тобто американський і загалом євроатлантичний підхід полягає в розділенні військових і цивільних інформаційних упливів, але у взаємозв'язку з реалізацією стратегічних інтересів уряду. Така модель відповідає реаліям суспільних комунікацій у США, де держава не втручається в медійну сферу, що саморегулюється зусиллями незалежних учасників медіаринку. Визначальну роль у цьому процесі відіграють ефективне законодавство й судочинство, а також громадянська свідомість. Із іншого боку, це дає змогу чітко виокремити "конвенційні" ІО, які можуть застосовуватись у ході конфліктів і розглядаються в рамках МГП.

В українській доктрині інформаційної безпеки, прийнятій у відповідь на гібридну війну з боку Росії, також використовується термін "стратегічні комунікації" відповідно до стандарту НАТО (скоординоване й належне використання комунікативних можливостей держави — публічної дипломатії,

[73] NATO STANDARD AJP-3.10.1 ALLIED JOINT DOCTRINE FOR PSYCHOLOGICAL OPERATIONS Edition B Version 1. WITH UK NATIONAL ELEMENTS SEPTEMBER 2014. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf

зв'язків із громадськістю, військових зв'язків, інформаційних і психологічних операцій, заходів, спрямованих на просування цілей держави), а побудова дієвої й ефективної системи стратегічних комунікацій вказана серед пріоритетів державної політики в інформаційній сфері [74]. Також створення системи стратегічних комунікацій оголошено серед основних напрямів зовнішньополітичної і внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки (Стратегія національної безпеки України)[75]. У свою чергу, відповідно до прийнятої в 2021 р. оновленої воєнної доктрини, взято курс на запровадження об'єднаного керівництва з підготовки й ведення всеохоплюючої оборони України, де одним із цільових напрямів є розвиток спроможностей сил оборони України щодо стратегічних комунікацій у сфері оборони й виконання завдань, використовуючи єдиний інформаційний простір [76]. Отже, в Україні загалом прийнято західний підхід у військово-політичній сфері інформаційної- та кібер-безпеки з виділенням військових і цивільних компонентів у єдиній системі стратегічних комунікацій.

На противагу західній моделі східна тяжіє до втручання влади в усі сфери інформаційного суспільства, в тому числі й в аспекті військово-політичних інтересів. Зрощення медіасфери й державної машини, особливо в інтересах геополітичних стратегій, призводить до появи такого феномену як "інформаційні війни", тобто інформаційний вплив держави всіма засобами для досягнення стратегічних цілей. Звідси беруть початок і "гібридні війни", як породження державної монополії на управління медіа-каналами і створення спеціалізованих державних пропагандистських майданчиків, які працюють у координації з військово-політичним керівництвом.

[74] УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: https://www.president.gov.ua/documents/472017-21374

[75] УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №392/2020. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». URL: https://www.president.gov.ua/documents/3922020-35037

[76] УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №121/2021. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України». URL: https://www.president.gov.ua/documents/1212021-37661

У російській практиці також скорочується застосування терміну “інформаційні війни”, який містився в доктрині інформаційної безпеки РФ 2000 р. й відсутній у документі з аналогічною назвою від 2016 р[77]. Оновлена доктрина, тим не менше, також орієнтує на протидію певним ворогам, серед яких “окремі держави” , “окремі / різні організації”, або “окремі особи”, що здійснюють “інформаційний уплив на населення”, “скоординовані комп’ютерні атаки”, “нарощування загроз застосування інформаційних технологій із метою завдання шкоди суверенітету РФ” . Із тексту документа зрозуміло, що Росія готується до захисту від “інформаційно-психологічного впливу, спрямованого на дестабілізацію внутрішньополітичної й соціальної ситуації, що призводить до підриву суверенітету й порушення територіальної цілісності” й має протидіяти зовнішньому інформаційному впливу на молодь Росії, який здійснюється “з метою розмивання традиційних російських духовно-моральних цінностей[78]”.

У документі використовується термін “інформаційне протиборство”, причому як його суб’єкти вказані, окрім збройних сил, також “інші війська, військові формування й органи”. Тобто порівняно з західною моделлю інформаційної безпеки Росія, по-суті, дотримується концепції “інформаційних війн”, де засоби інформаційного впливу з військово-політичною метою, а саме інформаційне протиборство, легалізуються не тільки в військовій, але й у цивільній сфері.

Загалом російська (східна) модель інформаційної безпеки не розділяє військові й невійськові впливи, а отже по своїй суті непридатна для адаптації до діючих міжнародно-правових норм і вимагає формування окремого режиму на кшталт “міжнародної інформаційної безпеки” (про що йтиметься далі). Очевидно цим пояснюється, що серед загроз інформаційній безпеці, виділених у згаданій вище російській доктрині, є “відсутність міжнародно-правових норм, що регулюють міждержавні відносини в інформаційному просторі, а також

[77] Указ Президента Российской Федерации от 05.12.2016 г. № 646. Об утверждении Доктрины информационной безопасности Российской Федерации. URL: http://kremlin.ru/acts/bank/41460/page/1

[78] Там само.

механізмів і процедур їх застосування", що "ускладнює формування системи міжнародної інформаційної безпеки"[79].

Варто відмітити й те, що поняття "інформаційного протиборства", зокрема розвиток його сил і засобів вказано серед завдань Військової доктрини РФ[80]. Суть інформаційного протиборства пояснено в словнику, розміщеному на веб-сайті Міністерства оборони РФ як інформаційний уплив на інформаційну сферу противника (при захисті власної), причому цей термін пов'язано з іншим — "інформаційна війна", в якій "політичні, економічні й інші цілі досягаються руйнуванням інформаційного середовища протилежної сторони й оволодінням її інформаційними ресурсами[81].

Детально розкрито бачення військово-політичної сфери інформаційної безпеки в документі стратегічного значення "Концептуальні погляди на діяльність Збройних Сил Російської Федерації в інформаційному просторі[82]", опублікованому Міністерством оборони РФ у 2011 р. Документ містить формулювання поняття "Інформаційна війна" як протиборства між двома або більше державами в інформаційному просторі з метою завдання шкоди інформаційним системам, процесам і ресурсам, критично важливим та іншим структурам, підриву політичної, економічної й соціальної систем, масованої психологічної обробки населення для дестабілізації суспільства й держави, а також примусу держави до прийняття рішень в інтересах протиборчої сторони. Причому "інформаційний простір" визначається тут як "сфера діяльності, пов'язана з формуванням, створенням, перетворенням, передачею, використанням, зберіганням інформації, що чинить уплив, у тому числі на індивідуальну й суспільну свідомість, інформаційну інфраструктуру й власне інформацію". Отже, по-суті, військова стратегія РФ принципово охоплює весь

[79] Там само.

[80] Военная доктрина Российской Федерации. URL: http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf

[81] *Информационное противоборство*. Справочник МО РФ. URL: https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary

[82] Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. 2011. URL: https://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle

цей “простір”, включно з усією інформацією, індивідуальною й суспільною свідомістю, тобто все суспільство, всю економіку й політичну сферу загалом, хоча в зазначеному документі й заявляється, що “Збройні Сили Російської Федерації зобов’язані дотримуватися норм міжнародного гуманітарного права під час своїх операцій в інформаційному просторі[83]”.

Підхід російської влади до реалізації військово-політичних інструментів із точки зору інформаційної безпеки стає ще більше зрозумілим із резюмуючого твердження в зазначеному вище документі про те, що “обороноздатність Російської Федерації істотно залежить від ефективності діяльності Збройних Сил в інформаційному просторі й багато в чому визначається їх можливостями щодо стримування, запобігання й вирішення конфліктів, що виникають в інформаційному просторі”, а власне Збройні Сили РФ “будуть прагнути до максимального використання можливостей інформаційного простору для зміцнення обороноздатності держави, стримування й запобігання військових конфліктів, розвитку військового співробітництва, а також формування системи міжнародної інформаційної безпеки в інтересах усього світового співтовариства[84]”.

Тобто сьогодні російська концепція політичного й військово-політичного виміру інформаційної безпеки заснована на експлуатації моделі “інформаційних війн” — комплексної сфери забезпечення політичних і геополітичних інтересів держави за допомогою військових і цивільних інформаційних- та кібер-засобів. Причому офіційно пропагується екстраполяція цієї моделі на сферу міжнародних відносин із формуванням спеціального режиму “міжнародної інформаційної безпеки”, що вочевидь передбачає необхідність формування спеціального домена в міжнародному праві. Натомість західна модель побудована на розвитку системи стратегічних комунікацій у такий спосіб, що це дає змогу забезпечити відповідність діючим міжнародно-правовим нормам.

[83] Там само.
[84] Там само.

1.3. Інформаційна (кібер) безпека

Розглянуті в попередніх параграфах відмінності в трактуванні інформаційних загроз відображають особливості національних підходів до питання інформаційної безпеки — як на національному, так і на міжнародному рівнях. Загалом є два різних бачення інформаційної безпеки з точки зору держави. Назвемо їх західним (демократичним і технократичним) і східним (авторитарним та ідеологічним). Держави, що практикують східний підхід, пропонують норми, які включають сильний урядовий контроль над інформацією, тоді як із позицій західного підходу це сприймається це як загроза політичній стабільності.

Західне бачення, що сформувалось у США, базується на розумінні інформаційної безпеки як безпеки даних і, відповідно, інформаційних систем, що з ними пов'язані. Регулювання сфери інформації стало пріоритетом американської державної політики раніше, ніж в інших країнах, оскільки США стали епіцентром інформаційної революції вже в другій половині XX ст., і розвивалось відповідно до принципів функціонування демократичної соціально-економічної моделі. Головним завданням тут стало гарантування рівних можливостей виробництва й споживання інформації кожному індивіду.

Законодавство США визначає, в загальному випадку, дані як комерційно значущу інформацію, володіння й законне розповсюдження якої дає змогу отримати вигоду або уникнути збитків. Наприклад отримання, зберігання, обробка й обіг персональних даних у США регулюються законодавством саме з точки зору комерційної значущості вказаної категорії інформації. У 1966 р. федеральним Законом про свободу інформації (Freedom of Information Act, FOIA) закріплено підзвітність влади народу, якому вона служить, оскільки інформований електорат є критично важливим для належного функціонування демократії. У такому аспекті інформаційна безпека має на меті забезпечення функціонування інформаційних систем задля належного функціонування виконавчої влади та її звітності перед народом. З іншого боку влада має забезпечити недоторканність інформації, що належить особі, так само як і будь-

якої іншої приватної власності. Відтак концепція свободи інформації була розвинута з прийняттям у 1974 р. Закону про конфіденційність (The Privacy Act), який встановлює кодекс добросовісної інформаційної практики, регулюючи збір, технічне обслуговування, використання й розповсюдження особистої інформації про фізичних осіб, що ведеться в системах записів федеральних органів. Також, як відомо, в США свобода волевиявлення й свобода слова гарантовані першою поправкою до Конституції [85]. Відповідно держава не може безпосередньо вводити цензуру чи фільтрувати зміст інформації, що також відображається на підході до інформаційної безпеки. Окрім того для Сполучених Штатів характерне відкрите неприйняття безпосереднього державного регулювання. Таким чином забезпечуються ефективні ринкові відносини. Завдання ж держави в такій моделі полягає в забезпеченні можливостей розвитку ринкових відносин. Тому загалом американський підхід до забезпечення інформаційної безпеки, який спирається на досить давні документи, заснований на захисті інфраструктури (в тому числі й критично важливої) передавання, зберігання й обробки даних, та історично не включає в себе проблему впливу ”шкідливого“ контенту на діяльність держави, суспільства, особистості.

Комітет із систем національної безпеки США поняття “інформаційна безпека” розкриває як захист інформації й інформаційних систем від несанкціонованого доступу, використання, розкриття, руйнування, зміни чи знищення з метою забезпечення цілісності (захист від несанкціонованої модифікації чи знищення інформації), конфіденційності, а також доступності (забезпечення своєчасного й надійного доступу до інформації) [86]. Подібно визначає інформаційну безпеку також Асоціація аудиту й контролю інформаційних систем (”Забезпечує, що лише авторизовані користувачі (конфіденційність) мають доступ до точної й повної інформації (цілісність) коли

[85] The First amendment. Legal Information Institute. URL: http://www.law.cornell.edu/anncon/html/amdt1afrag1_user.html#amdt1a_hd4

[86] Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010. URL: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

це потрібно (наявність)"[87]). Тобто це поняття в американській практиці зводиться тільки до захисту даних і не містить такого складника, як захист від шкідливого контенту (небажаного інформаційного впливу).

Політика Європейського Союзу у сфері інформаційної безпеки також ґрунтується на принципах, властивих західному підходу. Вперше їх сформульовано в комюніке Європейської комісії "Мережева й інформаційна безпека: пропозиції для підходу європейської політики[88]" в 2001 р. Відповідно до цього документа "мережева й інформаційна безпека" (Network and Information Security) визначається як здатність мережі або інформаційної системи протистояти на заданому рівні надійності випадковим загрозам або умисним шкідливим діям, які ставлять під загрозу доступність, достовірність, цілісність і конфіденційність збережених або переданих даних і пов'язаних із ними служб, доступ до яких здійснюється за допомогою таких мереж або систем. Єврокомісією запропоновано такі принципові засади в політиці щодо забезпечення мережевої й інформаційної безпеки: по-перше, забезпечення прикладного характеру правових норм на основі загального розуміння основних питань безпеки і спеціальних заходів щодо її забезпечення (що властиво загалом західному підходу); 2) необхідність постійного вдосконалення правового регулювання з урахуванням технічного прогресу й породжуваних ним нових загроз (це ще одна характерна для західного підходу риса, яку на міжнародному рівні підтримують США); 3) потреба в доповненні ринкових механізмів політичними заходами (відображає важливість проблеми інформаційної безпеки, що розглядається на рівні комунітарної політики ЄС); 4) формування європейського внутрішнього ринку інформаційно-телекомунікаційних послуг (базовий підхід у всіх галузевих і секторальних політиках ЄС).

[87] ISACA (2008). Glossary of terms, 2008. URL: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

[88] Communication from the Commission to the Council, the European parliament, the European Economic and Social Committee and the Committee of the Regions «Network and Information Security: Proposal for A European Policy Approach». Brussels, 6.6.2001. COM (2001)298 final.

Підхід японського уряду також відповідає західній, або технократичній, моделі. У Стратегії кібербезпеки Японії, підготовленій і винесеній на обговорення в 2013 р.[89], можна виділити такі основні цілі: забезпечення вільного й безпечного обміну інформацією; спроба вивести проблему кібербезпеки на більш високий рівень; оптимізація відповідних дій, спрямованих на розв'язання проблеми кібербезпеки; розробка плану дій і зміцнення співробітництва на основі принципів соціальної відповідальності. Відповідно до цієї стратегії уряд має забезпечити надійність і стійкість кіберпростору, підвищивши рівень інформаційної безпеки й забезпечивши захист від кібернападів, стимулювати науково-дослідницьку діяльність для розвитку кіберпростору, залучити на конкурентній основі нові кадри для забезпечення кібербезпеки й забезпечити освіту громадян із питань кібербезпеки.

Східна концепція значної уваги надає питанню захисту держави, суспільства й особистості від негативного інформаційного контенту. Одним із перших документів, у якому сформульовано таке бачення, стала Доктрина інформаційної безпеки Російської Федерації[90], затверджена у вересні 2000 р. У 2016 р. прийнято нову доктрину[91], яка стала логічним продовженням першої — якщо в документі 2000 р. йдеться про зростання впливу інформаційних технологій на національні інтереси країни, то в новій версії вони вже визнаються невід'ємною частиною всіх сфер життя.

Для російського підходу характерне формулювання інформаційних загроз загального характеру, які розцінюються як суттєві з точки зору національної безпеки. Наприклад, для згаданої доктрини 2000 р. ключовими проблемами були "розкладання моральних цінностей молоді", відтік фахівців у сфері безпеки. Під

[89] Japan Cybersecurity Strategy. Information Security policy Council, 2013. URL: http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf

[90] Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895) Совет безопасности РФ. URL: http://www.scrf.gov.ru/documents/5.html

[91] Доктрина информационной безопасности Российской Федерации
Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

інформаційною безпекою країни з такої точки зору розуміється стан захищеності її національних інтересів у інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства й держави. Нова доктрина називає головними загрозами кіберзлочинність і поширення дестабілізуючих ситуацію в країні матеріалів із-за кордону, зокрема таких, що критикують Російську Федерацію, популяризація тенденцій, що тиснуть на молодь. Формулюючи такі ”проблеми“ як загрозливі для суспільства й особи, влада обґрунтовує своє втручання в перебіг інформаційних процесів необхідністю захисту національного інформаційного поля від іноземних упливів.

Східний підхід не передбачає безумовного гарантування свободи слова й масової інформації, відкриваючи шлях до цензури й контролю інформаційної сфери. Наприклад у російській доктрині 2000 р. міститься таке формулювання однієї з проблем, що потребує розв’язання: ”недостатність нормативного правового регулювання відносин у галузі реалізації можливостей конституційних обмежень свободи масової інформації в інтересах захисту основ конституційного ладу, моральності, здоров'я, прав і законних інтересів громадян, забезпечення обороноздатності країни й безпеки держави суттєво ускладнює підтримання необхідного балансу інтересів особистості, суспільства й держави в інформаційній сфері”. Цей же документ дає підстави й для суб‘єктивної цензури, оскільки до загроз інформаційної безпеки країни віднесено, зокрема, такі як ”девальвація духовних цінностей, пропаганда зразків масової культури, заснованих на культі насильства, на духовних і моральних цінностях, що суперечать цінностям, прийнятим в російському суспільстві; зниження духовного, морального й творчого потенціалу населення Росії“.

Фактично йдеться про реалізацію державного контролю в інформаційній сфері, що сьогодні часто подається як “інформаційний суверенітет” або “кібер-суверенітет”. Поняття “інформаційного суверенітету” не нове, воно розробляється і втілюється в практику з часів початку масового поширення інтернет-технологій у країнах, що тяжіють до авторитарного типу організації суспільства. У Китаї на державному рівні кібер-суверенітет формується,

починаючи з початку 2000-х. У Росії в квітні 2014 р. Максим Кавджарадзе, член Ради Федерації, верхньої палати російського парламенту, запропонував створити повністю недоступну з-за кордону національну внутрішню мережу Росії. Тоді з'явилася й назва — "ЧебурашкаNet" на честь російського мультиплікаційного героя Чебурашки, персонажа з відомого анімаційного фільму[92]. А в 2019 р. прийнято зміни до федерального законодавства, які отримали неформальну назву "Закону про суверенний інтернет"[93]. Метою закону є створення автономних систем управління інтернетом і тим самим створення можливості відокремлення російського інтранету від глобальної мережі Інтернет.

Згідно з законом Росія вимагає від національних постачальників послуг інтернету використовувати лише точки обміну інтернетом, затверджені Роскомнаглядом, російським регулятором телекомунікацій, а оператори зв'язку зобов'язані встановити державне обладнання на точках обміну трафіком для аналізу й фільтрації трафіку всередині країни й лініях зв'язку, які перетинають кордон Росії. Крім того, Росія матиме можливість відключити свою мережу від глобальної системи доменних імен (DNS).

Закон викликав певну протидію з боку громадськості[94], що розглядає цю ініціативу як нову форму цензури. На відміну від Китаю, громадяни якого увійшли в епоху інтернету майже в той самий час, коли уряд почав його регулювати, й звикли до такого способу життя, де інтернет є національною інтрамережею, громадяни Росії завжди мали доступ до глобальної мережі й широкого спектру контенту та послуг із будь-якої країни. Крім того, сьогодні, порівняно з періодом становлення масового інтернету, мережа вже міцно "вросла" в економіку, яка залежать від інтернету й безперебійного функціонування певних додатків і послуг. У наш час відключення від іноземних цифрових послуг має великий негативний вплив на національну економіку. Тому

[92] Канев Сергей (2014). Чебурашка, или Хорошими делами прославиться нельзя. *Новая Газета*. 5 мая 2014. URL: https://novayagazeta.ru/articles/2014/05/05/59473-cheburashka-ili-horoshimi-delami-proslavitsya-nelzya

[93] Принят закон о "суверенном интернете". *Государственная Дума Федерального собрания Российской Федерации*. 16.04.2009. URL: http://duma.gov.ru/news/44551/

[94] В Москве прошел митинг против изоляции Рунета. *РБК*, 10 марта 2019 года. URL: https://www.rbc.ru/politics/10/03/2019/5c851a2d9a7947fefc8e4288

такий ”цифровий суверенітет“ може виявитися надто дорогим для Росії, уряд якої, проте, переслідує в такий спосіб насамперед політичні й геополітичні цілі. Такий підхід, заснований на безапеляційному “захисті“ державою ”інформаційного суверенітету“, знайшов своє відображення в усіх основних законодавчих актах, прийнятих Росією у сфері інформаційної безпеки.

Крім Доктрини інформаційної безпеки в масштабі міжнародної взаємодії Росія керується документом, уперше прийнятим у 2013 р. й оновленим у 2021 р. — це, відповідно, “Основи державної політики в галузі міжнародної інформаційної безпеки на період до 2020 року[95]” та “Основи державної політики Російської Федерації в галузі міжнародної інформаційної безпеки[96]”. У цьому документі вже в 2013 р. закріплювались такі тези, як: ”втручання у внутрішні справи суверенної держави з використанням ІКТ, порушення суспільної стабільності, розпалювання міжетнічної й міжнаціональної ворожнечі“, що, очевидно, є відображенням подій ”арабської весни“ (2010—2011 рр.), в ході якої активне використання соцмереж забезпечило координацію дій протестного руху.

Подібний підхід до інформаційної безпеки властивий і владі Китаю. У Національній стратегії розвитку інформатизації на 2006—2020 рр. Національний інформаційний консультативний комітет КНР визначає інформаційну безпеку як ключовий компонент системи національної безпеки, необхідний для забезпечення сталого, здорового застосування інформаційних технологій, а також для соціальної й культурної стабільності й ідеологічного розвитку.[97]

---

[95] Основы государственной политики в области международной информационной безопасности на период до 2020 года. URL: http://www.consultant.ru/document/cons_doc_LAW_178634/

[96] Основы государственной политики Российской Федерации в области международной информационной безопасности (Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213). URL: http://www.scrf.gov.ru/security/information/document114/

97 2006-2020 年国家信息化发展战略 (2006-2020 Nián guójiā xìnxī huà fāzhǎn zhànlüè) [Державна стратегія із розвитку інформатизації на період з 2006 до 2020 р.]. 08.05.2005. URL: https://baike.baidu.com/item/2006-2020%20%E5%B9%B4%E5%9B%BD%E5%AE%B6%E4%BF%A1%E6%81%AF%E5%8C%96%E5%8F%91%E5%B1%95%E6%88%98%E7%95%A5/16956741?fr=aladdin.

Східна концепція інформаційної безпеки передбачає виключний пріоритет держави в питаннях, що стосуються "інформаційного суверенітету". Йдеться про контроль усього, що відбувається в інформаційному полі, яке влада вважає належним до своєї юрисдикції. Прикладом такого ревнісного ставлення до інформації в питанні її захисту є Закон про кібербезпеку КНР, прийнятий у 2016 р.[98] Закон робить акцент на зборі, зберіганні й використанні персональних даних китайських громадян та інформації, що має відношення до національної безпеки. Такі відомості повинні зберігатись усередині країни (також і в Росії в 2015 р. набуло чинності положення закону, яке зобов'язує операторів персональних даних обробляти й зберігати персональні дані росіян із використанням баз даних, розміщених на території РФ). Забороняється експорт економічних, технологічних, наукових даних, які становлять загрозу національній безпеці чи громадським інтересам.

В основі законів, що охоплюють цивільну сферу безпеки кіберпростору в Китаї, лежить так звана "класифікація багаторівневої системи захисту" (Multiple-level Protection Scheme, MLPS), відповідно до якої приймаються рішення про рівень допуску іноземних товарів у ту чи іншу сферу або систему. MLPS визначає п'ять рівнів інформаційної безпеки з точки зору потенційних наслідків, від шкоди правам громадян, організацій, громадському порядку, до загрози національній безпеці[99]. Покладаючись на MLPS і законодавство, влада вимагає доступу до протоколів шифрування й значної частини вихідного коду від компаній, що працюють у сфері фінансів, телекомунікацій, медицини, освіти й енергетики.

Однією з основних рис східного підходу до мінімізації загроз інформаційній безпеці є запобігання проникненню небажаної інформації всередину країни й витоку чутливої інформації за кордон, в т. ч. шляхом блокування соціальних

98 中华人民共和国网络安全法(Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ) [Закон Китайської народної республіки про кібербезпеку]. 07.11.2016. URL: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

99 Yan Luo, Zhijing Yu, Nicholas Shepherd (2021). Cybersecurity risk classification under China's multi-level protection scheme. Practical Law. Thomson Reuters. URL: https://uk.practicallaw.thomsonreuters.com/w-022-3160?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true

мереж і пошукових систем. Наприклад керівництво КНР уважає, що сама суть інформаційної безпеки полягає в уведенні обмежень на поширення небажаної інформації[100].

Певною мірою східний (російсько-китайський) підхід до політики інформаційної безпеки протилежний західному (американському та європейському), орієнтованому на кібербезпеку. Основна відмінність полягає в тому, що уряд (держава) забезпечує безпеку не тільки інфраструктури, але й самої інформації, декларуючи її невід'ємним складником національного суверенітету. Інформаційний суверенітет трактується російською владою як "нерозповсюдження" іноземної інформації серед російських громадян та обмін "належною інформацією про Росію з іноземними партнерами"[101], в той час як у західній концепції суверенітет в інформаційну епоху — це заохочення глобального обміну інформацією через безпечну технологічну інфраструктуру.

Західний підхід базується на безпечному зв'язку, — інформація безпечна, доки безпечна технологічна інфраструктура, а відповідальність уряду полягає в тому, щоб кожен громадянин міг вільно користуватися безпечними технологіями. На такій позиції заснований базовий підхід країн Заходу до політики кібербезпеки в епоху інтернету — правило мережевого нейтралітету, що означає забезпечення рівного доступу та швидкості спілкування для кожного користувача, виключаючи таким чином будь-яку можливість маніпулювання вмістом. Принцип мережевого нейтралітету підтримується Федеральною комісією зв'язку США[102] на підставі Закону про комунікації (1934 р.), хоча й піддавався певним обмеженням у період президенства Д. Трампа. Також цей

100 汪玉凯: 中央网络安全与信息化领导小组的由来及其影响 (Wāngyùkǎi: Zhōngyāng wǎngluò ānquán yǔ xìnxī huà lǐngdǎo xiǎozǔ de yóulái jí qí yǐngxiǎng) [Ван Юкай. Походження провідної малої групи з інформатизації та безпеки в мережі інтернет]. Baidu.com. 06.03.2014. URL: https://wenku.baidu.com/view/0c29475252d380eb62946d86.html.

101 Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

102 STATEMENT OF ACTING CHAIRWOMAN ROSENWORCEL ON DEPARTMENT OF JUSTICE DECISION TO WITHDRAW LAWSUIT TO BLOCK CALIFORNIA NET NEUTRALITY LAW. URL: https://docs.fcc.gov/public/attachments/DOC-369799A1.pdf

принцип присутній у більшості європейських стратегій кібербезпеки, а на рівні Європейського Союзу його закладено в стратегію Єдиного цифрового ринку ЄС[103] (проголошено в 2015 р.). Основні рамки для забезпечення нейтралітету мережі на території всього Європейського Союзу, зокрема, встановлено Регламентом ЄС 2015/2120[104].

Країни, де домінує східний підхід, не забезпечують невтручання в роботу мережі, наприклад у Росії на початку 2018 р. кабінет міністрів запропонував формально відмовитись від принципу мережевого нейтралітету, який і так не підтримувався в країні[105]. Не застосовується принцип мережевого нейтралітету й у Китаї, де уряд використовує інтернет-провайдерів для перевірки й регулювання вмісту, доступного для громадян країни. За допомогою так званого ”Великого брандмауера“ блокуються як іноземні, так і китайські сайти, що надають інформацію, яку уряд не може ефективно змінити, наприклад, IP-адреси соціальних мереж або інформаційні сайти[106].

Загалом суть відмінностей між американським і російським підходами полягає в самому трактуванні поняття “інформаційна безпека”. Якщо в США виступають виключно за технічне регулювання кіберсередовища (захист комп’ютерних мереж і ресурсів) і використовують поняття “кібербезпека”, а не “інформаційна безпека”, то Росія включає в це поняття як технічне забезпечення кібербезпеки систем і мереж, так і політико-ідеологічні аспекти — протидію пропаганді й недопущення інформаційного впливу.

---

[103] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. A Digital Single Market Strategy for Europe. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

[104] REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015. laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&rid=2

[105] Правительство РФ не видит необходимости в законодательном закреплении сетевого нейтралитета. *Роскомсвобода.* 29.10.2018. URL: https://roskomsvoboda.org/42667/

[106] Hu, Henry L. (2011). "The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration". *The China Quarterly*. 207 (207). P. 523–540.

1.4. Кібер-війни й міжнародне право

Беручи до уваги аргументи послідовників обох концепцій — як прихильників “інформаційних загроз” та “інформаційних війн” в “інформаційному просторі” й, відповідно, “міжнародної інформаційної безпеки”, так і тих, хто відстоює принцип застосовності діючого міжнародного права у сфері інформаційних військово-політичних загроз, потрібно розглянути зв’язок самого предмета дискусії зі сферами права на ведення війни й права під час війни, тобто МГП.

Jus ad bellum (лат. “право на війну”) стосується умов, за яких національні держави можуть вдатися до війни або загалом до застосування збройної сили. Хоча історично jus ad bellum розумілося на рівні міжнародно-правових звичаїв, прийняття Статуту ООН у 1945 р. перетворило ці принципи на обов’язкові норми міжнародного права. Стаття 2 (4) забороняє “загрозу або застосування сили проти територіальної цілісності чи політичної незалежності будь-якої держави чи будь -якої іншої способом, що не відповідає цілям Організації Об’єднаних Націй”. Із цієї заборони є два явних винятки. По-перше, Рада Безпеки може застосувати силу, якщо вона встановлює, що необхідно “підтримувати міжнародний мир і безпеку”. По-друге, Стаття 51 зберігає “невід’ємне право індивідуальної або колективної самооборони, якщо здійснено збройний напад на члена Організації Об’єднаних Націй”.

Отже, за режимом Статуту ООН держави обмежені в застосуванні сили проти інших держав за винятком випадків, коли така сила застосовується під управлінням Ради безпеки ООН, або використовується для “індивідуальної чи колективної самооборони” проти “збройного нападу”.

У зв’язку з можливістю широкого трактування й інтерпретації зазначених винятків з обмеження застосування сили, держави дотримуються двох полярних позицій — одні виступають за більш широкі можливості застосування сили, а інші наполягають на обмеженні застосування сили державами. Перші (серед них — США й країни НАТО) зазвичай виступають за широке визначення самооборони, відмову від монополії ООН на санкціонування військових дій і

допустимість гуманітарних чи продемократичних втручань[107]. З іншого боку, ряд держав, серед яких Росія й Китай, дотримуються позитивістської позиції щодо тексту Статуту ООН, відповідних резолюцій Генеральної Асамблеї, обмежуючи самооборону вузьким набором обставин і зазвичай не визнають інших винятків із загальної заборони застосування сили державами.

Така розбіжність у поглядах на питання безпеки ґрунтується, з одного боку, на неприйнятті Росією і, значною мірою, Китаєм, силового врегулювання загрозливих з точки зору США ситуацій, що мало наслідком військові операції в Іраку, на Балканах, Афганістані та ін. З іншого боку, США й інші країни Заходу не приймають, наприклад, позиції Росії, за якої остання зводить трактування сили до формальних критеріїв, заперечуючи, наприклад, участь своїх військ у війні в Україні з 2014 р., видаючи своїх комбатантів за місцеве "ополчення".

Росія й Китай підкреслюють важкість адаптації міжнародних правил до кіберпростору й зосередилися на просуванні "міжнародного кодексу поведінки" для кіберпростору. Натомість уряд США публічно й неодноразово заявляв, що "кібер-діяльність за певних обставин може бути підставою для застосування сили в значенні Статті 2 (4) Статуту ООН та міжнародного звичаєвого права[108]".

Ймовірно, виходячи саме з такої позиції, коментуючи завершення в 2017 р. роботи Групи урядових експертів ООН у сфері інформатизації й телекомунікацій в контексті міжнародної безпеки (UN GGE)[109], представник США Мішель Маркофф зазначила, що деякі країни (маючи на увазі Росію й Китай) наполягали, що застосування основних принципів jus ad bellum (право початку війни) і jus in bello (право при веденні війни) призведе до мілітаризації ІКТ сфери, а не до запобігання використання ІКТ в міжнародних конфліктах[110].

---

[107] Ruys Tom, Corten Olivier, Hofer Alexandra (2018). *Use of Force in International Law.* Oxford University Press, 2018. URL: https://books.google.com.ua/books?id=MkdiswEACAAJ&printsec=frontcover&hl=uk#v=onepage&q&f=false

[108] Koh Harold Hongju (2012). International Law in Cyberspace. *Harvard International Law Journal.* 54 (December 2012).

[109] *детальніше про роботу зазначеної Групи урядових експертів див. у наступних параграфах.

[110] Markoff Michele G. (2017). *Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security.* US Department of State, June 23, 2017. URL: https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm

З цього приводу потрібно зазначити, що Росія й Китай, разом з партнерами по ШОС, Таджикистаном та Узбекистаном, у 2011 р. та в 2015 р. подали Генеральному секретарю ООН проєкт міжнародного Кодексу поведінки з питань інформаційної безпеки[111]. Документ є важливим індикатором світогляду країн східного підходу щодо міжнародного регулювання кібер-діяльності. Членам ООН пропонується зобов'язатися "не використовувати інформацію й комунікаційні технології, включаючи мережі, для здійснення ворожої діяльності або актів агресії, або якщо вони становлять загрозу міжнародному миру й безпеці". Але не пропонується жодних вказівок щодо того, як ці заборони щодо застосування сили застосовуватимуться в кібер-контексті (детальніше це питання розглянуто в наступних параграфах).

Розбіжність у підходах чітко проявляється в площині інформаційної безпеки, оскільки інформаційні загрози, по-перше, по різному формулюються представниками обох таборів, а по-друге, мають ряд специфічних рис, що ускладнює їх ідентифікацію як таких. Норми міжнародного права ґрунтуються на історичному досвіді, але у зв'язку з швидким розвитком ІКТ й трансформацією системи суспільних комунікацій, сьогодні залишаються актуальними певні проблеми.

Розглянута вище проблема підходів до розуміння силового військово-політичного впливу в інформаційному/кібер-просторі має загальний характер і викликає суперечки на міжнародних майданчиках найвищого рівня. Але, окрім того, предметній сфері кіберпростору властивий також ряд особливостей, пов'язаних зі специфікою його організації й функціонування, які накладають відбиток на безпекові проблеми. Загалом щодо потенційно загрозливих операцій у кіберпросторі застосовується термін "кібервійна", — війна, що ведеться в комп'ютерах та із комп'ютерів і мереж, що їх пов'язують, ведеться державами чи їхніми довіреними особами проти інших держав. Кібервійну зазвичай ведуть проти урядових і військових мереж із метою їх пошкодження, знищення чи

[111] Правила поведения в области обеспечения международной информационной безопасности, Документ ООН A/69/723/, 13 января 2015.

блокування їх використання[112]. Якщо інтерпретувати це поняття в аспекті застосування міжнародного гуманітарного права, то кібервійна охоплює засоби й методи ведення військових дій, що є операціями, спрямованими проти комп'ютерів, або через комп'ютери чи комп'ютерні мережі шляхом інформаційного потоку, коли такі операції в кіберпросторі здійснюються в контексті збройного конфлікту за змістом МГП[113]. Тобто поняття "кібервійна" є вужчим порівняно з "інформаційною війною" й "інформаційними операціями" в різних трактуваннях, що розглянуто вище.

Із точки зору застосування міжнародного права кібервійна породжує цілий ряд проблем. Насамперед це проблема ідентифікації сторін конфлікту, адже в умовах інформаційного протиборства засоби враження не прив'язані до території й не мають розпізнавальних знаків, а їхню національну належність можливо встановити лише за опосередкованими ознаками. Відповідно проблематично встановити й ініціатора конфлікту, принаймні це потребуватиме значного часу. Це ж стосується і встановлення суб'єкта відповідальності, — взагалі кібер-операція може здійснюватись особами, що навіть не підозрюють про їхню роль в конфлікті (наприклад цивільними, що працюють на певну інтернет-компанію, що в свою чергу виконує підряд екстериторіального замовника), тому, якщо неможливо встановити особу, організацію чи державу-замовника, то таку діяльність складно ідентифікувати як операцію військового конфлікту. Окрім того, такі операції можуть мати значний прихований період, коли вони себе не проявляють, або проявляють без якихось руйнівних наслідків. Тому в цей час практично неможливо визначити наявність конфлікту. Також важко ідентифікувати сторону конфлікту своєчасно.

Неможливість ідентифікації сторони, що здійснює конкретну операцію в кіберпросторі, створює критичну проблему для застосування МГП до цієї операції, причому в цьому аспекті, крім юридичних, виникають також і технічні

[112] Cyberwar. Bratannica. URL: https://www.britannica.com/topic/cyberwar

[113] ICRC 'How is the Term "Armed Conflict" Defined in International Humanitarian Law?', Opinion paper, March 2008. URL: http://www.icrc.org/eng/assets/files/other/opinion-paper-armed- conflict.pdf

питання. Кібер-діяльність у контексті інформаційного протиборства може мати як військовий, так і невійськовий прояви, а отже виникає питання — чи буде вона сприйнята в якості “збройної сили”. Також, якщо інформаційний вплив і буде трактовано як “загрозу силою”, то, відповідно до ст. 2 Статуту ООН, швидше за все він не буде однозначно спрямованим проти “територіальної недоторканності чи політичної незалежності будь-якої держави” і вимагатиметься обґрунтування його дії будь-яким іншим чином, несумісним з цілями Об’єднаних Націй. Загроза силою, відповідно до ст. 2, трактується як така, що має носити примусовий характер і потрібна чітка заява про намір застосувати силу[114]. Але інформаційна загроза, через складність її ідентифікації, становить проблему для такого трактування. А в умовах гібридних воєн така загроза силою взагалі може заперечуватися стороною конфлікту.

Якщо операції в кіберпросторі застосовуються у взаємозв’язку з конвенційними кінетичними озброєннями, наприклад втручання в роботу систем протиповітряної оборони в ході конфлікту, то їх ідентифікація може здійснюватися за ознаками останніх. Також і у випадку згаданого вище прецеденту застосування ракетного удару проти локації джерела кіберзагрози останнє, по суті, може бути до певної міри ідентифіковане за певними матеріальними об’єктами, як у випадку зруйнованих комп’ютерних систем ХАМАС.

Значно складніше ідентифікувати операцію в кіберпросторі, якщо вона виступає окремим актом. І взагалі кваліфікація такого інциденту в аспекті jus ad bellum, як застосування сили чи збройний напад, відповідно до Статуту ООН, досить проблематична, навіть у випадку очевидного руйнування інфраструктурних об’єктів під упливом комп’ютерної програми. Зрозуміло, що згаданий вище комп’ютерний хробак Stuxnet був спеціально розроблений із метою кібер-нападу, який мав суттєві політичні наслідки через підрив іранської

[114] Xinmin Ma (2013) 马新民，“The Law of Use of Force: Development and Challenges,” China International Law Yearbook 1, 中国国际法年刊 (2013), 93.

ядерної програми, але відкритим залишається питання — чи мав Іран право на відповідь із застосуванням зброї кінетичної дії? Якщо так, то проти якої сторони він цю зброю міг би застосувати?

Також складно ідентифікувати операції в кіберпросторі й із точки зору jus in bello, тобто у сфері застосування міжнародного гуманітарного права. Очевидно, що у випадку чітко визначеного кінетичного впливу кіберзасобів у ситуаціях збройних конфліктів, відповідно до Женевських конвенцій 1949 р. і Додаткових протоколів до них 1977 р., вони можуть розглядатися так як і кінетична зброя, якщо їх дія буде аналогічною, тобто мати наслідком руйнування важливої інфраструктури з довготривалими наслідками, що створює серйозні труднощі для населення. Відповідно може здійснюватися захист цивільного населення від таких наслідків.

Специфічною проблемою, пов'язаною з "нематеріальністю" інформації та кібервпливів, є їх потенційна значущість в аспекті завданих збитків при одночасній "непомітності" такого впливу. Тобто виведення з ладу, скажімо, важливого інфраструктурного чи військового об'єкта через блокування керуючих процесорів спеціальною програмою не те ж саме, що його фізичне пошкодження зброєю кінетичної дії, хоча наслідки можуть бути не менш масштабними.

Будь-які акти насильства щодо супротивника, незалежно від того, здійснюються вони під час наступу чи під час оборони, відповідно до Додаткового протоколу I до Женевських конвенцій (Ст. 49), розцінюються як напади, а отже, по суті, їх інструментом можуть бути й кібер-засоби, тим більше, що це стосується "будь-яких військових дій на суші, в повітрі або на морі, які можуть завдати шкоди цивільному населенню, окремим цивільним особам або цивільним об'єктам[115]". Проте у цьому випадку мова може йти не про фізичне пошкодження таких об'єктів, а про втрату функціональності. Ще одним

[115] Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text

специфічним моментом є фактична неможливість ідентифікації осіб, які беруть участь у кібер-нападі (на противагу "звичайному" нападу, коли має місце ідентифікація учасників-комбатантів).

Також тим самим протоколом (Ст. 51) заборонені невибіркові напади, що у свою чергу викликає проблему, оскільки кібер-операції зазвичай здійснюються через інтернет, що ускладнює їх фокусування на чітко визначених об'єктах. При цьому суттєвих пошкоджень можуть зазнавати, як у випадку Stuxnet, їх певні категорії. Але в той же час універсальність інтернету й взаємопов'язаність усіх його мереж, вузлів і ліній передачі даних призводять до неможливості гарантувати вибірковість нападу, оскільки атака на військові об'єкти може "попутно" зачіпати цивільні мережі і їх користувачів, призводячи до непередбачуваних наслідків в аспекті їх функціонування.

Талліннський посібник

Питання щодо можливості застосування міжнародного права у сфері кібер-воєн стало ще актуальнішим після скоординованої кібератаки на комп'ютерні системи державних установ Естонії в квітні—травні 2007 р. на тлі загострення російсько-естонських відносин, пов'язаних із перенесенням монумента Невідомому солдату в Таллінні. У відповідь на такі атаки з боку НАТО вжито невідкладних заходів, зокрема проведено внутрішню оцінку кібербезпеки й інфраструктурного захисту з оприлюдненням у жовтні того ж року відповідного звіту[116]. Це стало початком розвитку політики Альянсу в галузі кіберзахисту. Вже в травні 2008 р. в Таллінні створено Центр передового досвіду кіберзахисту НАТО (CCDCOE), який наприкінці 2009 р. зібрав міжнародну групу юристів і практиків, щоб розробити посібник, у якому б роз'яснювалися питання щодо застосування існуючих норм міжнародного права, зокрема права початку війни й міжнародного гуманітарного права, в контексті кібер-операцій та кібервійни. У квітні 2013 р. опубліковано перше видання так званого "Талліннського посібника" "The Tallinn Manual on the International Law Applicable to Cyber

[116] 2007 cyber attacks on Estonia. URL: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

Warfare"[117], який противники застосування міжнародного права в кіберпросторі (найбільше — в Росії) називають набором рекомендацій щодо ведення кібервійни й обґрунтуванням застосування фізичної сили у відповідь на кібернапади[118]. Проте Талліннський посібник не є офіційним документом, а являє собою лише точку зору учасників робочої групи фахівців, які, зважаючи на відсутність загальновизнаних міжнародних норм з кібербезпеки, наводять оцінку застосовності чинних норм до цієї сфери. Формат проєкту не був новим. Подібним чином на початку 2000-х рр. у рамках програми з дослідження гуманітарної політики й конфліктів Гарвардського університету опрацьовано Посібник із міжнародного права, що застосовується в повітряному й ракетному протиборстві[119].

Талліннський посібник — це науково обґрунтована відповідь на ряд принципових питань у сфері інформаційної (кібер) безпеки з точки зору як міжнародного співробітництва в цій сфері, так і з позиції вироблення національних підходів і політик. Насамперед автори впорядкували ряд понять і концептуальних речей, що традиційно викликають гострі розбіжності з позиції різних держав, зокрема прихильників західного й східного підходів. Так, по-перше, однозначно стверджується, що Міжнародна група експертів відкинула будь-які твердження про те, що кіберпростір є новим доменом у сфері міжнародно-правового регулювання. Навпаки — до нього застосовуються загальні принципи міжнародного права. По-друге, щодо популярної в Росії й Китаї концепції "кіберсуверенітету", встановлено, що жодна держава не може претендувати на суверенітет над кіберпростором як таким, але може застосовувати суверенні прерогативи щодо будь-якої інфраструктури кіберпростору, розташованої на їх території, а також діяльності, пов'язаної з цією кіберінфраструктурою ("суверенітет, яким володіє держава над територією,

[117] Schmitt Michael N. (ed.) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press.

[118] "Таллинское руководство" о войне в интернете встревожило Россию - этот документ сам по себе опасен. *NEWSru.com*. 27.05.2013. https://www.newsru.com/hitech/27May2013/cyber.html

[119]HPCR Manual on International Law Applicable to Air and Missile Warfare. Bern, 15 May 2009. URL: https://reliefweb.int/sites/reliefweb.int/files/resources/8B2E79FC145BFB3D492576E00021ED34-HPCR-may2009.pdf

дає їй право контролю кібер-інфраструктури та кібер-діяльності на її території"). Звідси — логічний висновок, що кібер-операція держави, спрямована проти кібер-інфраструктури, розташованої в іншій державі, може порушити суверенітет останньої. І критерієм такого порушення є завдання шкоди, хоча міжнародна група експертів не змогла досягти єдиної думки щодо того, чи буде розміщення шкідливого програмного забезпечення, яке не завдає фізичної шкоди (як і у випадку зі шкідливим програмним забезпеченням, яке використовується для моніторингу діяльності) порушенням суверенітету. Також кібер-операція може кваліфікуватися як "збройний напад", що провокує право особистої або колективної самооборони. А дії, які не є збройним нападом, але тим не менше порушують норми міжнародного права, можуть дати право державі-цілі вдаватися до контрзаходів. Держава, що стала жертвою "збройного нападу" в кіберпросторі, що спричинило людські жертви або іншу серйозну шкоду, має право відповісти за допомогою сили в кіберпросторі або фізичному світі.

Важливим моментом є кваліфікація конфліктів, які ведуться в кіберпросторі. Автори посібника, по-перше, фіксують їх актуальність, а по-друге, встановлюють відповідність цього феномена міжнародному поняттю "збройний конфлікт", що відповідно дає підстави для застосування норм МГП. Відтак керівництво кіберопераціями, що призвели до жертв серед цивільного населення (або можуть спричинити таку шкоду) класифікується як військові злочини.

Звісно, до кібероперацій мають застосовуватися й інші норми jus in bello, зокрема щодо спрямування проти конкретних цілей і об'єктів, заборона "віялових" атак, які можуть зачепити цивільне населення, заборона атак на об'єкти, необхідні для виживання цивільного населення (лікувальні установи, продовольчі магазини, об'єкти житлово-комунального господарства), а також випадкові напади на некомбатантів.

Також держави несуть відповідальність за кібероперації проти інших держав, які ведуться з їх території, навіть якщо такі операції ведуться не спецслужбами, але при цьому держава підтримує тих, хто атакує інші країни. У

цьому аспекті відзначимо допустимість застосування контрзаходів щодо кібертерористів, у т. ч. й на території іноземних держав.

У 2017 р. опубліковано новий посібник, відомий як "Tallinn 2.0[120]" Перше видання Талліннського посібника зосереджене на найбільш руйнівних кібер-операціях, які можна кваліфікувати як "збройні атаки" що дозволяє державам застосовувати заходи захисту, а також на тих, що відбуваються під час збройного конфлікту. Натомість Таллінн 2.0 охоплює кібер-операції, а не кібер-конфлікти, як у видані 2013 р.

[120] Schmitt, Michael N. (ed.) (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. NATO Cooperative Cyber Defence Centre of Excellence.

Розділ 2. НАЦІОНАЛЬНІ Й РЕГІОНАЛЬНІ ПІДХОДИ ДО БЕЗПЕКИ КІБЕРПРОСТОРУ

2.1. Підхід Росії

Сьогодні національні підходи до інформаційної безпеки суттєво відрізняються, але інформаційні загрози мають глобальний характер і очевидно, що державам необхідно досягти згоди щодо універсальних норм використання кіберпростору. Проте міжнародної згоди поки що досягти не вдалося. Східний підхід не узгоджується з західним і ці розходження з часом проявляються все більше.

Офіційний підхід Росії називається “міжнародна інформаційна безпека”. Ця позиція відображена в проєкті Конвенції про забезпечення міжнародної інформаційної безпеки (2011 р.)[121], опублікованому на веб-сайті Міністерства закордонних справ РФ. Тут інформаційна безпека розглядається як ”стан захищеності інтересів особистості, суспільства й держави від загроз деструктивних та інших негативних упливів у інформаційному просторі”, а ”міжнародна інформаційна безпека“ — як ”стан міжнародних відносин, що виключає порушення світової стабільності та створення загрози безпеці держав і світової спільноти в інформаційному просторі”. Документ чітко відображає позицію Росії, суть якої — в упередженому ставленні до міжнародного оточення як до джерела “інформаційних загроз“. Причому складено докладний перелік цих загроз і наголошено на тому, що це — ”основні загрози міжнародному миру й безпеці в інформаційному просторі”. У переліку домінують типові для східного підходу застереження проти потенційних ворогів, зокрема[122]:

- використання інформаційних технологій і засобів для здійснення ворожих дій і актів агресії;

[121] CONVENTION ON INTERNATIONAL INFORMATION SECURITY. The Ministry of Foreign Affairs of the Russian Federation. URL: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

[122] Там само.

- неправомірне використання інформаційних ресурсів іншої держави без узгодження з державою, в інформаційному просторі якої розташовуються ці ресурси;
- дії в інформаційному просторі з метою підриву політичної, економічної та соціальної систем іншої держави, психологічна обробка населення, що дестабілізує суспільство;
- маніпулювання інформаційними потоками в інформаційному просторі інших держав, дезінформація та приховування інформації з метою спотворення психологічного й духовного середовища суспільства, ерозія традиційних культурних, моральних, етичних і естетичних цінностей;
- протидія доступу до новітніх інформаційно-комунікаційних технологій, створення умов технологічної залежності у сфері інформатизації на шкоду іншим державам;
- інформаційна експансія, отримання контролю над національними інформаційними ресурсами іншої держави.

Предметно розкривають позицію Росії в аспекті задекларованої нею "Міжнародної інформаційної безпеки" згадані вище "Основи державної політики Російської Федерації в галузі міжнародної інформаційної безпеки"[123], оновлений варіант яких прийнято в 2021 р. Це документ стратегічного планування РФ, який відображає офіційні погляди на сутність того, що в Росії називають міжнародною інформаційною безпекою, й визначає основні загрози "міжнародній інформаційній безпеці", мету й завдання державної політики Росії в цій сфері. По суті, тут конкретизуються окремі положення Стратегії національної безпеки РФ, Доктрини інформаційної безпеки, Концепції зовнішньої політики й інших документів стратегічного планування РФ. Зусилля Росії спрямовані на формування блоку міжнародної підтримки її політики й так званої "системи забезпечення міжнародної інформаційної безпеки", яка має

[123] Основы государственной политики Российской Федерации в области международной информационной безопасности (Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213). URL: http://www.scrf.gov.ru/security/information/document114/

являти собою сукупність міжнародних і національних інститутів, що регулюють діяльність у глобальному інформаційному просторі з метою запобігання (мінімізації) загроз цій міжнародній інформаційній безпеці.

У згаданому документі також перераховано “загрози міжнародній інформаційній безпеці”, серед яких:

- використання інформаційно-комунікаційних технологій у військово-політичній та інших сферах з метою підриву (обмеження) суверенітету, порушення територіальної цілісності держав, здійснення в глобальному інформаційному просторі інших дій, що перешкоджають підтриманню міжнародного миру, безпеки й стабільності;
- використання інформаційно-комунікаційних технологій у терористичних цілях, в тому числі для пропаганди тероризму й залучення до терористичної діяльності нових прихильників;
- використання інформаційно-комунікаційних технологій в екстремістських цілях, а також для втручання у внутрішні справи суверенних держав;
- використання інформаційно-комунікаційних технологій в злочинних цілях, в тому числі для здійснення злочинів у сфері комп’ютерної інформації, а також для здійснення різних видів шахрайства;
- використання інформаційно-комунікаційних технологій для проведення комп’ютерних атак на інформаційні ресурси держав, у тому числі на критичну інформаційну інфраструктуру;
- використання окремими державами технологічного домінування в глобальному інформаційному просторі для монополізації ринку інформаційно-комунікаційних технологій, обмеження доступу інших держав до передових інформаційно-комунікаційних технологій, а також для посилення їх технологічної залежності від домінуючих в сфері інформатизації держав та інформаційної нерівності.

Як бачимо, окрім загроз, пов’язаних з кіберзлочинністю, кібертероризмом і враженням критичної інфраструктури, відкриває й замикає список класична

пересторога перед потенційними загрозами військово-політичного впливу й технологічного відставання, асоційовані з загрозами міжнародному миру, безпеці й стабільності, — відповідно до формату міжнародних майданчиків найвищого рівня. Виходячи з такої позиції, Росія намагається врегулювати міжнародний інформаційний простір для мінімізації зазначених загроз для себе.

Сьогодні зовнішня політика Росії в цій сфері базується на просуванні прийнятої нею ідеї "міжнародної інформаційної безпеки". Росія першою запустила на майданчику ООН дискусію з цієї проблеми, представивши у 1998 р. проєкт резолюції "Досягнення в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки[124]" на засіданні Першого комітету Генеральної Асамблеї. Проєкт був прийнятий без голосування і з тих пір Генеральний секретар щороку подавав Генеральній Асамблеї доповідь, що містить позиції держав — членів Організації Об'єднаних Націй із цієї теми. Спочатку російську ініціативу підтримували неохоче, але через постійне наголошення Росією своєї позиції проблема інформаційної безпеки закріплювалася в порядку денному ООН та інших міжнародних майданчиків, таких як Шанхайська організація співробітництва, Співдружність незалежних держав, Організація договору про колективну безпеку та БРІКС. Росія також ініціювала роботу Групи урядових експертів (ГУЕ, UN GGE) — органу ООН, який об'єднує експертів із різних країн для обговорення питань управління інтернетом і пошуку спільного порозуміння.

Загалом РФ здійснює чітку й послідовну реалізацію своїх інтересів через позицію в сфері інформаційної безпеки. Відповідно до вже згаданих "Основ державної політики Росії в області міжнародної інформаційної безпеки[125]", прийнятих у квітні 2021 р., метою державної політики в галузі міжнародної інформаційної безпеки є "сприяння встановленню міжнародно-правового режиму, при якому створюються умови для запобігання (врегулювання)

[124] Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. UN. A/RES/53/70. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R

[125] Основы государственной политики Российской Федерации в области международной информационной безопасности (Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213). URL: http://www.scrf.gov.ru/security/information/document114/

міждержавних конфліктів у глобальному інформаційному просторі, а також для формування з урахуванням національних інтересів Російської Федерації системи забезпечення міжнародної інформаційної безпеки". Досягнення цієї мети здійснюється шляхом розв'язання завдань щодо розвитку співробітництва РФ з іноземними державами з питань формування цієї "системи забезпечення міжнародної інформаційної безпеки", а також "протидії основним загрозам міжнародної інформаційної безпеки на глобальному, регіональному, багатосторонньому й двосторонньому рівнях"[126].

Суть російського підходу до міжнародного співробітництва у сфері інформаційної безпеки, як показано вище, полягає в установленні спеціального міжнародно-правового режиму, тобто по суті, — правових важелів упливу на інформаційне суспільство, головними рушіями якого поки що є інформаційно-комунікаційні технології, — сфера, де традиційно лідирують країни Заходу. Зокрема на рівні ООН РФ діє в напрямі створення умов для прийняття державами — членами згаданої вище "Конвенції про забезпечення міжнародної інформаційної безпеки" і вироблення, з урахуванням специфіки інформаційно-комунікаційних технологій, нових принципів і норм міжнародного права, що регулюють діяльність держав у глобальному інформаційному просторі.

Як дієвий інструмент для досягнення своїх цілей Росія використовує спеціально розроблену термінологію, послідовно просуваючи й закріплюючи її на міжнародних майданчиках. Наприклад, серед термінів і визначень, уміщених в текст "Конвенції про забезпечення міжнародної інформаційної безпеки", можна знайти такий: "Загроза в інформаційному просторі (загроза інформаційній безпеці)" — чинники, що створюють небезпеку для особистості, суспільства, держави і їх інтересів у інформаційному просторі". І далі — в переліку таких загроз — "протидія доступу до новітніх інформаційно-комунікаційних технологій, створення умов технологічної залежності в сфері інформатизації на

[126] Там само.

шкоду іншим державам” [127] . Тобто з позиції Росії технологічна перевага, отримана на основі вільної конкурентної боротьби на світовому ринку ІКТ, також становить загрозу інформаційній безпеці, якщо власник технології добровільно не надасть її в розпорядження тим, хто такою технологією не володіє. Очевидно, Росія в такий спосіб намагається нівелювати своє все більш відчутне технологічне відставання у сфері ІТ. З іншого боку російська ідея міжнародної інформаційної безпеки передбачає значну відповідальність уряду й контроль над інформаційними ресурсами, що не відповідає інтересам учасників ринку ІКТ.

Тому Росія, просуваючи ці ідеї на міжнародному рівні, стикається зі значним спротивом західних країн, які відстоюють свободу ринку, гарантії вільної конкуренції й недоторканості інформації з точки зору приватної власності. Також держави Заходу традиційно пропонують підходи, засновані на прозорості, що також не підтримується російськими чиновниками через нібито загрозу національному суверенітету. З такої причини, наприклад, у 2012 р. Росія заблокувала резолюцію про раннє попередження про кібератаки в ОБСЄ[128].

Специфічно подається в тлумаченні російського проєкту згаданої вище конвенції поняття “Інформаційний простір”, — як “сфера діяльності, пов'язана з формуванням, створенням, перетворенням, передаванням, використанням, зберіганням інформації, що здійснює вплив, у тому числі на індивідуальну й суспільну свідомість, інформаційну інфраструктуру та власне інформацію”. На відміну від більш поширеного в російськомовному науковому сегменті конструктивного розуміння “інформаційного простору” як сукупності інформаційних ресурсів, створених суб’єктами інформаційної сфери, засобів взаємодії таких суб’єктів, їх інформаційних систем і необхідної інформаційної

[127] CONVENTION ON INTERNATIONAL INFORMATION SECURITY. The Ministry of Foreign Affairs of the Russian Federation. URL: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

[128] Sternstein Aliya (2012). Cyber early warning deal collapses after Russia balks. *Nextgov,* 7 Dec. 2012. URL: https://www.nextgov.com/cybersecurity/2012/12/cyber-early-warning-deal-collapses-after-russia-balks/60035/

інфраструктури (див., наприклад, у [129],[130]), тут це поняття відображає політичну точку зору російського керівництва на суть міжнародних відносин в інформаційній сфері, як спосіб отримати певні вигоди для держави-актора.

Натомість у західному баченні переважно розглядається концепт кіберпростору — "Cyberspace", який визначається в рекомендації "Про розвиток і використання багатомовності й загальному доступі до кіберпростору", прийнятій на 32-й сесії Генеральної конференції ЮНЕСКО у 2003 р., як "віртуальний світ цифрової й електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою [131] ". Наукове визначення інформаційного простору в західному трактуванні наближене до кіберпростору: "Тип інформаційної конструкції, в якій репрезентації інформаційних об'єктів розташовані в організованому просторі. У такому просторі розташування й напрямок мають значення, таким чином стають можливими створення карт і навігація[132]".

У розглянутому в попередньому параграфі дослідженні "Талліннський посібник" (2013) запропоновано визначення кіберпростору як середовища, сформованого з фізичних і нефізичних елементів, яке характеризується використанням комп'ютерів та електромагнітного спектру для зберігання, зміни й обміну даними з використанням комп'ютерних мереж[133].

У типовому навчальному плані НАТО з кібербезпеки (2016 р.)[134] є модуль "Структура інформаційного простору: опорна мережа інтернету й мережева інфраструктура держав", присвячений виключно технічним аспектам

[129] Ryjov Alexander P., Mikhalevich Igor F. (2020). Hybrid Intelligence Framework for Improvement of Information Security of Critical Infrastructures. In *Handbook of Research on Cyber Crime and Information Privacy.* P. 310—337.

[130] Манойло А.В. (2003). *Государственная информационная политика в особых условиях: Монография.* Москва. МИФИ. 388 с.

[131] Рекомендация о развитии и использовании многоязычия и всеобщем доступе к киберпространству. Принята 15 октября 2003 года. URL: https://www.un.org/ru/documents/decl_conv/conventions/multilingualism_recommendation.shtml

[132] MIT Artificial Intelligence Laboratory, *The JAIR Information Space*, *MIT Artificial Intelligence Laboratory.* 10 June 1998. URL: http://www.ai.mit.edu/projects/infoarch/jair/jair-space.html

[133] Schmitt, Michael N. (ed.) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York. Cambridge University Press. URL: http://www.cambridge.org/tallinnmanual2

[134]DEEP: Cybersecurity – A Generic Reference curriculum. NATO. URL: https://www.nato.int/cps/en/natohq/topics_157591.htm

інформаційного простору. Основна увага при цьому надається глобальній інфраструктурі, а також інформаційним системам, створеним у масштабі держав і окремих підприємств. А інформаційний простір включає в себе архітектуру інтернету, комп'ютерні й мобільні мережі, де в першу чергу розглядаються принципи загальної структури й конкретна топологія інтернету в окремих державах (тобто національна інфраструктура, що підтримує роботу мереж, провайдери телекомунікаційних послуг, а також схеми маршрутизації).

Як йшлося вище, Росія систематично подає проєкти резолюцій ГА ООН з питань безпеки інформаційного простору. Суть їх незмінна й серед членів ООН існує група держав, які ці резолюції традиційно підтримують. Це, зокрема, члени БРІКС, ШОС і частина країн, що розвиваються. Наприклад Резолюцію 73/27 2018 р. "Досягнення у сфері інформатизації й телекомунікацій в контексті міжнародної безпеки[135]", яка просувалася Росією в співавторстві з 32 державами, підтримали 119 держав, 46 — проти, 14 утрималися.

Ця резолюція має декілька ключових особливостей. По-перше, вона спрямована на захист інтересів усіх країн в цифровій сфері незалежно від того, на якому рівні технологічного розвитку вони знаходяться. У зв'язку з цим наголошується на важливості надання допомоги деяким державам для подолання розриву в сфері інформаційно-комунікаційних технологій, що, на думку авторів документа, має важливе значення для міжнародної безпеки. По-друге, в резолюції представлено перелік правил, норм і принципів поведінки держав в інформаційному просторі з оголошеною метою — закласти основу мирної взаємодії держав у ІКТ-середовищі, забезпечити запобігання воєн, конфронтації й будь-яких агресивних дій.

У документі 2018 р., на відміну від резолюцій, які раніше щорічно вносилися Росією й містили лише згадки про необхідність вироблення правил поведінки держав у мережі, вперше перераховані ці норми (усього 13 пунктів).

[135] 73/27. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27&Lang=R

Наприклад, першим пунктом сформульовано, що “відповідно до цілей Статуту Організації Об'єднаних Націй, в тому числі що стосуються підтримання міжнародного миру й безпеки, держави повинні співпрацювати в розробці й здійсненні заходів зі зміцнення стабільності й безпеки в використанні ІКТ і запобігання вчиненню дій в сфері ІКТ, визнаних шкідливими, або здатних створити загрозу міжнародному миру й безпеці”.

У другому пункті зазначено, що держави не повинні огульно звинувачувати одна одну в протиправних діях в інтернеті, а всі подібні претензії повинні бути “обґрунтованими” (хоча як саме має здійснюватися обґрунтування цих звинувачень, не уточнено). Також у переліку “норм” є заборона державам дозволяти використовувати свою територію та інфраструктуру для здійснення кібератак, і зобов'язання співпрацювати “з метою обміну інформацією, надання взаємодопомоги, переслідування осіб, винних у терористичному й злочинному використанні інформаційно-комунікаційних технологій”. Наголошується на забороні країнам здійснювати кібератаки щодо критично важливої інфраструктури й зобов'язанні “задовольняти прохання про надання допомоги, що надходять від інших держав, критично важлива інфраструктура яких стає об'єктом зловмисних дій”. В останньому пункті зазначено, що “держави повинні співпрацювати з приватним сектором і організаціями громадянського суспільства в області здійснення правил відповідальної поведінки держав в інформаційному просторі з урахуванням їх потенційної ролі”.

При складанні цього переліку автори, очевидно, спиралися на документ Шанхайської організації співпраці (ШОС) від 2015 р. “Правила поведінки в галузі забезпечення міжнаціональної інформаційної безпеки[136]“, намагаючись унести в документ і такі норми, як ”неприпустимість використання кіберзасобів для втручання в справи держав і їх дестабілізації”, а також про можливості обмеження прав і свобод користувачів за певних умов, зокрема ”для охорони

[136] Правила поведения в области обеспечения международной информационной безопасности, Документ ООН A/69/723/, 13 января 2015. URL: https://bit.ly/31dRCX0

державної безпеки, громадського порядку, здоров'я чи моральності населення”[137]. Проте у підсумковий текст вони не увійшли.

Хоча західні політичні системи виявилися більш ефективними в інформаційну еру, Росія дотримується консервативних політичних традицій. Країни Заходу отримують вигоди від інформаційної ери, тоді як російська економіка все ще значною мірою покладається на експорт енергоносіїв і низькотехнологічне ресурсоємне виробництво. На все більш помітне технологічне відставання в IT-сфері російський уряд реагує шляхом посилення інформаційної політики на внутрішньому рівні. Ця тенденція призводить до подальшої фрагментації російського сегмента кіберпростору та до ізоляції Росії в міжнародних відносинах. Нездатність російської політичної системи адаптуватися до реалій інформаційної епохи спричиняє відсутність довіри до західного світу й пошук шляхів змінити ситуацію на свою користь через міжнародні інститути, де Росія історично має суттєві важелі впливу.

Об’єктивно одним з головних результатів раніше прийнятих резолюцій було створення в 2004 р з ініціативи російської сторони Групи урядових експертів у сфері інформатизації й телекомунікації в контексті міжнародної безпеки, — з метою вивчення існуючих і потенційних загроз із боку ІКТ середовища й можливих спільних заходів щодо їх усунення. Проте вже перша група завершила свою роботу без доповіді через гострі суперечності між позиціями США й Росії з питання використання інформації й контенту як фактора загрози національній безпеці держави. Потім були скликані ще 3 групи, які завершили свою роботу консенсусними доповідями в 2010, 2013 і 2015 рр., але робота п'ятої групи в 2017 р. закінчилася невдачею, оскільки учасники не змогли дійти згоди щодо питання застосування права держави на самооборону у відповідь на шкідливе використання ІКТ, а також застосування міжнародного гуманітарного права до кіберпростору. Також російські представники не погоджувалися з тим, що США

[137] Россия и США перетягивают всемирную паутину. В ООН представлены конкурирующие резолюции по кибербезопасности. *Коммерсантъ*. №207. 12.11.2018, с. 6. URL: https://www.kommersant.ru/doc/3797617

наполягали на включенні в доповідь пункту про право держав на самооборону в кіберпросторі.

Свою роль зіграли й напружені відносини між Росією і США, які є одними з постійних учасників ГУЕ. Як відомо, американська сторона звинуватила Росію у втручанні в американські президентські вибори 2016 р., а також в скоєнні кібератак і проведенні інформаційних кампаній у соціальних мережах. Більш того, висловлювалися думки, що формат ГУЕ себе зжив і необхідно шукати нові майданчики для обговорення правил відповідальної поведінки держав у кіберпросторі. Проте робота ГУЕ 2019—2020 рр. успішно завершила свою роботу, прийнявши консенсусний звіт у травні 2021 р.[138], що свідчить про актуальність такого формату співпраці, хоча в 2018 р. з подачі Росії закладено новий майданчик для обговорення проблем інформаційної безпеки — Робочу групу відкритого складу (РГВС, OEWG), в якій беруть участь "усі зацікавлені держави" (детальніше про цю групу йтиметься далі).

Потрібно відмітити, що ГУЕ ООН складається "на основі справедливого географічного розподілу". Традиційно беруть участь у всіх ГУЕ п'ять постійних членів Ради Безпеки, а решта місць розподіляються за групами. На заклик до вираження інтересів держави надсилають офіційний запит про місце у Групі. Офіс Високого представника з питань роззброєння має завдання запропонувати склад Групи Генеральному секретарю. Більшість ГУЕ збиралися на кількатижневі сесії. Засідання експертів Групи закриті, без участі спостерігачів (чи то представників інших урядів, неурядових організацій, приватного сектора чи міжнародних організацій), без оголошення загальнодоступних підсумків засідань. Формат закритих дверей вважається важливим для відвертих дискусій, щоб дати можливість учасникам досягти згоди[139].

[138] Final Session of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. UNODA, 28 May 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/05/HR-remarks-at-Final-Session-of-the-Group-of-Governmental-Experts-on-Advancing-responsible-State-behaviour-in-cyberspace-in-the-context-of-international-security.pdf

[139] UNIDIR. Report of the International Security Cyber Issues Workshop Series. 2016. URL: https://www.unidir.org/publication/report-international-security-cyber-issues-workshop-series

Важливим фактом є підпорядкування ГУЕ Першому комітету ООН, відтак Група інтерпретує свій мандат, обмежуючи обсяг завдання. Перший Комітет є Головним Комітетом Генеральної Асамблеї й розподіляє питання порядку денного з питань роззброєння й міжнародної безпеки. Тому питання, які не входять до компетенції Першого Комітету, такі як шпигунство, управління інтернетом, розвиток і конфіденційність у цифровому режимі, технічні питання — не в пріоритетах роботи Групи. Наприклад неодноразово пропонувалося запросити Міжнародний телекомунікаційний союз (МСЕ, ITU), спеціалізоване агентство ООН, відповідальне за розробку технічних стандартів для ІКТ, в якості спостерігача в роботі Групи, що однак не було підтримано Генеральною Асамблеєю з огляду на те, що робота ГУЕ має бути зосереджена безпосередньо у сфері міжнародної безпеки й роззброєння[140].

У 2017 р. Росія представила проєкт конвенції ООН "Про співпрацю в сфері протидії інформаційній злочинності[141]". Документ розроблено як альтернативу Конвенції про комп'ютерні злочини Ради Європи (Будапештська конвенція), яку ратифікували всі країни ЄС, а також США, Японія, Австралія, Ізраїль (єдиною країною-членом Ради Європи, яка не підписала конвенцію, стала Росія). У Будапештській конвенції Москву не влаштувала стаття про ”транскордонний доступ до комп'ютерних даних, що зберігаються”, тобто можливість різним спецслужбам без офіційного повідомлення проводити операції в комп'ютерних мережах третіх країн і що, на думку уряду Росії, загрожує безпеці й суверенітету країни.

Наприкінці 2019 р. ГА ООН прийняла запропоновану Росією резолюцію щодо боротьби з кіберзлочинністю. Підтримана більшістю голосів Генеральної Асамблеї ООН резолюція “Протидія використанню інформаційно-

[140] UNIDIR. Report of the International Security Cyber Issues Workshop Series. 2016. URL: https://www.unidir.org/publication/report-international-security-cyber-issues-workshop-series

[141] Приложение к письму Постоянного представителя Российской Федерации при Организации Объединенных Наций от 11 октября 2017 года на имя Генерального секретаря Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности. URL: https://namib.online/wp-content/uploads/2020/04/Проект-Конвенции-Организации-Объединенных-Наций-о-сотрудничестве-в-сфере-противодействия-информационной-преступности.pdf

комунікаційних технологій в злочинних цілях[142]" фактично орієнтована на закріплення цифрового суверенітету держав над інформаційним простором, а під егідою Генасамблеї ООН створюється переговорний майданчик для розробки універсальної конвенції по боротьбі з кіберзлочинністю — спеціальний комітет у складі експертів з усіх країн світу (подібним чином просувалися конвенції ООН проти корупції та проти транснаціональної організованої злочинності). Разом з Росією співавторами цієї резолюції виступили 47 держав, серед яких Білорусь, Казахстан, Азербайджан, Таджикистан, Вірменія, Китай, Індія, Сирія, Єгипет, КНДР, Іран, і Венесуела. "Проти" проголосували США, Канада, Франція, Німеччина, Велика Британія, Україна і ще 54 держави.

Росія послідовно відстоює свій підхід, вважаючи, що поведінка держав і їх права в кіберпросторі повинні бути регламентовані міжнародними угодами, подібними до угод про космічний простір і мореплавство.

2.2. Підхід Китаю

Про основу підходу Китайського керівництва до проблематики загроз, пов'язаних із розвитком інформаційно-комунікаційної активності суспільства, вже згадано в першому розділі. Він у загальних рисах подібний до підходу Росії, полягаючи в широкому трактуванні саме "інформаційної безпеки", а не безпеки в кіберпросторі, й претензіях на управління певним сегментом цього самого кіберпростору (а в розумінні місцевої влади — частини всесвітньої мережі й інформаційних ресурсів, що належать до юрисдикції Китаю). Китай загалом послідовно підтримує ініціативи Росії щодо формування міжнародного режиму інформаційної безпеки на міжнародних форумах, виступаючи з нею єдиним табором в дискусіях на майданчику ООН і спільно висуваючи ініціативи на форумах у площині спільних інтересів (таких як ШОС).

[142] 74/247. Противодействие использованию информационнокоммуникационных технологий в преступных целях. Резолюция, принятая Генеральной Ассамблеей 27 декабря 2019 года. URL: https://undocs.org/ru/A/RES/74/247

Але в Китаю є власна траєкторія розвитку й стратегічне бачення національної безпеки, невід'ємною частиною якої політичне керівництво країни вбачає усе, що пов'язано з політико-ідеологічними, технічними й економічними аспектами безпеки в сферах інформації та ІКТ. Сучасна політика в сфері інформаційної безпеки почала формуватись із розгортанням процесів масового використання технологій мережної комунікації в усіх сферах суспільного життя. Китай пізніше за країни Заходу, лише у 1994 р., отримав доступ до інтернету, але з того часу швидкими темпами ліквідував технологічне відставання, при цьому створюючи власну унікальну систему відносин у сфері ІКТ. Головним принципом політики Китаю у сфері інформаційної безпеки є так званий "кіберсуверенітет", тобто безапеляційне застереження виключного права держави на контроль будь-якої інформації, технологій і телекомунікації в мережі. Причому цей контроль здійснюється виключно в інтересах правлячої Комуністичної партії Китаю (КПК). Провідна роль компартії в китайському суспільстві посилюється, особливо під керівництвом нинішнього лідера країни Сі Цзіньпіна, за словами якого "Лідерство Комуністичної партії Китаю є найважливішою ознакою соціалізму з китайськими особливостями... Партія, уряд, військові, громадяни й освіта, північ, південь, схід, захід і центр, партія є лідером у всьому[143]".

Курування питань національної безпеки в країні покладено на Центральну комісію з питань національної безпеки Китаю, а серед одинадцяти областей безпеки поряд із політичною, внутрішньою, військовою, економічною, виділено й інформаційну[144]. Система кібербезпеки в Китаї формується відповідно до

[143] **中国共**产党领导是中国特色社会主义最本质的特征. **来源**：《**求是**》2020/14 **作者**：习近平 (Zhōngguó gòngchǎndǎng lǐngdǎo shì zhōngguó tèsè shèhuì zhǔyì zuì běnzhí de tèzhēng. Láiyuán:"Qiú shì"2020/14 zuòzhě: Xíjìnpíng) [Лідерство Комуністичної партії Китаю є найважливішою ознакою соціалізму з китайськими особливостями. Джерело: "Пошук правди" 2020/14 Автор: Сі Цзіньпін]. Qishi. http://www.qstheory.cn/dukan/qs/2020-07/15/c_1126234524.htm

[144] Dingli Shen (2014). Framing China's National Security. *China/US Focus.* Apr 23, 2014. URL: https://www.chinausfocus.com/peace-security/%20%20framing-chinas-national-security

Комплексної концепції національної безпеки Сі Цзіньпіна[145], в якій традиційний військовий підхід до національної безпеки як до захисту кордонів трансформується й полягає в забезпеченні, по-перше, абсолютної влади КПК в управлінні Китаєм і, по-друге, таких умов для влади КПК, як швидкий розвиток країни в сфері високих технологій і контроль ідеології й інформації.

Сьогодні координація інформаційної безпеки країни здійснюється Центральною комісією КПК з кібербезпеки та інформатизації, яка об'єднує членів керівної групи з усебічного поглиблення реформ, Державного управління із захисту державної таємниці КНР, керівної групи з пропаганди й ідеології, а також велику кількість представників різних міністерств КНР. Вони грають роль спеціалізованих інститутів, забезпечуючи інформаційну безпеку в інтернет-просторі. У сфері зовнішньої політики Комісія діє спільно з Центральним комітетом з міжнародних справ[146]. Для роботи в цьому напрямі в складі Комісії сформовано Центральну малу групу із зовнішньої політики. Контроль інформації й кіберпростору в цивільній сфері здійснюється міністерствами й відомствами під патронатом Міністерства державної безпеки, а в промисловості — адміністрацією державних підприємств. У військовій сфері Китаю діє своя система інформаційної та кібер-безпеки Національно-визвольної армії Китаю (НВАК) за участі Держради, Постійного комітету політбюро ЦК КПК, Центральної комісії з державної безпеки, Центральної військової ради, установ і спеціалізованих управлінь у підпорядкуванні НВАК[147].

Центральній комісії з кібербезпеки й інформатизації підпорядковується провідний орган у сфері адміністрування безпеки кіберпростору —

---

[145] 全面贯彻落实总体国家安全观 为全方位推进高质量发展超越筑牢安全屏障 (Quánmiàn guànchè luòshí zǒngtǐ guójiā ānquán guān wèi quán fāngwèi tuījìn gāo zhìliàng fāzhǎn chāoyuè zhù láo ānquán píngzhàng) [Повністю реалізувати загальну концепцію національної безпеки, щоб всебічно сприяти високоякісному розвитку та вийти за межі створення міцного бар'єру безпеки]. 17.04.2021. URL: http://www.cac.gov.cn/2021-04/17/c_1620246064486609.htm

[146] Носов С. (2021). Система кибербезопасности в Китае (2021). *Зарубежное военное обозрение*. №2. С. 17-24. URL: http://factmil.com/publ/strana/kitaj/sistema_kiberbezopasnosti_v_kitae_2021/59-1-0-1833

[147] Ромашкина Наталья, Задремайлова Вероника (2020). Эволюция политики КНР в области информационной безопасности. *Пути к миру и безопасности*. № 1(58). С. 122-138. URL: https://www.imemo.ru/publications/periodical/pmb/archive/2020/1-58/in-focus-east-asia/security-policies-of-east-asian-states/evolution-of-chinas-information-security-policy

Адміністрація кіберпростору Китаю (Cyberspace Administration of China, CAC), заснований на тій же системі, що й Управління з питань зовнішньої пропаганди Комуністичної партії Китаю. CAC бере участь у формуванні та реалізації політики з різних питань, пов'язаних з китайським інтернетом. Серед областей, які регулює CAC, — імена користувачів у китайському інтернеті, доречність висловлювань, поширених в інтернеті, віртуальні приватні мережі, вміст інтернет-порталів та ін. Наприклад у травні 2020 р. оголошено восьмимісячну кампанію з ”очищення” політичного й релігійного онлайн-контенту, який вважається ”незаконним”. [148] CAC також здійснює деякі цензурні функції, включаючи видання директив медіа-компаніям у Китаї[149]. Причому під наглядом перебувають не лише публікації на веб-сайтах, а й коментарі до них, — під виглядом самодисципліни управління веб-сайтами. Наприклад, серед формулювання категорій заборонених коментарів такі, що: ”завдають шкоди національній безпеці”; ”шкодять честі або інтересам нації”; ”шкодять релігійній політиці нації”; ”поширюють чутки, порушують громадський порядок“ і якщо ”опублікована інформація не має сенсу або використовує комбінацію символів навмисно, щоб уникнути технічного огляду”[150]. У 2021 р. CAC запустила гарячу лінію, щоб повідомляти про онлайн-коментарі проти Комуністичної партії Китаю[151]. Крім того Адміністрація кіберпростору контролює безпеку пристроїв, виготовлених зарубіжними країнами й програмне забезпечення (у грудні 2020 р.

[148] 国家网信办启动 2020“清朗”专项行动，为期 8 个月. URL (Guójiā wǎng xìn bàn qǐdòng 2020“qīnglǎng” zhuānxiàng xíngdòng, wéiqí 8 gè yuè) [Управління кіберпростору Китайської Народної Республіки розпочало спеціальну кампанію «чистий» 2020 рік на 8 місяців]. URL: http://politics.people.com.cn/n1/2020/0522/c1001-31719589.html

[149] Qiang, Xiao (September 18, 2015). Congressional-Executive Commission on China (CECC) Hearing: Urging China's President Xi Jinping to Stop State-Sponsored Human Rights Abuses. URL: https://www.cecc.gov/sites/chinacommission.house.gov/files/CECC%20Hearing%20-%20Human%20Rights%20Abuses%20-%2018Sept15%20-%20Xiao%20Qiang.pdf

[150] 29 家网站签署《跟帖评论自律管理承诺书》. 2014 年 11 月 06 日 22:36 新华网 (29 Jiā wǎngzhàn qiānshǔ “gēn tiē pínglùn zìlǜ guǎnlǐ chéngnuò shū”. 2014 Nián 11 yuè 06 rì 22:36 Xīnhuá wǎng) [29 веб-сайтів підписали "Зобов'язання щодо самодисциплінованого менеджменту публікації коментарів". Сіньхуа, 06 листопада 2014]. URL: http://news.sina.com.cn/c/2014-11-06/223631106669.shtml

[151] Cadell Cate (2021). China launches hotline for netizens to report 'illegal' history comments. *Reuters,* 2021-04-11. URL: https://www.reuters.com/world/china/china-launches-hotline-netizens-report-illegal-history-comments-2021-04-11/

із магазинів додатків у Китаї видалено 105 програмних застосунків, які були визнані “незаконними”, щоб “очистити інтернет у Китаї”[152].

Також повідомлялося про те, що CAC систематично встановлює цензурні обмеження для китайських ЗМІ й соціальних мереж, регулюючи масову комунікацію щодо COVID-19, залучаючи фальшивих інтернет-коментаторів, щоб відволікати увагу в соціальних мережах від чутливих, з точки зору китайської влади, питань[153]. З 2013 року CAC, спільно з Міністерством громадської безпеки, здійснює технічне управління Великим брандмауером. Взаємопов’язані стратегії, закони, заходи, норми й стандарти в Китаї охоплюють правила захисту даних, критичної інфраструктури, шифрування, вмісту в інтернеті, а також зміцнення китайської індустрії ІКТ.

Отже сьогодні Китай перебуває в розпалі побудови найширшого режиму управління кіберпростором та ІКТ серед усіх країн світу. Очевидно враховуючи досвід режимів, які постраждали через те що технології розвивалися швидше, ніж здатність уряду контролювати їх, китайське керівництво формує політику й нормативно-правову базу, що під загальним наглядом КПК охоплює кібербезпеку, цифрову економіку й контент медіа в інтернеті.

Законодавство Китаю в сфері безпеки кіберпростору, незважаючи на порівняно невелику історію, розвивається досить динамічно. Перші правила регулювання для забезпечення безпеки комп’ютерних та інформаційних систем прийнято в 1994 р[154]. Саме тоді повноваження щодо контролю, інспекції й забезпечення національної інформаційної безпеки, розслідування, розкриття й запобігання злочинів у сфері ІКТ надано Міністерству державної безпеки Китаю. Вже в 1997 р. прийнято закон про безпеку мережної інфраструктури й мережі

[152] Soo Zen (2020). China orders removal of 105 apps, including TripAdvisor. *Associated Press,* December 9, 2020. URL: https://apnews.com/article/media-prostitution-china-hong-kong-pornography-84314d74600bd87d6dcea77524e43ed7

[153] Zhong, Raymond; Mozur, Paul; Krolik, Aaron; Kao, Jeff (2020). "Leaked Documents Show How China's Army of Paid Internet Trolls Helped Censor the Coronavirus". *ProPublica*, December 19, 2020.

[154] 计算机信息系统安全管理制度 (Jìsuànjī xìnxī xìtǒng ānquán guǎnlǐ zhìdù) [Система управління безпекою комп'ютерної інформаційної системи]. URL: https://wenku.baidu.com/view/8814c60716fc700abb68fc31.html.

Інтернет, що стало одним з перших кроків на шляху до розбудови ”кібернетичного суверенітету” Китаю. Цим актом уведено заборону на використання мережі для створення, поширення, копіювання чи передачі певних видів інформації, до яких віднесено заклики до невиконання чи порушення державних законів, терористичної діяльності або порушення цілісності країни (”Користувачам забороняється використовувати інтернет для створення, тиражування, пошуку чи передачі інформації, яка викликає опір Конституції КНР, законам чи адміністративним нормам; сприяння поваленню уряду чи соціалістичної системи; підриву національного об’єднання; спотворення правди, поширення чуток або руйнування суспільного ладу...[155]”).

Протягом 2000—2015 рр. прийнято ряд нормативних актів у сфері регулювання кібербезпеки в Китаї, зокрема документи стратегічного планування, які визначали горизонти інформатизації в країні разом із основними напрямами регулювання. Наприклад Державна стратегія з розвитку інформатизації на період 2006—2020 рр., серед стратегічних цілей якої — “Створити національну систему гарантій інформаційної безпеки“ [156]. У 2012 р. прийнято документ Держради КНР із просування інформатизації й розвитку діючої системи захисту інформаційної безпеки, яким установлювався контроль над інтернет-додатками, віртуальними угодами в торгово-економічній сфері, інформаційно-мовними послугами, упроваджено затвердження осіб, відповідальних за заходи щодо забезпечення безпеки в регіонах, уведено дозволи на застосування регіональною владою заходів щодо обмеження доступу до

[155] New PRC Internet Regulation. A January 1998 report from U.S. Embassy Beijing. URL: https://fas.org/irp/world/china/netreg.htm

[156] 2006-2020 年国家信息化发展战略 (2006-2020 Nián guójiā xìnxī huà fāzhǎn zhànlüè) [Державна стратегія із розвитку інформатизації на період з 2006 до 2020 р.]. 08.05.2005. URL: https://baike.baidu.com/item/2006-2020%20%E5%B9%B4%E5%9B%BD%E5%AE%B6%E4%BF%A1%E6%81%AF%E5%8C%96%E5%8F%91%E5%B1%95%E6%88%98%E7%95%A5/16956741?fr=aladdin.

листування в інтернеті й інтернет-трафіку при виникненні загроз безпеці країни[157].

У 2015 р. започатковано дешифрування інтернет-трафіку, застосування адміністративних заходів щодо вилучення в іноземних компаній і підприємств інформації при підозрі в її використанні для терористичних цілей, а також уведення цензури для новинної діяльності на території КНР у рамках антитерористичного закону (”Оператори телекомунікаційного бізнесу й постачальники послуг інтернету, відповідно до законів та адміністративних правил, упроваджують безпеку мережі, системи нагляду за інформаційним умістом та технічні запобіжні заходи безпеки для запобігання поширенню інформації, що містить тероризм та екстремізм[158]”).

Еволюція правил і норм з кібербезпеки з різних рівнів і сфер увінчалася прийняттям структурованого закону щодо кібербезпеки на макрорівні. Закон КНР про кібербезпеку прийнято в 2016 р. і задіяно з 1 червня 2017 р. Головною метою прийняття закону проголошується захист національного “кіберсуверенітету” КНР, а одним з найважливіших його положень є вимога до операторів мережі зберігати вибрані дані в межах Китаю й дозвіл китайській владі проводити перевірки мережевих операцій компаній. Закон суттєво обмежує анонімність користувачів за рахунок введення вимоги про обов’язкову перевірку на доступ до мережі (Стаття 37: “Оператори критичної інформаційної інфраструктури, які збирають або виробляють особисту інформацію, або важливі дані під час операцій на території материкової частини Китайської Народної Республіки, повинні зберігати її в межах материкового Китаю. Якщо через вимоги бізнесу дійсно необхідно надати його за межами материка, вони повинні

[157] 国务院关于大力推进信息化发展和切实保障信息安全的若干意见 (2012) 23 号 (Guówùyuàn guānyú dàlì tuījìn xìnxī huà fāzhǎn hé qièshí bǎozhàng xìnxī ānquán de ruògān yìjiàn (2012) 23 hào) [Кілька думок Державної ради щодо енергійного сприяння розвитку інформатизації та ефективної гарантії інформаційної безпеки, 2012)]. 17.07.2012. URL: http://www.gov.cn/gongbao/content/2012/content_2192395.htm.

[158] 中华人民共和国反恐怖主义法 (Zhōnghuá rénmín gònghéguó fǎn kǒngbù zhǔyì fǎ) [Закон Китайської Народної Республіки про боротьбу з тероризмом]. 27.12.2015. URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm

виконувати заходи, спільно сформульовані державними департаментами кібербезпеки й інформатизації та відповідними департаментами Державної ради для проведення оцінки безпеки [159] ”). Якщо користувач не надає реальні ідентифікаційні дані, провайдер не має права відкривати доступ до мережі. Від іноземних компаній вимагається проходження спеціальної сертифікації, що, в тому числі, передбачає необхідність розкриття вихідних кодів програмного забезпечення, шифрування чи іншої важливої інформації для перевірки владою.

Такий підхід, звісно, не влаштовує бізнес, оскільки підвищує ризик крадіжки інтелектуальної власності, яка може дістатися місцевим конкурентам в особі контрольованих владою державних корпорацій. Тепер іноземні компанії не можуть розраховувати на комерційну таємницю, — будь-яка таємниця, яку вони прагнуть зберегти на сервері чи мережі в Китаї, автоматично стане доступною китайському уряду, а отже, потенційно й усім їхнім конкурентам в особі китайських держкорпорацій, а також китайським військовим. І якщо раніше іноземні компанії для уникнення контролю могли користуватися нормами й технологіями (наприклад VPN), які не допускаються в роботі китайських компаній, то відповідно до нового закону про іноземні інвестиції, який набрав чинності 1 січня 2020 р., виключається будь-який особливий статус, пов'язаний з тим, що фірма має статус компанії з іноземними інвестиціями (спільні підприємства, представництва), а іноземні компанії з точки зору кіберконтролю розглядаються так само, як і китайські компанії[160]. Відповідно до Закону про кібербезпеку китайський уряд має право на отримання від будь-якої фізичної чи юридичної особи в Китаї будь-якої інформації, яка, як вважатиме китайський уряд, має якийсь вплив на безпеку Китаю. Китайський закон про кібербезпеку не лише генералізував попередні напрацювання у цій сфері, але й став основою для

[159] 中华人民共和国网络安全法(Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ) [Закон Китайської народної республіки про кібербезпеку]. 07.11.2016. URL: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

[160] China's foreign investment regime. Pinsent Masons. *OUT-LAW GUIDE*. 26 Nov. 2020. URL: https://www.pinsentmasons.com/out-law/guides/chinas-foreign-investment-law

подальшого розвитку комплексної програми безпеки/спостереження [161] в інтернеті за планом, який включає ряд допоміжних законів та нормативних актів, у відповідності з рішеннями XIX з'їзду КПК, на якому ІКТ поставлено в центр економічного розвитку й наголошено на важливості кібербезпеки в міру поширення загроз і ризиків[162].

З нормативної й технологічної точок зору всі китайські закони, стратегії, нормативні документи й керівні дії в сфері безпеки кіберпростору можна розглядати як діючі в шести системах, які разом складають еволюційну основу для регулювання використання ІКТ у Китаї [163] : система управління інформаційним вмістом інтернету; багаторівнева система забезпечення кібербезпеки; система захисту критичної інформаційної інфраструктури; система захисту персональних і важливих даних; система управління мережевими продуктами й послугами; система управління інцидентами з кібербезпеки.

Реалізація згаданого комплексного плану має полягати в отриманні Міністерством безпеки Китаю повного доступу до всіх необроблених даних, що передаються через китайські мережі й розміщуються на серверах у Китаї, а також у забезпеченні цільової обробки цих даних. Причому забезпечується повне охоплення всього підконтрольного китайській владі кіберпростору, кожного району, кожного міністерства, кожного бізнесу, всіх мереж та інформаційних систем, хмарних платформ, Інтернету речей, систем управління, великих даних і мобільного інтернету[164].

Технологічним компонентом комплексної програми збору, спостереження та контролю даних є згадана вже першому розділі Багаторівнева схема захисту кібербезпеки (MLPS 2.0), що функціонує з 1 грудня 2019 р. й забезпечує

[161] Triolo Paul, Sacks Samm, Graham Webster, Creemers Rogier (2017). China's Cybersecurity Law One Year On, An Evolving and Interlocking Framework. *New America*, Now. 30, 2017. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/

[162] Cyber Policy and the 19th Party Congress. CSIS. October 26, 2017. URL: https://www.csis.org/analysis/cyber-policy-and-19th-party-congress

[163] Там само.

[164] Dickinson Steve (2019). China's New Cybersecurity Program: NO Place to Hide. *Harrais/Bricken*. Sept. 30, 2019. URL: https://harrisbricken.com/chinalawblog/chinas-new-cybersecurity-program-no-place-to-hide/

реалізацію технічного й організаційного компонентів контролю, яких повинні дотримуватись усі компанії й приватні особи в Китаї, відповідно до зобов'язань щодо безпеки інтернету, передбачених Законом Китаю про кібербезпеку. Формально всі аспекти відповідності MLPS описано у відповідних стандартах[165]. Її цілями є спостереження й контроль з боку уряду КНР та КПК, для чого забезпечується, з одного боку, закритість інформаційних систем від доступу потенційно небезпечних суб'єктів (іноземців і внутрішніх дисидентів), а з другого — повна прозорість для Міністерства громадської безпеки й інших китайських установ безпеки в інтернеті, а тому не дозволяється жодна технологія, яка блокує доступ до ресурсів у мережі для Міністерства громадської безпеки, — ні VPN, ні шифрування, ні приватні сервери (Положення про нагляд і перевірку безпеки в інтернеті органами громадської безпеки[166]). Причому Міністерство громадської безпеки має повноваження здійснювати операції з примусового виконання вимог, пов'язаних із безпекою кіберпростору в Китаї, наприклад копіювати або видаляти практично будь-яку інформацію чи дані (в тому числі ті, що належать фізичним особам і компаніям), які воно знаходить на серверах під час перевірки. Очевидно, що такий підхід суперечить інтересам країн походження іноземних компаній (США, Великобританія, країни ЄС), які в питаннях власної національної безпеки покладаються на технології приватного бізнесу, і в яких ці компанії можуть бути виконавцями в програмах, що реалізуються в стратегічно-важливих сферах.

Із часом система регулювання кіберпростору вдосконалюється й посилюється, охоплюючи все більше раніше не контрольованих сфер. Так, у липні 2021 р. Адміністрація кіберпростору Китаю повідомила про те, що компанії, які володіють даними не менше мільйона клієнтів і хочуть провести

[165] China Security GB Standarts List. URL: http://www.gbstandards.org/index/Standards_Search.asp?word=security

[166] 公安机关互联网安全监督检查规定 (Gōng'ān jīguān hùliánwǎng ānquán jiāndū jiǎnchá guīdìng) [Положення про нагляд та перевірку безпеки в Інтернеті органами громадської безпеки, Наказ Міністерства громадської безпеки КНР від 15 вересня 2018 р. № 151]. URL: http://www.gov.cn/gongbao/content/2018/content_5343745.htm

зарубіжні розміщення акцій, повинні проходити додаткову перевірку [167]. Відомство має намір розглядати потенційні загрози для національної безпеки й оцінювати надійність зберігання компаніями даних китайських користувачів і ризики розкрадання, витоку, ушкодження чи незаконного експорту такої інформації.

Що стосується персональних даних, то формально вони захищені і в цьому напрямі прийнято ряд нормативних актів, які водночас доповнюють згадану вище комплексну систему державної кібербезпеки Китаю. У 2021 р., зокрема, прийнято Закон про захист особистої інформації (Personal Information Protection Law)[168], який вперше встановлює вичерпний набір правил щодо збору й захисту персональних даних і може застосовуватися до зарубіжних обробників, а також Закон про безпеку даних [169], сфокусований на захисті національної безпеки Китаю через створення всеосяжної системи захисту даних, керованої державою.

Протягом усього періоду інтернет-інформатизації в Китаї формувалася система контролю, покликана зробити всю мережеву інформацію, яка перетинає китайський кордон, прозорою для китайського уряду й водночас закритою для несанкціонованого доступу іноземних і внутрішніх суб'єктів, які не мають зв'язку з КПК. В аспекті міжнародного обміну інформацією це означає, що вся інформація, яка перетинає китайський кордон, повинна бути доступною для КПК та її агентів.

Для розуміння системності кібербезпеки в Китаї потрібно враховувати, що сьогодні КПК керує китайськими державними корпораціями й курує приватний бізнес, який безпосередньо конкурує з іноземними компаніями, а отже

---

[167] 国家互联网信息办公室关于《网络安全审查办法（修订草案征求意见稿）》公开征求意见的通知 (Guójiā hùliánwǎng xìnxī bàngōngshì guānyú "wǎngluò ānquán shěnchá bànfǎ (xiūdìng cǎo'àn zhēngqiú yìjiàn gǎo)" gōngkāi zhēngqiú yìjiàn de tōngzhī) [Повідомлення Державного інформаційного офісу Інтернету про "Заходи з огляду кібербезпеки (переглянутий проект збору коментарів, 10 липня 2021)" Публічне звернення за коментарями]. URL: http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm

[168] Chipman Koty Alexander (2021). Personal Data Regulation in China: Personal Information Protection Law, Other Rules Amended. *China Briefing*. May 13, 2021. URL: https://www.china-briefing.com/news/personal-data-regulation-in-china-personal-information-protection-law-other-rules-amended/

[169] Chen Abby (2021) A Close Reading of China's Data Security Law, in Effect Sept. 1, 2021. *China Briefing*. July 14, 2021. URL: https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021/

зацікавлена в отриманні доступу до технологій і обмеженні свободи й безпеки бізнесу іноземним компаніям (до того ж КПК контролює науково-дослідні центри, відповідальні за розробку технологій відповідно до національних програм і планів). Також КПК здійснює командування НВАК, яка зацікавлена в інформації, знову ж таки, з метою доступу до технологічних і розвідувальних даних, а також в проведенні спеціальних операцій.

2.3. Підхід США

Підхід США в політиці інформаційної безпеки екстраполюється на міжнародний рівень як наполягання на добровільному характері норм і правил відповідальної поведінки держав у сфері використання ІКТ. Він суттєво відрізняється від підходу Росії, яка намагається встановити розроблений нею правовий режим, заснований на понятті гіпотетичних "загроз" уявному "інформаційному простору" держави від потенційних ворогів.

Як показано в першому розділі, підхід США базується на значному досвіді й досить давніх документах, але актуалізація загроз національній безпеці країни після терактів 11 вересня 2001 р. стимулювала поштовх до розробки нових стратегічних підходів у аспекті змін у міжнародній обстановці й технологічного прогресу. Вже в 2003 р. прийнято "Національну стратегію захисту кіберпростору[170]", відповідно до якої координацію роботи щодо забезпечення безпеки кіберпростору, зокрема щодо запобігання збиткам, несанкціонованого доступу і виведення з ладу інфраструктури здійснює утворене в 2001—2002 рр. Міністерство внутрішньої безпеки США (Department of Homeland Security, DHS), а в його складі, зокрема Національний центр кібербезпеки (NCSC). DHS спільно з міністерствами й агентствами, а також приватним сектором бере участь у міжнародних переговорах, в тому числі щодо вироблення міжнародних принципів поведінки й обміні інформацією. Роботу щодо забезпечення безпеки кіберпростору здійснюють агентства й федеральні міністерства, а Державний

[170] THE NATIONAL STRATEGY TO SECURE CYBERSPACE. FEBRUARY 2003. URL: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

департамент розвиває співробітництво з усіх питань кібербезпеки на міжнародній арені, формуючи міжнародне середовище передусім з державами, які поділяють спільне бачення з США на проблему інформаційної (кібер) безпеки.

Стосовно сфери міжнародної співпраці "Національна стратегія захисту кіберпростору" цілком відображала бачення загроз національній безпеці тодішньою адміністрацією США (Дж. Буш-молодший) значною мірою через призму боротьби з тероризмом і, зокрема, наголошувала на таких напрямах роботи, як: взаємодія з міжнародними організаціями та з промисловістю для сприяння глобальній культурі безпеки; розвиток безпечних мереж; сприяння створенню національних і міжнародних мереж спостереження й попередження для виявлення й запобігання кібератакам у міру їх виникнення; заохочення інших країн приєднатися до Конвенції Ради Європи про кіберзлочинність або забезпечити, щоб їх закони й процедури були принаймні всеосяжними.

Адміністрація Б. Обами, враховуючи нові обставини у сфері кібербезпеки й нові виклики, ініціювала новий етап розвитку системи кібербезпеки, основні положення якої розкрито в документах "Всеосяжна національна ініціатива кібербезпеки[171]" (2008) та "Огляд політики в кіберпросторі[172]" (2009). Саме при Обамі, в 2010 р., створено кіберкомандування, розроблено й затверджено низку документів, якими закріплено основи проведення оборонних і наступальних операцій в кіберпросторі. Кібербезпеку оголошено однією з найсерйозніших проблем економічної й національної безпеки. Незабаром після вступу на посаду президент наказав ретельно переглянути федеральні зусилля щодо захисту інформаційної й комунікаційної інфраструктури США й розробити комплексний підхід до забезпечення цифрової інфраструктури країни. З метою координації системи кібербезпеки утворено посаду Координатора державної політики з кібербезпеки, який має регулярний доступ до президента. Виконавча влада була

[171] The Comprehensive National Cybersecurity Initiative. URL: https://fas.org/irp/eprint/cnci.pdf

[172] Cyberspace PolIcy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. URL: https://fas.org/irp/eprint/cyber-review.pdf

спрямована на тісну співпрацю з усіма ключовими гравцями кібербезпеки США, включаючи державні й місцеві органи влади й приватний сектор, щоб забезпечити організовану та єдину систему реагування на майбутні кібер-інциденти, зміцнити державно-приватне партнерство для пошуку технологічних рішень, які забезпечують безпеку й процвітання США, інвестувати в передові дослідження й розробки й розпочати кампанію щодо сприяння поінформованості про кібербезпеку й цифрову грамотність, розпочати розвиток цифрової робочої сили XXI століття. І вся ця діяльність розвивалась у такий спосіб, щоб це відповідало забезпеченню прав на конфіденційність і громадянських свобод, гарантованих Конституцією[173]. При цьому держава відійшла від керівної ролі в питаннях захисту критично важливої інфраструктури, поклавшись на стандартизацію й загальні керівництва, відповідно до яких приватний бізнес повинен сам забезпечити свою кібербезпеку.

Важливого значення набув розвиток взаємодії з питань кібербезпеки на міжнародному рівні, зокрема створення єдиної платформи міжнародної взаємодії з питань кіберпростору на основі американських підходів до кібербезпеки. У 2010 р. представники США брали активну участь в підготовці доповіді Групи урядових експертів ООН, яка була узгоджена консенсусом і схвалена Генасамблеєю ООН. Для просування політики США в області кібербезпеки на міжнародній арені в першій половині 2011 р. в Державному департаменті США створено пост координатора з питань кіберпростору й прийнято нову "Міжнародну стратегію для кіберпростору[174]". Із точки зору національної безпеки виникла актуальна потреба в розв'язанні масштабних проблем, пов'язаних з атаками в мережі, які можуть серйозно загрожувати національній безпеці, що було продемонстровано в ході кібератак проти Естонії навесні 2007 р. Як відмічено в "Міжнародній стратегії для кіберпростору", Сполучені Штати прагнуть до середовища кіберпростору, яке винагороджує

[173] The Comprehensive National Cybersecurity Initiative. URL: https://fas.org/irp/eprint/cnci.pdf

[174] International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

інновації, надає людям можливості, зміцнює громади, формує кращі уряди, розширює відповідальність, гарантує основні свободи, підвищує особисту конфіденційність і посилює національну й міжнародну безпеку.

Стовпами стратегії оголошено[175]:

- досягнення глобального консенсусу щодо відповідальної поведінки держав у кіберпросторі, включаючи застосування чинного міжнародного права для посилення стабільності, обґрунтування політики національної безпеки, зміцнення партнерства й запобігання неправильним тлумаченням, які можуть призвести до конфліктів;
- підвищення здатності держав боротися з кіберзлочинністю, включаючи сприяння міжнародному співробітництву й обміну інформацією; зміцнення державної політики й управління інтернетом, сприяючи міжнародним стандартам та інноваціям, підвищуючи безпеку, надійність і стійкість, розширюючи співпрацю й верховенство права, сприяючи інклюзивним структурам та інститутам управління інтернетом за участі зацікавлених сторін з уряду, громадянського суспільства й приватного сектора;
- підтримку свободи інтернету як відкритого, глобального простору, сприяння міжнародному консенсусу щодо застосування прав людини в кіберпросторі;
- розвиток і зміцнення відносин з іншими країнами для покращення глобальної кібербезпеки шляхом посилення внутрішньої оборони мереж, розширення участі в існуючих регіональних і глобальних структурах кібербезпеки;
- розвиток інтернету й інформаційно-комунікаційних технологій для економічного зростання.

Також в американській "Міжнародній стратегії для кіберпростору" наявна теза про так зване "нарощуванні потенціалу", тобто допомогу країнам, що

[175] Pillars of The International Strategy for Cyberspace. U.S. Department of State. URL: https://2009-2017.state.gov/s/cyberissues/strategy/index.htm

розвиваються через надання необхідних ресурсів, знань, і фахівців, у тому числі для підготовки національних стратегій кібербезпеки.

За роки президентства Б. Обами потенціал використання ІКТ-інструментів набув значення важливого фактора міжнародних відносин. Із точки зору дієвості заходів виконавчої влади в протидії кіберзагрозам став президентський указ від 1 квітня 2015 р., що дозволяє уряду Сполучених Штатів здійснювати блокування власності осіб, причетних до значної шкідливої діяльності в кіберпросторі[176]. Президент Обама в цьому документі підкреслює, що ”зростання поширеності й серйозності шкідливих дій, пов'язаних із кіберзахистом, які походять від або керуються особами, які перебувають повністю або значною мірою за межами Сполучених Штатів, становить надзвичайну загрозу національній безпеці, зовнішній політиці й економіці США” й оголошує національну надзвичайну ситуацію для подолання цієї загрози. По суті, указом оголошено потенційно злочинним фактором будь-яку політичну, економічну чи соціальну загрозу, що виходить із кіберпростору, хоча злочинна діяльність в його рамках розуміється надзвичайно широко. Хоча указ і не розкриває методики ідентифікації кіберзлочинця.

Варто підкреслити, що зазначений указ цілком відповідає американському підходу до кібербезпеки, оскільки зовсім не стосується жодних політичних аспектів кіберзагроз, а охоплює лише:

- заподіяння шкоди або інших істотних ушкоджень для надання послуг комп’ютером або мережею комп’ютерів, які підтримують одну чи кілька організацій у секторі критичної інфраструктури;
- значні перешкоди в наданні послуг одним або кількома суб’єктами господарювання в секторі критичної інфраструктури;
- спричинення значних порушень у роботи комп’ютера або мережі комп’ютерів;

[176] Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". URL: https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

- спричинення значного привласнення коштів чи економічних ресурсів, комерційної таємниці, особистих ідентифікаторів або фінансової інформації з метою комерційної чи конкурентної переваги чи приватної фінансової вигоди.

Говорячи про зовнішню політику США в сфері інформаційної (кібер-) безпеки, необхідно враховувати й загальні тенденції у вибудовуванні відносин країни зі світом. Після Другої світової війни США завжди впливали на політичні процеси в усіх регіонах в аспекті власних інтересів і національної безпеки. Це, звісно ж, давало суттєві переваги національному бізнесу. Під кутом зору інтересів у зовнішній політиці формувалися й стратегія і тактика кібербезпеки. Але в період президентства Дональда Трампа (2017—2020 рр.) проголошений ним ізоляціоністський підхід відобразився й на такій масштабній та інерційній сфері, як зовнішня політика. І це стосувалося також безпекових питань, пов'язаних із кіберпростором. Видавець авторитетного часопису "Foreign Affairs" Річард Хаас характеризує такий підхід як "руйнування" зовнішньої політики США, наводячи слова Д. Трампа: "Протягом багатьох десятиліть ми збагачували іноземну промисловість за рахунок американської, субсидували армії інших країн, допускаючи при цьому сумне виснаження наших збройних сил. Ми витратили трильйони і трильйони доларів за кордоном, в той час, як інфраструктура Америки прийшла в занепад ... З цього дня на першому місці буде тільки Америка"[177]. Той самий автор ілюструє концепцію американської адміністрації в безпековій сфері в аспекті міжнародних завдань висловом Трампа під час звернення до курсантів у військовій академії Вест-Пойнт: "Ми відновлюємо фундаментальні принципи, згідно з якими завдання американського солдата полягає не в тому, щоб відновлювати іноземні держави, а в рішучому захисту нашої країни від зовнішніх ворогів[178]".

[177] Haass Richard (2020). Present at the Disruption. How Trump Unmade U.S. Foreign Policy. *Foreign Affairs*. September/October 2020. URL: https://www.foreignaffairs.com/articles/united-states/2020-08-11/present-disruption

[178] Там само.

Фактично в такому дусі й повністю відповідно до мети "Зробити Америку великою знов", дбаючи виключно про Америку, підготовлено опубліковану в 2018 р. "Національну кібер-стратегію Сполучених Штатів Америки" [179] . Документ відображає глибинний підхід в оцінці ризиків, пов'язаних із кібер-простором і чи не вперше в американській політиці інтегрує кібер-діяльність в систему владних відносин: "Кіберпростір більше не розглядатиметься як окрема категорія політики або діяльності, відокремлена від інші елементів національної влади. Сполучені Штати будуть інтегрувати використання кібер-опцій у всі елементи національної влади". Подібне бачення вже давно було властивим для держав, що дотримувалися російсько-китайського підходу в інформаційній безпеці.

В аспекті міжнародної політики в кіберстратегії Трампа закладено позицію захисту національних інтересів перед загрозою чинників, які можуть впливати на інформаційні системи, критичну інфраструктуру й економічні процеси й пов'язані з конкретними акторами, серед яких виділено Росію, Китай, Іран, КНДР і міжнародний тероризм: "Адміністрація визнає, що Сполучені Штати ведуть постійну конкуренцію зі стратегічними супротивниками, державами, які не визнають міжнародних норм, терористичними й кримінальними мережами. Росія, Китай, Іран і Північна Корея повністю використовують кіберпростір як засіб для створення реальної загрози Сполученим Штатам, їх союзникам і партнерам, часто з безглуздям, яке вони ніколи не проявляли би в інших сферах діяльності. Ці протиборчі сторони використовують кіберінструменти, щоб підірвати нашу економіку й демократію, вкрасти нашу інтелектуальну власність і посіяти розбрат у наших демократичних процесах. Ми вразливі перед кібератаками в мирний час на критичну інфраструктуру, а також зростає ризик того, що ці країни будуть проводити кібератаки проти Сполучених Штатів під час кризи, близької до війни. Ці протиборчі сторони постійно розробляють нову

[179] National Cyber Strategy of the United States of America. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

й більш ефективну кіберзброю [180] ". Очевидно, при підготовці документа враховано й реакцію суспільства на звинувачення зовнішніх сил у втручанні в перебіг президентських виборів у США в 2016 р., і досвід інформаційної експансії Росії в Україну.

Враховуючи характер і масштаб конкретних противників, зовнішньополітична лінія в сфері кібербезпеки вибудовується з урахуванням досвіду попередніх адміністрацій, але з розширенням сфери застосування політики від переважно технократичного підходу до системи політичних кроків, спрямованих на стримування й запобігання подальшої ескалації, зокрема згуртування навколо США союзників і дружніх держав. Головними цілями на міжнародному напрямі проголошено "збереження миру й безпеки шляхом посилення спроможності Сполучених Штатів — спільно з союзниками й партнерами стримувати й, у разі необхідності, карати тих, хто використовує кіберінструменти на шкідливі цілі"; й "розширити вплив Америки за кордоном, щоб розширити ключові принципи відкритої, сумісної взаємодії, надійний і безпечний інтернет[181]". Звісно, головним завданням цієї національної стратегії є відстоювання національних інтересів, зокрема в аспекті впливу на функціонування інтернету.

Фактично цей американський продукт, будучи демонстративно виведеним з-під державного контролю в США, й відданим на саморегуляцію, є спокусливим полем діяльності для суперників і противників Америки. Тому Сполучені Штати наполягають на багатосторонній моделі управління інтернетом і намагаються обмежити спроби інших держав поширювати свій вплив на певні сегменти мережі під виглядом "відстоювання суверенітету в кіберпросторі". Загалом США чітко й прозоро формулюють свою логічну мету з точки зору, зокрема, національних економічних інтересів: "Багато країн все частіше вдаються до різних обмежень для локалізації даних і впроваджують механізми регулювання

[180] National Cyber Strategy of the United States of America. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[181] Там само.

з метою реалізації політики цифрового протекціонізму під приводом забезпечення національної безпеки. Ці дії мають негативний вплив на конкурентоспроможність американських компаній[182]". Очевидно, що з позиції глобальної конкуренції стратегічно актуальним залишається збереження домінуючої позиції країни в сучасному цифровому світі. Так, у розділі Кіберстратегії "Збереження миру за допомогою сили", — це "виявлення, протидія, припинення, ослаблення інтенсивності, а також стримування дій у кіберпросторі, які дестабілізують і суперечать національним інтересам США, зі збереженням переваги США в кіберпросторі й за допомогою кіберпростору[183]".

Сполучені штати відкрили свої технології для світу й світового ринку. Це інтернет, комп'ютери, глобальна система позиціонування й багато іншого, але натомість залишають за собою право вимагати толерантної й відповідальної поведінки тих, хто цими технологіями користується. Головним завданням американської влади в цьому аспекті на зовнішньополітичному напрямі є запобігання потенційним загрозам, що походять від політичних і геополітичних суперників, які можуть використати ці технології в боротьбі за домінування чи досягнення якихось інших цілей на шкоду Сполученим Штатам. Суперники й противники США отримують вигоду від відкритості інтернету, при цьому обмежуючи й контролюючи доступ до нього своїх громадян. Для легітимізації такої поведінки вони активно прагнуть підірвати принципи вільного доступу всіх бажаючих до всесвітньої мережі на міжнародних форумах.

У Національній кіберстратегії США 2018 р. наголошено на дотриманні незмінних принципів США щодо безпеки інформації в системі міжнародних відносин — це заохочення відповідальної поведінки держав у кіберпросторі відповідно до міжнародного права, дотримання добровільності й необов'язкових норм відповідальної державної поведінки які застосовуються в мирний час задля зміцнення довіри й зменшення ризику конфліктів, пов'язаних із шкідливою кібер-діяльністю й підтримка універсальності міжнародного права у сфері

[182] Там само.
[183] Там само.

інформаційних відносин і протидії інформаційним (кібер-) загрозам, а також захист свободи інтернету.

Прикладом реалізації закладеного в цій стратегії підходу в рамках внутрішньодержавної політики з розвитку системи управління ризиками в ланцюжках поставок федерального рівня, стали обмеження й заборони на застосування у федеральних інформаційних системах і мережах продуктів IT-компаній з Росії й Китаю, зокрема пов'язаних із компаніями Лабораторія Касперського (Росія), Huawei і ZTE (Китай). У цей період набули суспільного резонансу повідомлення про впровадження зі схвалення уряду Китаю апаратних закладок, що під час виробничого процесу на китайських заводах вставлялися оперативними агентами з підрозділу Народно-визвольної армії Китаю в серверні плати, що використовуються багатьма американськими компаніями, в тому числі Amazon і Apple[184]. Також особливої ваги надано захисту чутливих нових технологій і комерційної таємниці — для запобігання використання національними державами результатів американських досліджень і розвитку для завоювання несправедливої переваги. І ще одним важливим напрямом стратегії є розвиток боротьби із кіберзлочинністю, передусім транснаціональною. У цьому аспекті розбудовуються можливості американських правоохоронних органів щодо проведення оперативно-слідчих і судово-процесуальних дій як у США, так і за їх межами, а також йдеться про розвиток співпраці з іноземними державами. Прикладом такої діяльності є збір необхідної інформації, що регулюється угодами про взаємну правову допомогу, які реалізуються, в тому числі, в рамках Будапештської конвенції з протидії кіберзлочинності. Натомість прийнятий у 2018 р. "CLOUD Act[185]" дає правоохоронним органам змогу отримувати інформацію, що зберігається на серверах американських компаній, які знаходяться за межами США.

[184] Robertson Jordan, Riley Michael (2018). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg Businessweek*, 4 Oct., 2018. URL: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[185] A Bill to amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes. URL: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

Сфера протидії кіберзлочинності є однією з пріоритетних в американській кіберстратегії, — тут США планують відігравати лідируючу роль у розробці сумісних і взаємовигідних механізмів для ефективного транскордонного обміну інформацією в сфері правоохоронних дій, а також просувають використання існуючих міжнародних інструментів — Конвенції ООН із протидії транснаціональній організованій злочинності й Мережі цілодобових контактних центрів G7.

Можливо найбільш суттєвою новацією кіберстратегії Трампа стало внесення до переліку видів зловмисної діяльності, окрім кібератак, також і зловмисних кампаній пропаганди й дезінформації, — у розділі, що стосується неприпустимої поведінки в кіберпросторі. А на протидію "безвідповідальній поведінці держав у кіберпросторі, що створює збитки США або американським партнерам", для запобігання, реагування й стримування зловмисної кіберактівності можуть бути використані всі доступні інструменти, в тому числі дипломатичні, інформаційні, військові (як кінетичні, так і кібернетичні), фінансові, розвідувальні механізми, публічна атрибуція, дії правоохоронних органів. У міжнародній діяльності в цьому аспекті США декларують "Ініціативу кіберстримування", суть якої полягає в координації спільної відповіді широкої коаліції держав-однодумців на серйозні зловмисні інциденти в кіберпросторі, в тому числі за допомогою обміну розвідувальними даними, атрибуції, публічних заяв про підтримку та інших спільних дій. Співпраця щодо виявлення, протидії й запобігання використанню цифрових платформ для здійснення злісного іноземного впливу має вестися з іноземними державними партнерами, а також приватним сектором, представниками наукових кіл і громадянського суспільства.

Національна кіберстратегія знову орієнтована на централізацію захисту мереж федеральних департаментів і відомств під відповідальністю Міністерства національної безпеки, але також посилює потенціал у сфері кібербезпеки Міністерства оборони й Розвідувального співтовариства США (у рамках їх

повноважень). Так, Міністерство оборони отримало власну кіберстратегію[186], розроблену відповідно до національної, і яка спрямована на розвиток кіберможливостей, призначених як для ведення бойових дій, так і для боротьби зі зловмисними акторами в кіберпросторі. У площині міжнародного співробітництва, відповідно до цієї стратегії, Пентагон ”працюватиме з союзниками США й партнерами над зміцненням кіберпотужності, розширенням об’єднаних операцій у кіберпросторі й збільшенням двостороннього обміну інформацією з метою просування наших спільних інтересів[187]”.

Загалом період президентства Д. Трампа характеризується розбудовою стратегії й системи кібербезпеки США. Національні спроможності у сфері захисту кіберпростору суттєво посилено в стратегічному, нормативному й інституційному плані (наприклад утворено федеральне Агентство з кібербезпеки й захисту інфраструктури США задля координації програм кібербезпеки з штатами США й покращення захисту держави від дій приватних і національних хакерів). У міжнародному вимірі, незважаючи на ізоляціоністську риторику президента, США послідовно дотримувалися раніше напрацьованих підходів.

Президентство Дж. Байдена розпочалося із його заяви про те, що “Америка повертається, дипломатія повертається[188]”, анонсуючи перегляд курсу Трампа на обмеження військового впливу США у світі. Президент оголосив про посилення співпраці з партнерами й протидію загрозам, що походять від конкретних акторів: ”Ми відновимо наші союзи й знову займемось світом не для того, щоб відповідати вчорашнім викликам, а сьогоднішнім і завтрашнім. Американське керівництво має зустріти цей новий момент просування авторитаризму,

[186] Summary. DEPARTMENT OF DEFENSE CYBER STRATEGY (2018). URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[187] Там само.

[188] Sink Justin, Parker Mario (2021). ‘America is back, Diplomacy is back’ – Biden reverses Trump’s foreign policy moves. ThePrint, Feb. 5-th, 2021. URL: https://theprint.in/world/america-is-back-diplomacy-is-back-biden-reverses-trumps-foreign-policy-moves/599152/

включаючи зростаючі амбіції Китаю конкурувати зі США й рішучість Росії завдати шкоди нашій демократії[189]".

Отже розробка питань кібербезпеки адміністрацією Дж. Буша-молодшого проходила на тлі протистояння з міжнародним тероризмом після терактів 2001 р.; Б. Обами — після показової масштабної кібер-атаки проти Естонії; Д. Трампа — з оглядом на приклади національного протекціонізму Китаю й Росії над окремими сегментами інтернету й активної експансії окремих країн у сфери кібер-простору, чутливі для США та з урахуванням наслідків інформаційного втручання Росії в політичне життя іноземних країн, зокрема виборчі кампанії в США. Натомість обраний президентом наприкінці 2020 р. Дж. Байден зіткнувся з новими викликами, як-от тотальна кібернетизація суспільного життя й економічних відносин через пандемію COVID-19 і радикальна активізація у зв'язку з цим загрозливої діяльності в кіберпросторі, приклади чого розглянуто в першому розділі цієї книги.

У першому виступі президента Байдена про місце Америки в світі відмічено збільшення ваги кібербезпеки з точки зору національних інтересів США: "Ми підняли статус кібер-питань у нашому уряді, включно з призначенням заступника радника з питань національної безпеки з питань кібернетики й нових технологій. Ми запускаємо термінову ініціативу для покращення наших можливостей, готовності й стійкості в кіберпросторі"[190].

Вже у травні 2021 р. на сайті Білого дому опубліковано президентський указ про покращення національної кібербезпеки[191]. Документ з'явився невдовзі після масштабних кібер-інцидентів, які сталися з американськими компаніями стратегічного значення SolarWinds, Microsoft і Colonial Pipeline, що виявило потребу в доопрацюванні механізмів взаємодії між державою і приватним

[189] Remarks by president biden on america's place in the world. February 04, 2021. The White House. URL: Https://www.Whitehouse.Gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/

[190] Там само.

[191] Executive Order on Improving the Nation's Cybersecurity. The White House, May 12, 2021. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

сектором у аспекті запобігання кіберзагрозам і реагування на них. Повідомлено, що це лише перший із багатьох амбітних кроків, які адміністрація робить для модернізації національного кіберзахисту [192]. У документі детально описано процедурні моменти, які стосуються реалізації кіберзахисту, важливого значення надано особливостям використання хмарних служб і покращенню безпеки ланцюгів постачання. У плані розбудови інституційної спроможності забезпечення безпеки створюється Рада з огляду безпеки в сфері кібербезпеки, спільно очолювана представниками уряду й приватного сектору, яка може збиратися після значного кібер-інциденту, щоб проаналізувати те, що сталося й дати конкретні рекомендації щодо покращення кібербезпеки. Також указом упроваджується стандартизований посібник і набір визначень для реагування на кібер-інциденти федеральними департаментами й відомствами.

Очевидно, що, враховуючи підходи Байдена в зовнішній політиці, США активно реалізуватимуть свої цілі у відносинах з країнами-партнерами й опонентами. У цьому аспекті важливою стала зустріч президентів США й Росії в Женеві у червні 2021 р., на якій обговорено питання кібербезпеки. Байден розповів про останні кібернапади на операторів інфраструктури США й сказав, що вживатиме заходів проти будь-яких російських кібератак. Путін заперечив, що Росія несе відповідальність за будь-які кібератаки проти США[193]. Натомість обидва лідери домовилися розпочати переговори про кібербезпеку, що ймовірно матиме суттєве значення для розробки проблеми безпеки кіберпростору / інформаційної безпеки, адже співпраця в цій сфері між США й Росією, фактично, не здійснювалася, крім окремих заяв і декларацій, про що йтиметься нижче. Тобто сьогодні на певному рівні в обох держав зберігається інтерес до продовження контактів щодо інформаційної безпеки — хоча б тому, що

[192] FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks. The White House, May 12, 2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

[193] Soldatkin Vladimir, Holland Steve (2021). Far apart at first summit, Biden and Putin agree to steps on cybersecurity, arms control. *Reuters*, June 17, 2021. URL: https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/

відсутність комунікації в цьому напрямі може призвести до неконтрольованої ескалації з важко прогнозованими наслідками.

Отже США залишаються провідною країною в кіберпросторі, сформувавши, починаючи з 2001 р., цілісну політику з питань кібербезпеки й використання ІКТ-інструментів для просування національних інтересів.

Позиція США в ООН

Сьогодні Сполучені Штати беруть активну участь у формуванні порядку денного з питань інформаційної (кібер) безпеки на рівні ООН. Після того, як у 1998 р. Росія внесла проєкт резолюції "Досягнення в сфері інформатизації й телекомунікацій у контексті міжнародної безпеки" й згодом розпочала роботу Група урядових експертів, США брали активну участь у її роботі, дотримуючись своїх принципів у питаннях безпеки кіберпростору. Так, вже перший підсумковий документ, підготовлений першим складом ГУЕ у 2005 р. за активної участі Росії, США не підтримали, єдиним голосом не допустивши утвердження російського підходу на рівні ООН.

Робота наступних скликань ГУЕ завершувалася консенсусом, який максимально можливо відповідав саме інтересам США, зокрема щодо застосування міжнародного права й відповідальної поведінки держав у сфері ІКТ. США змогли не тільки відстояти свою позицію, але й до певної міри повернути хід дискусії в бажаному для себе напрямі при тому, що групу очолював російський дипломат, спецпредставник президента Росії з питань міжнародного співробітництва в сфері інформаційної безпеки Андрій Крутських (Російська Федерація головувала в ГУЕ в 2005 та 2010 рр., Австралія — в 2013 р., Бразилія — в 2015 й 2019—2021 рр., Німеччина — в 2016 р.).

Попередніми звітами ГУЕ 2010, 2013 та 2015 рр. і наступними резолюціями ГА ООН, які затверджують ці звіти, по суті створено основу для певної системи підходів у сфері інформаційної (кібер) безпеки. Її компонентами є[194]: визнання

194 Efrony Dan (2021). The UN Cyber Groups, GGE and OEWG – A Consensus is Optimal, But Time is of the Essence. *Just Security*, July 16, 2021. URL: https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/

того, що міжнародне право, зокрема Статут ООН і чотири принципи jus in bello — гуманності, необхідності, пропорційності й відмінності (щоправда без використання терміну МГП) застосовні до кіберпростору та є важливими для підтримки миру, безпеки й стабільності; дотримання всіма державами одинадцяти добровільних, необов'язкових норм відповідальної поведінки, визнаючи, що додаткові норми можуть бути розроблені й додані з часом; рекомендовані конкретні заходи щодо зміцнення довіри, потенціалу й співробітництва; залучення регіональних міжнародних організацій, приватного сектора, наукових кіл.

Проте ці звіти не мають обов'язкового характеру. Досі політично і юридично не вирішені питання про те, як застосовуються в кіберпросторі такі основні норми й принципи міжнародного права, як правила атрибуції, суверенітету й належної обачності (правило due dilligence, відповідно до якого у випадку вчинення суб'єктами (діяння яких не може бути приписано державі) певних дій, що утворюють порушення міжнародного зобов'язання, вина держави полягає в тому, що вона не застосувала необхідних заходів із метою дотримання відповідного міжнародного зобов'язання). Тому сформульовані заяви, засновані на правилах, та інші норми в списку зазначених одинадцяти норм залишаються мало придатними для виконання.

Необов'язковість згаданих норм сьогодні не дає можливостей урегульовувати все гостріші проблеми кібербезпеки. Наприклад, правило due dilligence мало б застосовуватися в разі виявлення кібератаки, що походить з конкретної країни. Так, за підсумками телефонної розмови з президентом Росії в липні 2021 р., в контексті атаки комп'ютерного вимагача "Kaseya", здійсненої російськими хакерами, президент Байден сказав: "Я чітко дав йому зрозуміти, що Сполучені Штати припускають, що операція з вимагачем походить з його землі, хоча не спонсорується державою, ми очікуємо, що вони діятимуть, якщо

ми їм дамо достатньо інформації, щоб визначити, хто це"[195]. Байден також повідомив про можливість наслідків, ймовірно, якщо попередження не принесе очікуваних результатів.

Після 2015 р. переговорний процес із питань кібернетичної безпеки застопорився й п'ятий склад ГУЕ в 2016—2017 рр. не зміг прийняти консенсусної доповіді, про що йшлося вище. На цьому тлі в 2018 р. Росія вже вкотре висунула ініціативу, започатковану ще в 1998 р., під гаслом: "Досягнення в сфері інформатизації й телекомунікацій у контексті міжнародної безпеки", наполягаючи на формуванні режиму "міжнародної інформаційної безпеки". Але з позиції США у стратегічному аспекті саме відповідальна поведінка суб'єктів у сфері ІКТ має знизити ризик порушення міжнародного миру й підвищити ступінь довіри між державами, а відтак забезпечити більшу передбачуваність дій і максимально зменшити можливість виникнення непорозумінь між країнами. Тому США зі свого боку проявили ініціативу на найвищому міжнародному майданчику, і в грудні 2018 р. Генеральною Асамблеєю ООН схвалено Резолюцію 73/266 "Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки[196]", проєкт якої висунули Сполучені Штати спільно з 35 співавторами (139 за, 11 проти, 16 утрималися). Резолюцію переважно підтримали держави — члени ЄС, НАТО й інші союзники США, хоча ряд країн (усього 77, включаючи Індію, ПАР, Казахстан, Індонезію та ін.) голосували за обидві резолюції, американську й російську. Цікаво, що географія підтримки згаданих вище проєктів резолюцій відповідає розподілу країн за їх демократичним статусом відповідно до щорічних звітів організації Freedom House[197], — "не-вільні" країни підтримали російський проєкт, а "вільні" й переважно "частково-вільні" — американський.

195 Holland Steve, Shalal Andrea (2021). Biden presses Putin to act on ransomware attacks, hints at retaliation. *Reuters*, July 10, 2021. URL: https://www.reuters.com/technology/biden-pressed-putin-call-act-ransomware-attacks-white-house-2021-07-09/

196 73/266. Advancing responsible State behaviour in cyberspace in the context of international security. Resolution adopted by the General Assembly on 22 December 2018. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266

197 Global Freedom Status. Freedom House. URL: https://freedomhouse.org/explore-the-map?type=fiw&year=2021.

В американському проєкті наголошено на важливості добровільного характеру норм і правил відповідальної поведінки держав у сфері використання ІКТ для зниження ризику порушення міжнародного миру й підвищення ступеня довіри між державами. Відповідно до концепції західного підходу, метою співпраці держав у кіберпросторі в сфері міжнародної безпеки оголошено "забезпечення відкритого, інтероперабельного, надійного й безпечного інформаційно-комунікаційного середовища, виходячи з необхідності зберегти вільний потік інформації[198]".

Автори документа посилаються на результативну роботу Групи урядових експертів із досягнень у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки й відповідні доповіді Генерального секретаря за 2010, 2013 і 2015 рр., відповідно до яких міжнародне право, й зокрема Статут Організації Об'єднаних Націй, може бути застосоване й має суттєво важливе значення для підтримки миру й стабільності й створення відкритого, безпечного, стабільного, доступного й мирного інформаційно-комунікаційного середовища. Наголошено, що саме "добровільні й необов'язкового норми, правила й принципи відповідальної поведінки держав у сфері використання інформаційно-комунікаційних технологій можуть знизити ризик порушення міжнародного миру, безпеки й стабільності" й що "з урахуванням унікальних особливостей інформаційно-комунікаційних технологій з часом можуть бути розроблені додаткові норми[199]".

У преамбулі зазначено, що добровільні заходи зміцнення довіри можуть сприяти підвищенню ступеня довіри й установленню довірчих відносин між державами, а також сприяють зменшенню ризику виникнення конфліктів завдяки забезпеченню більшої передбачуваності й зниженню ймовірності виникнення непорозумінь, і таким чином можуть зробити важливий внесок у розв'язання проблем, що викликають заклопотаність держав у зв'язку з

[198] Там само.
[199] Там само.

використанням інформаційно-комунікаційних технологій і стати важливим кроком на шляху зміцнення міжнародної безпеки.

Американська резолюція передбачала скликання нової Групи урядових експертів на основі справедливого географічного розподілу, мандат якої передбачає продовження дослідження спільних заходів щодо усунення існуючих і потенційних загроз у сфері інформаційної безпеки, а також застосування міжнародного правка до ІКТ-середовища для врегулювання конфліктів. Також передбачено значну кількість зовнішніх заходів, покликаних поліпшити роботу групи, наприклад співпраця Управління ООН у справах роззброєння з регіональними організаціями (Африканський Союз, ЄС, ОАД, ОБСЄ, АСЕАН) з питань інформаційної безпеки, і що мають бути опубліковані національні позиції учасників групи з питання застосування міжнародного права до використання ІКТ державами.

На противагу американській, російська пропозиція, відповідно до резолюції "Досягнення в сфері інформатизації й телекомунікацій у контексті міжнародної безпеки[200]" 2018 р., передбачала створення так званої Робочої групи відкритого складу (РГВС). На відміну від паралельно працюючої ГУЕ, яка включала 25 членів, нова група була відкрита для участі всіх зацікавлених членів ООН, її засідання мали відкритий характер, а міжсесійні зустрічі — відкриті для представників інших стейкхолдерів: приватного сектора, наукових кіл, організацій громадянського суспільства (остання ГУЕ натомість проводила епізодичні консультації з регіональними міжнародними організаціями — АС, ЄС, ОАД, АРФ, Регіональний форум АСЕАН, а також з державами — членами ООН). Завданням групи оголошено продовження розробки норм, представлених у згаданій резолюції A/RES/73/27, шляхів їх імплементації, а також, за необхідності, внесення в них виправлень або подання додаткових норм. Група мала вивчити можливість інституціалізації діалогу з питань застосування

[200] 73/27. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27&Lang=R

міжнародного права на регулярній основі під егідою ООН і досліджувати існуючі й потенційні загрози у сфері інформаційної безпеки. Робота групи охоплює також питання розробки заходів щодо зміцнення довіри й спроможності, відповідні міжнародні концепції захисту глобальних ІТ-систем (для порівняння — до сфери ГУЕ входять норми, правила та принципи, заходи щодо зміцнення довіри й зміцнення потенціалу, а також застосування міжнародного права до кіберпростору).

Із моменту свого заснування в 2019 р., РГВС залучила близько 150 країн і спостерігачів, а в березні 2021 р. представила остаточний проєкт звіту, що містить рекомендації щодо просування миру й безпеки в кіберпросторі, і щодо якого досягнуто консенсусу [201] . У документі даються рекомендації для подальшого прогресу в області нових загроз, добровільних норм поведінки, норм міжнародного права, зміцнення потенціалу, заходів зі зміцнення довіри, а також потенційних форматів для регулярного діалогу ООН із цих питань.

Із точки зору формування середовища міжнародної взаємодії перед викликами кібербезпеки важливо, що у звіті РГВС у ширшому масштабі підтверджено рекомендації ГУЕ 2015 р. щодо добровільних норм і міжнародного права, що свідчить про успіх зусиль США й країн Заходу щодо просування їхнього підходу до відповідальності за шкідливу кібер-діяльність, яка порушує міжнародні норми: "Добровільні, необов'язкові норми відповідальної поведінки держави можуть зменшити ризики міжнародного миру, безпеки й стабільності й відіграють важливу роль у підвищенні передбачуваності й зменшенні ризиків помилкового сприйняття, сприяючи тим самим запобіганню конфліктів[202]".

У звіті повністю підтримано позицію країн Заходу в тому, що міжнародне право, зокрема Статут Організації Об'єднаних Націй, є застосовним і важливим для підтримки миру й стабільності й сприяння відкритому, безпечному,

[201] Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report. A/AC.290/2021/CRP.2. 10 March 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[202] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015). URL: https://undocs.org/A/70/174

стабільному, доступному й мирному середовищу ІКТ. Певним компромісом з їхнього боку було включення посилання на можливість “міжнародних юридичних зобов’язань”, усунення посилань на міжнародне гуманітарне право й зменшення акценту на правах людини. Також на міжнародний порядок денний висунуто питання, які раніше не були прийняті чи широко обговорювані в ООН, зокрема посилання на охорону критичної інфраструктури, а також підтвердження того, що країни намагатимуться забезпечити ”загальну доступність і цілісність інтернету”. Також піднято питання кіберзагроз проти виборчих процесів.

Згадана консенсусна доповідь РГВС 2021 р.[203] в цілому відповідає позиції, сформульованій в опублікованій у 2019 р. Державним департаментом США “Спільній заяві про просування відповідальної поведінки держави в кіберпросторі[204]”, яку підтримали 26 інших країн — партнери ”П‘яти очей”, 18 держав ЄС (включно з Німеччиною та Францією), а також Норвегія, Японія, Південна Корея й Колумбія. У документі, з посиланням на основу, закладену в звітах ГУЕ 2010, 2013 та 2015 рр., підписанти підтверджують підтримку ”еволюційних рамок відповідальної державної поведінки в кіберпросторі, яка підтримує міжнародний порядок, заснований на правилах, підтверджує застосовність міжнародного права до поведінки між державами, дотримання добровільних норм відповідальної державної поведінки в мирний час, а також розробку й упровадження практичних заходів щодо зміцнення довіри, які допоможуть зменшити ризик конфліктів, що виникають унаслідок кібер-інцидентів”. Також підписанти підкреслюють, що вони за необхідності працюватимуть разом на добровільних засадах, щоб притягнути до відповідальності держави, які діють усупереч цим рамкам, ”у тому числі шляхом вжиття заходів, які є прозорими й відповідають міжнародному праву”, —

[203] Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report. A/AC.290/2021/CRP.2. 10 March 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[204] Joint Statement on Advancing Responsible State Behavior in Cyberspace. URL: https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/

“Мають бути наслідки поганої поведінки у кіберпросторі[205]”. Також у документі підтримується цілеспрямоване нарощування потенціалу кібербезпеки для того, щоб відповідальні держави могли краще захистити свої мережі від руйнівної чи іншої дестабілізуючої кібер-діяльності. Резолюцією ГА ООН 75/240 від грудня 2020 р. поновлено мандат РГВС на період з 2021 до 2025 рр. і в червні 2021 р. відбулось її організаційне засідання.

Невдовзі після оприлюднення зазначеного звіту РГВС прийнято й звіт останньої ГУЕ, — у травні 2021 р[206]. У цьому звіті, попри певні очікування нових ініціатив і пропозицій, по суті лише розроблено додаткове розуміння добровільних норм GGE 2015. Хоча, з іншого боку, можна говорити про те, що почалося становлення основи відповідальної поведінки в кіберпросторі — з часом деякі норми можуть трансформуватися у звичаєве міжнародне право чи авторитетні тлумачення існуючих норм[207].

Також підтверджено застосовність міжнародного права, зокрема Статуту ООН у цілому, до середовища ІКТ. Значним кроком уперед стало визнання того, що міжнародне гуманітарне право застосовується до кібер-операцій під час збройного конфлікту. Група уточнила, що МГП застосовується лише в ситуаціях збройного конфлікту, а застосування встановлених міжнародно-правових принципів, уключаючи принципи гуманності, необхідності, пропорційності й відмінності, щодо сфери використання ІКТ потребує подальшого вивчення (причому нагадування про ці принципи жодним чином не легітимізує й не спонукає до конфліктів). Проте звіт ГУЕ 2021 р. став винятковим у тому сенсі, що було досягнуто консенсусу, незважаючи на те, що Група 2016—2017 рр. не змогла опублікувати звіт, і попри високу напруженість між ключовими гравцями

[205] Там само.

[206] Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. 28 May 2021. ADVANCE COPY. URL: https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

[207] Schmitt Michael (2021). The Sixth United Nations GGE and International Law in Cyberspace. *Just Security,* June 10, 2021. URL: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

через частоту й серйозність ворожих кібер-атак, у яких США, Росія й Китай звинувачують одне одного.

Отже Сполучені Штати Америки в умовах постійного тиску з боку Росії й країн, що дотримуються східної моделі інформаційної (кібер) безпеки, не тільки залишаються на своїх позиціях щодо демократичного розвитку кіберпростору й управління інтернетом, застосовності міжнародного права й відповідальної поведінки держав у кіберпросторі, але й посилюють свої позиції, співпрацюючи з міжнародними партнерами й проводячи відповідну роботу ООН у складі ГУЕ й РГВС і пропонуючи нові ініціативи у цій сфері.

2.4. Підхід ЄС

Європейський Союз, як регіональне інтеграційне об'єднання, є найуспішнішим і найамбітнішим проєктом міждержавної співпраці. Але його специфіка полягає в суто прагматичних підходах до проблем, які мають суттєве й загальне значення країн — членів. Тому в такому аспекті й розробляються усі комунітарні стратегії й реалізуються політики в розрізі окремих галузей або секторів. У контексті розглянутих вище концепцій інформаційної (кібер) безпеки, які відображають суто національні прагнення до реалізації певних стратегій у рамках характерних для країн моделей і шляхів розвитку, ЄС не демонструє чітко окреслених позицій, орієнтованих на підтримку чи то американського, чи російсько-китайського підходів. Але країни-члени ЄС однозначно підтримують демократичний шлях розвитку кіберпростору й відносин у сфері ІКТ. Це проявляється, наприклад, у їх підтримці американського проєкту резолюції ГА ООН "Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки[208]" в 2018 р. Тим не менше, окремі країни мають власні бачення перспектив міждержавного узгодження проблематики кібернетичної/інформаційної безпеки.

[208] 73/266. Advancing responsible State behaviour in cyberspace in the context of international security. Resolution adopted by the General Assembly on 22 December 2018. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266

Безпека в цій сфері розглядається на рівні ЄС в аспекті саме кібербезпеки й актуалізувалася вона недавно, порівняно з країнами, розглянутими вище, фактично лише після прийняття документа про стратегію кібербезпеки ЄС в 2013 р[209]. Але з того часу відбувається активний розвиток політики ЄС щодо кіберпростору. Починаючи з 2013 р. багато чого було досягнуто з точки зору політики ЄС у сфері кібербезпеки, яка поставлена в центрі політичних пріоритетів Європейської комісії, зайняла високі позиції в Стратегії єдиного цифрового ринку[210]. Кібербезпека та боротьба з кіберзлочинністю є одним із трьох стовпів Європейського порядку денного щодо безпеки[211] (2015 р.), а в Глобальній стратегії ЄС [212] (2016 р.) вона вже розглядається в якості горизонтальної політики унії, починаючи від загальнодоступного цифрового простору й закінчуючи елементами діяльності Європейського Союзу. Глобальна стратегія ЄС утілює новий підхід до розуміння проблеми безпеки й загроз для громадян і самого Союзу, серед яких виділено й кіберзагрози, поряд із гібридними загрозами, тероризмом, економічною нестабільністю, змінами клімату й енергетичними загрозами. Також в період, що співпадає з часом президентства Трампа в США, в питаннях безпеки з боку ЄС проголошувався курс на стратегічну автономію, що очевидно означало необхідність пошуку шляхів протистояння зазначеним вище загрозам силами самої унії. Не виключено, що до пошуків більш автономного підходу в розв'язанні проблем об'єднання спонукали як посилення загроз у кіберпросторі внаслідок прогресу ІКТ, так і непослідовність у зовнішній політиці провідного партнера ЄС, — США, і несподіваний прецедент виходу зі складу ЄС Великої Британії.

[209] EU Cyber Security strategy: An open, safe and secure Cyberspace. 7 February, 2013. URL: https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en

[210] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe /* COM/2015/0192 final */. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

[211] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS The European Agenda on Security. Strasbourg, 28.4.2015 COM(2015) 185 final. URL: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

[212] Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy. June 2016. URL: https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

Ймовірно, ЄС шукатиме й використовуватиме відповідні можливості й на рівні зовнішньої політики. У сфері кібербезпеки Глобальна стратегія ЄС передбачає узгодження захисту комп'ютерних загроз із гарантією збереження ”відкритого, вільного й безпечного кіберпростору” при зміцненні технологічного потенціалу для зменшення загроз, підвищення стійкості критичної інфраструктури, мереж та послуг і протидії кіберзлочинності. Глобальна стратегія ЄС загалом окреслює декілька рівнів політики кібербезпеки — перший охоплює відносини всередині ЄС, другий стосується відносин із третіми країнами й міжнародними організаціями, а третій відображає спільне бачення в цій сфері для узгодженої репрезентації на міжнародних майданчиках.

Усередині ЄС посилюється спроможність відповіді на кіберзагрози й відновлення критично важливої інфраструктури держав — членів при збереженні відкритого, вільного й безпечного кіберпростору. Буде посилено увагу до кібербезпеки, підвищено спроможність унії й забезпечено допомогу державам — членам у захисті від кіберзагроз, із збереженням при цьому відкритого, вільного й безпечного кіберпростору. ЄС підтримуватиме політичне, оперативне й технічне кібер-співробітництво між державами — членами, а також сприятиме взаємодії між структурами ЄС і відповідними інституціями держав — членів.

У відносинах із міжнародними організаціями у сфері кібербезпеки головним пріоритетом є посилення співпраці з такими основними партнерами, як США й НАТО. Але головним меседжем для міжнародного співтовариства, вміщеним у тексті стратегії, є чітко висловлена позиція, яка цілком відповідає західному (американському) підходу до забезпечення безпеки в кіберпросторі, — це реалізація своєї прагматичної мети стати “перспективним кібер-гравцем, захищаючи свої найважливіші активи й цінності в цифровому світі, зокрема шляхом просування вільного й безпечного глобального інтернету через прогресивний альянс між державами, міжнародними організаціями, промисловістю, громадянським суспільством і технічними експертами”. І найголовніше, — це те, що ЄС “шукатиме угод про відповідальну поведінку

держав у кіберпросторі на основі існуючого міжнародного права. Він підтримуватиме багатостороннє цифрове управління й глобальні рамки співпраці з кібербезпеки, поважаючи вільний потік інформації[213]". Тому можна стверджувати, що Європейський Союз виступає одним фронтом з іншими країнами Заходу в питанні політики інформаційної (кібер) безпеки, що проявляється, зокрема, в успішному розвитку концепції заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки, згодом (у 2018 р.) представленої Сполученими Штатами у вигляді проєкту резолюції ГА ООН.

Від початку розробки політики у сфері кібербезпеки ЄС орієнтувався більшою мірою на так звану м'яку безпеку: посилення зовнішнього виміру політики ЄС в області кібербезпеки, підвищення стійкості мереж і систем ІКТ до кіберзагроз, розробку можливостей та інструментів реагування на кібератаки, співпрацю в боротьбі з кіберзлочинністю, просування стандартів і цінностей в кіберпросторі. У 2016 р. Директивою про безпеку мереж та інформаційних систем (NIS)[214] прийнято перші загальні правила безпеки інформаційних систем. Директива NIS передбачає правові заходи для підвищення рівня кібербезпеки ЄС, забезпечуючи, щоб країни — члени: були готові реагувати на інциденти з кібербезпеки за допомогою групи реагування на інциденти комп'ютерної безпеки (CSIRT) і компетентних національних органів NIS; підтримували стратегічне співробітництво й обмін інформацією щодо конкретних питань про інциденти й ризики; сприяли розвитку кібербезпеки серед операторів критичної інфраструктури. У цій сфері працюють спеціалізоване Агентство ЄС із питань безпеки мережі й інформації (ENISA), Європейський центр кіберзлочинності (EC3) в структурі Європолу, Команда ЄС із питань комп'ютерного реагування на надзвичайні ситуації (CERT-EU) та Європейське оборонне агентство.

[213] Там само.

[214] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Однак згадана вище концепція стратегічної автономії, помітна в Глобальній стратегії ЄС, у найближчі роки, очевидно, буде вимагати відповідних заходів, підтриманих відповідним рівнем фінансування. Практичну реалізацію цього нового підходу розпочато з прийняттям у вересні 2017 р. так званого пакету кібербезпеки, з пропозицією ряду заходів, які надалі будуть координовано зміцнювати структури й можливості ЄС у сфері кібербезпеки при повній співпраці держав — членів і різних зацікавлених структур ЄС.[215]

Наприкінці 2020 р. Європейська комісія й Високий Представник Союзу із закордонних справ і політики безпеки презентували нову "Стратегію кібербезпеки для цифрового десятиліття" [216], яка має на меті посилити колективну стійкість об'єднання до кіберзагроз і гарантувати надійність цифрових послуг та інструментів. Також Комісія внесла дві нові пропозиції — оновлену Директиву NIS2 [217] про заходи щодо високого загального рівня кібербезпеки в усьому Союзі й нову Директиву щодо стійкості критичних організацій [218]. Разом ці документи складають новий пакет із кібербезпеки. Доповнення європейського вторинного права у сфері кібербезпеки стало логічним кроком після врахування виявлених недоліків попередніх нормативних актів і викликів, що з'явились у зв'язку з пандемією Covid-19.

Стратегія кібербезпеки для цифрового десятиліття покликана забезпечити відповідь на сучасні й потенційні кібер-пов'язані виклики, що виникли з посиленням цифровізації й залежності від сучасних ІКТ. Чи не вперше в нормативній практиці ЄС визнано, що кіберпростір є не лише потенційним джерелом загроз технічного чи економічного характеру й кіберзлочинності, а

[215] Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'. Publication 19 September 2017. URL: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu

[216] The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Publication 16 December 2020. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

[217] Revised Directive on Security of Network and Information Systems (NIS2). European Commission. Publication 16 December 2020. URL: https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2

[218] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. Brussels, 16.12.2020 COM(2020) 829 final. URL: https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf

“все частіше використовується в політичних та ідеологічних цілях”, а ЄС “не має колективної ситуаційної обізнаності щодо кіберзагроз”. Таким чином формулюється складне завдання поліпшення кібербезпеки ЄС для захисту основних прав і свобод і стимулювання ефективної й систематичної співпраці. Стратегія описує кібербезпеку як багаторівневу проблему, для розв’язання якої сформовано сфери діяльності: стійкість, технологічний суверенітет і лідерство; нарощування оперативного потенціалу для запобігання, стримування й реагування; просування глобального й відкритого кіберпростору.

ЄС планує побудувати мережу Оперативних центрів безпеки на всій своїй території, що працює на основі штучного інтелекту, щоб створити європейський “щит кібербезпеки [219] ”, розгорнути надзвичайно безпечну інфраструктуру квантового зв'язку для Європи для передачі конфіденційної інформації й упровадити ряд інших інструментів і заходів, наприклад зміцнити інструменти кібер-дипломатії, розробити план дій на випадок надзвичайних ситуацій ”для вирішення екстремальних сценаріїв, що впливають на цілісність і доступність глобальної кореневої системи DNS“, встановити стандарти безпеки.

Підвищити безпеку інтернету й інших важливих мереж та інформаційних систем планується шляхом створення “Європейського центру компетенції з питань промислової, технологічної й дослідницької роботи з кібербезпеки[220]”, — для об’єднання інвестицій у дослідження кібербезпеки, технології та в промисловий розвиток. Новий орган базуватиметься в Бухаресті й працюватиме разом із мережею національних координаційних центрів, призначених державами — членами та ENISA.

Відзначимо, що в ЄС реагує на посилення кіберзагроз розгортанням системи засобів та інструментів протидії, охоплюючи все більше сфер, пов’язаних із кіберпростором. Так, у резолюції, прийнятій 10 червня 2021 р., Європарламент

[219] New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. European Commission. 16 December 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

[220] Bucharest-based Cybersecurity Competence Centre gets green light from Council. European Council. 20 April 2021. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/

закликає забезпечити захист пов'язаних продуктів і супутніх послуг, включаючи ланцюжки поставок, в аспекті стійкості до кібер-інцидентів, наголошує на необхідності встановлення вимог кібербезпеки щодо програм, програмного забезпечення, вбудованого програмного забезпечення (яке контролює різні пристрої й машини, які не є комп'ютерами) й операційних систем (програмне забезпечення, яке виконує основні функції комп'ютера) до 2023 р[221]. Цілком ймовірно, що реалізація таких вимог матиме наслідки, подібні до обмеження присутності на ринку відповідних продуктів іноземного виробництва, як це мало місце в США.

Нова стратегія передбачає значне збільшення коштів у області кібербезпеки, зокрема в рамках програми досліджень та інновацій, стратегічної інвестиційної програми "Цифрова Європа" і програми "Горизонт Європа", а також у рамках Плану відновлення для Європи. Держави — [222] ОВД ЄС для підвищення кібербезпеки й відповідності інвестиціям на рівні ЄС. Мета — залучити до 4,5 млрд євро спільних інвестицій з ЄС, держав — членів та промисловості.

У березні 2021 р. Комісія виклала своє бачення цифрової трансформації Європи до 2030 р. в Комюніке "Цифровий компас: європейський шлях до Цифрового десятиліття"[223], в якому фактично виклала "європейське" бачення цифрового суверенітету, що полягає в амбітному плані щодо проведення цифрової політики, яка передбачає усунення вразливих місць і залежностей, а також прискорення інвестицій задля випереджаючого розвитку ЄС у відкритому й взаємопов'язаному світі. Поставлено цілі, орієнтовані на пришвидшений розвиток цифрової економіки й суспільства, запропоновано скласти набір цифрових принципів, що охоплюють такі сфери, як доступ до інтернет-послуг, безпечне й надійне онлайн-середовище, цифрові медичні послуги, цифрові

[221] European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)). URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html

[222] The Recovery and Resilience Facility. European Commission. URL: https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 2030 Digital Compass: the European way for the Digital Decade. COM/2021/118 final. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

державні послуги й адміністрація, орієнтовані на людину. Ці принципи доповнять існуючі права, які вже захищають і розширюють можливості європейців в інтернеті, такі як захист особистих даних і конфіденційності, свобода вираження поглядів, свобода створення й ведення бізнесу в інтернеті й захист інтелектуальної власності.

На перший погляд європейська стратегія за масштабом нагадує підхід Китаю, який полягає в державному управлінні й спрямовуванні економіки й усього суспільства, але насправді її суть — у перерозподілі стимулів і фактичній відсутності геополітичних амбіцій. А "суверенітет" ЄС у цифровому світі — це лише певна технологічна незалежність, заснована на інвестиціях у європейські дослідницькі й інвестиційні проєкти у сферах ІКТ й телекомунікацій.

Натомість ЄС залишається орієнтованим на західну (американську) концепцію в питаннях розвитку кіберпростору та його безпеки. Відповідно до нової стратегії, унія активізуватиме роботу з міжнародними партнерами щодо зміцнення заснованого на правилах глобального порядку, сприяння міжнародній безпеці й стабільності в кіберпросторі, захисту прав людини й основних свобод в інтернеті, буде просувати міжнародні норми й стандарти, які відображають ці основні цінності ЄС, співпрацюючи зі своїми міжнародними партнерами в ООН і на інших відповідних форумах.

Нова кіберстратегія однозначно вказує на продовження курсу співпраці з міжнародними партнерами для просування концепції глобального, відкритого, стабільного й безпечного кіберпростору, де поважається міжнародне право, зокрема Статут ООН, а також добровільні необов'язкові норми, правила й принципи відповідальної поведінки держав у кіберпросторі відповідно до доповідей ГУЕ в галузі інформації й телекомунікацій у контексті міжнародної безпеки, схвалених Генеральною Асамблеєю ООН. Очевидно, в загальних рисах така позиція відповідає й консенсусному звіту Робочої групи відкритого складу 2021 р.

Із загостренням багатосторонніх дебатів із питань міжнародної безпеки в кіберпросторі, зокрема після представлення конкуруючих проєктів резолюції ГА ООН у 2018 р. Росією й США, виникла очевидна необхідність зайняття

Європейським Союзом і державами — членами більш активної позиції в дискусіях в ООН і на інших міжнародних майданчиках. ЄС має найкращі можливості для просування, координації й закріплення позицій держав — членів на міжнародних форумах, а також, як зазначено в Стратегії кібербезпеки 2020 р., "...має виробити позицію ЄС щодо застосування міжнародного права в кіберпросторі".

У зв'язку з цим особливо варто відзначити проактивну позицію окремих держав — членів і самого ЄС. У жовтні 2020 р. Франція, з Єгиптом і 40 інших держав (Аргентина, Колумбія, Еквадор, Габон, Грузія, Японія, Марокко, Норвегія, Сальвадор, Сінгапур, Республіка Корея, Республіка Молдова, Республіка Північна Македонія, Сполучене Королівство, ЄС й його держави — члени) запропонува [224] програму дій (ПД) для просування відповідальної поведінки держав у кіберпросторі [225]. У світлі багаторічної конкуренції між російсько-китайським і західним підходами до інформаційної безпеки / безпеки кіберпростору це виглядало як спроба подолати роздвоєність дискусій із кіберпитань в ООН у рамках Групи урядових експертів і Робочої групи відкритого складу. Ця ініціатива була оформлена не у вигляді проєкту резолюції, а як записка, опублікована в рамках РГВС. Її основним прихильником, очевидно, є Франція, підтримана ЄС і всіма його членами, а також рядом держав, орієнтованих переважно на підтримку західного підходу в питаннях кібербезпеки. Ці країни заявляють, що вони хотіли б замість розділеної між ГУЕ та РГВС дискусії бачити один постійний форум, який займався би питаннями використання державами ІКТ в контексті міжнародної безпеки. Як модель вони пропонують взяти формат, власне, програм дій — за аналогією, наприклад, з програмами дій щодо запобігання й викорінення незаконної торгівлі стрілецькою зброєю й легкими озброєннями в усіх її аспектах і боротьби з нею,

[224] The future of discussions on ICTs and cyberspace at the UN. Updated version: 10/08/2020. URL: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf

[225] Там само.

щодо інвалідів, расизму, найменш розвинених країн, заборони підбурювання до насильства та мови ворожнечі (у міжнародній політиці Програма дій зазвичай є підсумковим, не обов'язковим юридично, але політично зобов'язуючим документом міжурядової конференції, що сигналізує про намір держав-учасниць працювати над глобальною проблемою всеосяжним і ретельним чином).

Два оформлених раніше треки, ГУЕ й РГВС, є результатом стратегічної конкуренції між Росією і США. За цих обставин дипломатичні спроби досягти успіху одного процесу в конкуренції з іншим, швидше за все, призведуть до невдачі обох, тому реалізація Програми дій з кібер-питань — це третій варіант, той, який може створити більш відкритий і всебічний переговорний процес, не потрапляючи в пастку існуючої дуополії[226].

Заснований згаданими вище державами "Постійний форум ООН для розгляду питання використання ІКТ державами в контексті міжнародної безпеки" передбачає, що ПД має діяти "в єдиному, довгостроковому, інклюзивному й орієнтованому на прогрес форматі; чиї умови можуть бути обговорені поточними ГУЕ та РГВС, тоді як впровадження й наступні заходи можуть бути згодом схвалені Генеральною Асамблеєю ООН. Відповідно до пропозиції, ПД може "створити рамки й політичні зобов'язання" на основі існуючих міжнародних рамок, тобто рекомендацій, норм і принципів, які вже узгоджені, зокрема в звіті ГУЕ ООН 2015 р. Відповідно проводитимуться регулярні щорічні зустрічі на робочому рівні, зосереджені на впровадженні існуючих рамок. ПД має сприяти посиленню співробітництва, а також ініціювати консультації з іншими зацікавленими сторонами, регіональними організаціями й установами ООН, а також залучати інші зацікавлені сторони. Запропоновано кожні 5 років проводити регулярні конференції, орієнтовані на консенсус, на яких держави можуть вирішити, чи слід розробляти додаткові норми.

[226] Géry Aude (2020). A New UN Path to Cyber Stability. Directions. *Cyber Digital Europe*, 6 October 2020. URL: https://directionsblog.eu/a-new-un-path-to-cyber-stability/

Запропонований формат програми дій можна розглядати як альтернативу ГУЕ й РГВС, або як доповнення до них обох. Тим не менше, ця ситуація відображає низькі очікування від поточних переговорних треків. І хоча Програма дій поки що залишається лише пропозицією з багатьма деталями, які ще належить вирішити, вона має потенціал для створення більш упливового й послідовного діалогу.

У Стратегії кібербезпеки ЄС 2020 р., яка побачила світ майже відразу після згаданої вище ініціативи щодо ПД, є безпосередня прив'язка до останньої. ЄС оголошує про просування консенсусної пропозиції, відповідно до Програми дій щодо покращення відповідальної поведінки держав у кіберпросторі, в ООН. Спираючись на існуючий доробок ГУЕ 2015, 2013 та 2010 рр., схвалений Генеральною Асамблеєю ООН, ЄС підтримує пропозицію платформи для співпраці й обміну кращими практиками в рамках ООН, а також пропонує створити механізм для впровадження на практиці норм відповідальної поведінки держав.

Про відповідність такої позиції Євросоюзу якомусь із двох домінантних підходів до кібербезпеки свідчить те, що ініціативу ПД не підтримали ні Росія, ні Китай, що зрозуміло з точки зору їхнього просування концепцій міжнародної інформаційної безпеки й кіберсуверенітету. Але й США також не підтримали цю пропозицію, хоча французько-єгипетський проєкт і за назвою й по суті наближений саме до американської ініціативи на рівні ООН щодо заохочення відповідальної поведінки держав у кіберпросторі. І врешті, у досягненні консенсусу на рівні РГВС у березні 2021 р., ймовірно певну роль відіграла саме поява зазначеної ПД і її потужна підтримка з боку ЄС. У такій ситуації представники західної концепції безпеки кіберпростору отримали явну перевагу. Відсутність підтримки ПД з боку провідних кібер-держав може бути пов'язана з вичікуванням більш конкретного оформлення цієї нової пропозиції, а також бажанням уникнути поляризації під час дебатів.

Відповідно до західного (демократичного) підходу до розвитку кіберпростору, ЄС ставить стратегічні цілі протидіяти цензурі, масовому стеженню, порушенню конфіденційності даних і репресіям проти громадянського суспільства й громадян із застосуванням ІКТ, лідируючи у сфері захисту й

просування прав людини й основних свобод в інтернеті. З цією метою ЄС має сприяти подальшому дотриманню міжнародного законодавства й стандартів у сфері прав людини, зокрема Статуту ООН і Загальної декларації прав людини, а також упроваджувати в життя прийнятий в ЄС у листопаді 2020 р. План дій із прав людини й демократії на 2020—2024 рр[227]. Також у цьому контексті варто згадати прийняті в ЄС у 2014 р., але актуальні й у стратегічній перспективі Настанови з прав людини щодо свободи вираження поглядів в інтернеті й офлайн[228].

Ще одним пунктом, у якому позиція ЄС співпадає з американською і протилежна російській, є міжнародна співпраця у сфері протидії кіберзлочинності. ЄС дотримується Будапештської конвенції Ради Європи про кіберзлочинність і заявляє про підтримку третіх країн, які бажають приєднатися до неї, а також про необхідність доопрацювання Другого додаткового протоколу до Будапештської конвенції, що включає заходи й гарантії для покращення міжнародної співпраці між правоохоронними й судовими органами, а також між органами влади й постачальниками послуг в інших країнах. Водночас Євросоюз виступає проти створення нового правового інструменту щодо кіберзлочинності на рівні ООН, ініційованого Росією в постаті поданого нею в 2017 р. проекту конвенції ООН "Про співпрацю в сфері протидії інформаційній злочинності", який "ризикує посилити розбіжності й уповільнити настільки необхідні національні реформи й зусилля з розбудови спроможності, що потенційно може перешкоджати ефективному міжнародному співробітництву у сфері боротьби з кіберзлочинністю: ЄС не бачить необхідності в будь-якому новому правовому інструменті щодо кіберзлочинності на рівні ООН[229]".

[227] EU Action Plan on Human Rights and Democracy 2020-2024. Council of the European Union. Brussels, 18 November 2020. URL: https://www.consilium.europa.eu/media/46838/st12848-en20.pdf

[228] EU Human Rights Guidelines on Freedom of Expression Online and Offline. Council of the European Union. Brussels, 12 May 2014. URL: https://www.consilium.europa.eu/media/28348/142549.pdf

[229] Там само.

Розділ 3. ВЗАЄМОДІЯ МІЖ ДЕРЖАВАМИ У СФЕРІ ІНФОРМАЦІЙНОЇ (КІБЕР) БЕЗПЕКИ

3.1. Міжнародна діяльність Китаю у сфері кібербезпеки

У сфері міжнародних відносин Китай послідовно педалює свою концепцію кіберсуверенітету, що подається як повага до права кожного уряду обирати власний шлях для кіберрозвитку й політики інтернету. Через кіберсуверенітет Китай декларує відстоювання права всіх країн на рівну участь у кібер-управлінні, протистояння кібергегемонії[230]. Також Китай не схвалює проведення, потурання й підтримку будь-яких дій, які можуть загрожувати кібербезпеці інших країн[231].

Віднедавна Китай претендує на роль провідного актора у сфері, пов'язаній із розвитком інтернету, зокрема в 2014 р. ним започатковано Всесвітню інтернет-конференцію, щорічний форум для обговорення глобальних питань і політики інтернету. Вже на першій Всесвітній інтернет-конференції невідома сторона розповсюдила проєкт спільної заяви, що підтверджує право окремих країн розвивати, використовувати й керувати інтернетом (який, проте, офіційно не розглядався)[232]. А на другій конференції в 2015 р., у якій взяли участь очільник Китаю й керівники урядів низки держав, Сі Цзіньпін закликав світ "поважати інтернет-суверенітет кожної країни, поважати право кожної країни вибирати власний шлях розвитку й модель управління інтернетом"[233].

Тоді ж започатковано Уженьську ініціативу, яка закликає всі країни сприяти розвитку інтернету, ділитися плодами його розвитку й покращувати глобальне управління мережею, сприяти культурному різноманіттю й забезпечувати мир і безпеку в кіберпросторі [234]. Проте із західної позиції ця ініціатива була

[230] Hao Yeli (2017). A Three-Perspective Theory of Cyber Sovereignty. URL: https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model

[231] Zunyou Zhou (2015). China's Draft Cybersecurity Law. *China Briefing.* 15, no. 24 (December 21, 2015). URL: https://jamestown.org/program/chinas-draft-cybersecurity-law/.

[232] China Delivers Midnight Internet Declaration — Offline. *The Wall Street Journal*. Nov. 21, 2014. URL: https://www.wsj.com/articles/BL-CJB-24963

[233] Xi Jinping calls for 'cyber sovereignty' at internet conference. *BBC*. 2015-12-16. https://www.bbc.com/news/world-asia-china-35109453

[234] Zhu, Shenshen (2015). Wuzhen initiative on Internet future. *Shanghai Daily*. 29 December 2015. URL: https://archive.shine.cn/business/it/Wuzhen-initiative-on-Internet-future/shdaily.shtml

розкритикована як спроба сприяти цензурі. За словами Розан Райф, директора із досліджень Східної Азії в Amnesty International, “Під виглядом суверенітету й безпеки китайська влада намагається переписати правила інтернету, щоб цензура й нагляд стали нормою скрізь. Це повний напад на свободи інтернету”[235].

Головним на сьогодні документом, у якому розкрито підходи Китаю до інформаційної безпеки на міжнародному рівні, є прийнята в 2017 р. “Міжнародна стратегія співробітництва в кіберпросторі”. У цьому документі цілком і повністю відображено китайське розуміння кіберпростору і його безпеки, передусім — домінуючої ролі держави в управлінні мережею, відповідно до національного бачення системи міжнародної взаємодії. В основу стратегії закладено чотири принципи — миру, суверенітету, спільного управління й спільної вигоди[236]. Ці принципи покладено в основу стратегічних цілей, чітко викладених у документі.

По-перше, заявлено про забезпечення кіберсуверенітету й те, що Китай “прагне підтримувати мир і безпеку в кіберпросторі й установлювати справедливий і розумний міжнародний порядок у кіберпросторі на основі суверенітету держави”, буде вести активну роботу над досягненням міжнародного консенсусу в зв’язку з цим, висловлює незгоду з “тенденцією мілітаризації й стримування в кіберпросторі”, яка “не сприяє міжнародній безпеці й стратегічній взаємній довірі”, і що “жодна країна не повинна прагнути до кібергегемонії”. Очевидним є натяк на американську ініціативу кіберстримування, в якій серед носіїв потенційних кіберзагроз, разом з Росією, Іраном і Північною Кореєю, безпосередньо вказано Китай. У відповідь КНР оголошує про посилення ролі військових “у захисті суверенітету країни, безпеки й інтересів розвитку в кіберпросторі”, прискорюючи розвиток кіберсил, посилюючи можливості кіберзахисту, підтримуючи “діяльність держави й участь у міжнародному співробітництві, запобіганні великій кіберкризі, захисті кіберпростору й підтримці національної безпеки й соціальної стабільності”.

[235] Griffiths, James (2015). Chinese President Xi Jinping: Hands off our Internet. *CNN*, 2015-12-16. URL: https://edition.cnn.com/2015/12/15/asia/wuzhen-china-internet-xi-jinping

[236] Full Text: International Strategy of Cooperation on Cyberspace. 2017-03-01. URL: http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_2.htm

По-друге, Китай знову послідовно підтверджує свою позицію щодо відходу від нинішньої моделі управління інтернетом, у якій політику мережі формують різні гравці — уряди, компанії та громадянське суспільство, в напрямі багатостороннього прийняття рішень між урядами, зокрема на платформі ООН: “відповідні зусилля мають відображати широку участь, розумне управління й демократичне прийняття рішень, при цьому всі зацікавлені сторони роблять внесок у свою частку залежно від своїх можливостей, а уряди займають провідне місце в управлінні інтернетом, зокрема державною політикою й безпекою”. Оголошено, що “Китай підтримує формулювання загальноприйнятих міжнародних правил і норм поведінки держав у кіберпросторі в рамках Організації Об’єднаних Націй[237]”.

Китай підтримував та активно брав участь у процесі прийняття міжнародних правил і декларує, що буде продовжувати робити свій внесок шляхом “посилення діалогу й співпраці з міжнародним співтовариством”. У цьому аспекті наголошується на важливості прийнятого в 2015 р. державами-членами ШОС і скерованого до ГА ООН Міжнародного кодексу поведінки з інформаційної безпеки.

По-третє, документ прямо закликає китайські технологічні компанії вийти на глобальний рівень, особливо в країнах, націлених на ініціативу “Один пояс — один шлях”. Заохочуватимуться й підтримуватимуться китайські інтернет-компанії разом із тими, що працюють у виробництві, фінансовому секторі й секторі ІКТ, для досягнення провідних позицій у глобальній участі в міжнародній конкуренції. Також китайські компанії заохочуються до активної участі в розбудові потенціалу інших країн, зокрема Китай підтримує допомогу країнам, що розвиваються, в розбудові можливостей кібербезпеки, включаючи передачу технологій, розвиток критичної інформаційної інфраструктури й навчання персоналу.

Звісно, Китай, завжди послідовний у своїй політиці, відповідно до прийнятої міжнародної стратегії продовжуватиме проводити щорічну Всесвітню

[237] Там само.

інтернет-конференцію й інші міжнародні конференції, двосторонні інтернет-форуми з відповідними країнами, двосторонні, багатосторонні й регіональні обговорення з Японією, Кореєю, у рамках Регіонального форуму АСЕАН, Баоського азійського форуму і, звісно ж, розвиватиме співпрацю й свою позицію в напрямі кібербезпеки у рамках ШОС та БРІКС.

Відповідно до цієї стратегії Китай планує закріпити за собою місце лідера і в регіональних відносинах із приводу політики у сфері кібербезпеки. Він буде заохочувати й підтримувати в цьому напрямі регіональні організації з різних частин світу, де він має сильні позиції, включаючи Нараду зі взаємодії й зміцнення заходів довіри в Азії (CICA), Форум китайсько-африканського співробітництва (FOCAC), Форум співробітництва між Китаєм і арабськими державами, Форум Китаю й Спільноти держав Латинської Америки й Карибського басейну, Азіатсько-африканську юридичну консультативну організацію. Також базу підтримки для своїх ініціатив Китай формуватиме в рамках АТЕС і G20 і, поза сумнівом досліджуватиме можливості діалогу щодо кіберпростору з іншими регіональними організаціями.

Як показано в попередніх розділах, головним інтересом китайської політики у сфері інформаційної (кібер) кіербезпеки є збереження беззаперечного домінування КПК в усіх сферах суспільного життя всередині країни й просування концепції кіберсуверенітету на міжнародному рівні. Якщо внутрішні справи Китаю мало стосуються міжнародного співтовариства, то китайський "кіберсуверенітет" дається взнаки активним суб'єктам глобалізації кіберпростору. Особливо помітна відмінність між поглядами на безпеку кіберпростору Китаю та США — світових лідерів у сфері інформатизації й телекомунікації, що ґрунтується на концептуальному розриві щодо вирішення проблеми управління кіберпростором. І Китай і США виступають за правила кібер-управління всередині країни й на міжнародному рівні, але їх контрастні підходи до цих питань завжди породжують непорозуміння й викликають підозри з іншого боку. Наприклад, концепція "кіберсуверенітету", висунута Китаєм, розглядає суверенітет як повагу до права кожного уряду обирати власний шлях для

кіберрозвитку й політики інтернету. Декларується право всіх країн на рівну участь у кібер-управлінні, протистояння "кібергегемонії". Китай не схвалює вчинення чи підтримку будь-яких дій, які можуть загрожувати кібербезпеці інших країн.

Однак ця експансивна концепція суверенітету послідовно критикується й відкидається Сполученими Штатами. США виступають проти такого підходу не лише з міркувань безпеки, економіки й ефективного міжнародного управління, а й з ідеологічних причин, розглядаючи цей китайський підхід як прямий контраст із фундаментальними американськими принципами свободи слова й поширення демократії. У США вважають, що китайська концепція кіберсуверенітету рівнозначна праву цензурувати локальну інформацію в Китаї, а також забороні доступу до китайського ринку для глобальних американських компаній, що працюють у кіберпросторі.

Спільність із російськими позиціями

В аспекті міжнародних відносин китайська позиція концептуально співпадає з російською, адже КНР послідовно відстоює претензії на виокремлення зі світової мережі національних сегментів для забезпечення над ними національного суверенітету. При тому, що Китай має власне бачення концепції кіберпростору та його безпеки, він традиційно підтримує російські проєкти резолюцій в ООН у сфері інформаційної безпеки й тісно співпрацює з Росією в рамках міжнародних форумів за їх спільної участі. Прикладом є співпраця країн у рамках ШОС, де в 2006 р. прийнято Заяву головних держав — членів із міжнародної інформаційної безпеки[238], у якій інформаційну безпеку оголошено важливим фактором забезпечення державного суверенітету, національної безпеки, соціально-економічної стабільності. У рамках угоди між державами в 2009 р. визначено перелік загроз, зокрема такі, що традиційно наголошуються Росією на міжнародних майданчиках, зокрема "використання домінуючого становища в інформаційному просторі на шкоду інтересам і

[238] Заявление глав государств-членов ШОС по международной информационной безопасности. Официальный сайт газеты "Жэньминь Жибао". 15.06.2006. URL: http://russian.people.com.cn/31857/102574/102589/7409849.html.

безпеці інших країн" і "розповсюдження інформації, що спричиняє шкоду суспільно-політичній і соціально-економічній системам, духовному, моральному й культурному середовищам інших держав"[239].

У рамках ШОС за участі Китаю проведено чимало зустрічей і прийнято ряд декларацій, у яких відмічено проблематику інформаційної безпеки. Наприклад декларація про спільну діяльність держав — членів у сфері інформаційної безпеки, організацію системи моніторингу можливих загроз у глобальному інформаційному просторі й протидії їм. З ініціативи Росії в цій організації піднімаються питання вироблення міжнародних правил поведінки в інформаційному просторі та ін.

Китай також зацікавлений у розвитку питання суверенітету в кіберпросторі. Наприклад у заяві Ради глав держав — членів ШОС від 11 жовтня 2020 р. повідомлено про "підтримку здійснюваної в ООН діяльності із вироблення правил, норм і принципів відповідальної поведінки держав у інформаційному просторі й підтверджено намір продовжити спільну роботу й координацію зусиль ШОС у цьому напрямі в рамках ключових профільних переговорних майданчиків ООН", а також про "необхідність посилення координації діяльності в ООН і на інших міжнародних майданчиках із питань удосконалення управління мережею Інтернет, в тому числі забезпечення рівних прав держав на участь у процесі управління мережею Інтернет[240]".

Ще одним майданчиком, на якому Китай просуває свої позиції, які принципово співпадають із російськими, стала група БРІКС (Бразилія, Росія, Індія, Китай, Південно-Африканська Республіка). Цей форум потужних держав, які концентрують понад сорок відсотків населення планети й характеризуються швидкими темпами інформатизації суспільства, кожна сторона використовує на свою користь, але в питаннях інформаційної безпеки / безпеки кіберпростору вони

[239] Соглашение между правительствами государств—членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. URL: https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreementRussian.pdf

[240] ЗАЯВЛЕНИЕ Совета глав государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2020/11/10. URL: http://ru.china-embassy.org/rus/zgxw/t1831178.htm

мають подібне бачення. Це стосується, зокрема, підходу до вироблення спільних правил для кіберпростору й тяжіння до інформаційного (кібер) суверенітету.

Ці питання піднімаються на самітах БРІКС і поступово набувають усе більш виразних формулювань у підсумкових документах. Так, на бразильському (2019 р.) саміті БРІКС прийнято декларацію, в якій сформульовано буквально те, чого домагається Росія й що декларує Китай: "Ми підкреслюємо важливість загальноприйнятих норм, правил і принципів під егідою ООН для відповідальної поведінки держав у сфері ІКТ і підтримуємо центральне значення Організації Об'єднаних Націй у їх розвитку[241]". Ще раніше, на Сяменьському саміті організації, організованому Китаєм на своїй території, в тексті прийнятої декларації розтлумачено позицію держав — членів із питань безпеки кіберпростору, з вказівкою на те, що "ООН відіграє центральну роль у розробці загальновизнаних норм відповідальної поведінки держав у використанні ІКТ для забезпечення мирного, безпечного, відкритого, кооперативного, стабільного, впорядкованого, доступного й справедливого середовища ІКТ" [242]. У документі вказується на необхідність універсального нормативно-обов'язкового інструменту щодо боротьби зі злочинним використанням ІКТ під егідою ООН (уперше цю позицію сформульовано в Уфімській декларації ШОС). А загальний підхід до кібербезпеки оформлено в деклараціях, що прийняті в Етеквіні, Форталезі, Уфі та Гоа.

Країнами — членами БРІКС утворено Робочу групу з питань безпеки у використанні інформаційно-комунікаційних технологій (WGSICT), і Дорожню карту практичного співробітництва БРІКС щодо забезпечення безпеки використання ІКТ. Також у рамках групи прийнято Дорожню карту практичного співробітництва БРІКС із забезпечення безпеки при використанні ІКТ.

Варто зазначити, що країни — члени БРІКС у питаннях кібербезпеки й підходів до політики ІКТ мають дещо відмінні позиції. Так, Росія подає пропозиції

[241] Brasília Declaration 11th BRICS Summit. 14 November 2019 in Brasília, Brazil. URL: http://brics2019.itamaraty.gov.br/images/documentos/Braslia_Declaration_-_hiperlinks_como_est_no_site_28-11.pdf

[242] BRICS Leaders Xiamen Declaration. Xiamen, China. 9.04.2017. URL: https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/BRICS+Leaders+Xiamen+Declaration+9-4-17.pdf

щодо міжурядової угоди БРІКС про співпрацю щодо забезпечення безпеки використання ІКТ, а Бразилія просуває ініціативу щодо двосторонніх угод між країнами БРІКС із цього питання. Китай натомість не проявляє значної формальної активності в цьому напрямі, беручи, проте, участь у всіх відповідних проєктах БРІКС і, в решті, ситуація в сфері безпеки кіберпростору на цьому форумі розвивається в потрібному для КНР напрямі. Зокрема отримала розвиток концепція цифрового суверенітету, активно пропагована Китаєм. Серед його партнерів по БРІКС, окрім Росії, наполегливо намагається зберігати дані про громадян на комп'ютерах усередині країни, а не за кордоном також Індія[243]. Робота в напрямі формування узгодженого підходу до кібербезпеки ведеться в рамках БРІКС у різних площинах, зокрема науковій, де ініційовано міжінституційний проєкт CyberBRICS, який має на меті передусім "зіставити існуючі нормативні документи, визначити найкращі практики й розробити пропозиції щодо політики у сферах управління кібербезпекою (включаючи регулювання персональних даних), політики доступу до інтернету" в країнах БРІКС[244].

3.2. Проблеми взаємодії США й Китаю в сфері кібербезпеки

Кібербезпека як сфера конкуренції між США й Китаєм

Тема кібербезпеки є набагато більш сучасною, ніж більшість інших питань в історії відносин між Сполученими Штатами й Китаєм. Проте швидкий розвиток технологій і зростаюча залежність суспільства від інтернету дають підстави перенести фокус уваги саме на цю сферу.

Відтоді як суспільно-економічні відносини почали розвиватися в напрямі кіберпростору, а інтернет став основним середовищем інформаційної роботи й комунікації, відносини між Сполученими Штатами й Китаєм ставали напруженими. Це стало результатом збільшення кількості проблем кібершпигунства з боку обох країн і в свою чергу призвело до того, що дві

[243] Basu Arindrajit, Hickok Elonnai and Chawla Aditya Singh (2019). Unpacking Policy Moves For Sovereign Control Of Data In India. *Cyberbricks*. 26.03.2019. URL: https://cyberbrics.info/unpacking-policy-moves-for-sovereign-control-of-data-in-india/

[244] Cyberbricks. About us. URL: https://cyberbrics.info/about-us/

держави стали найбільш звинуваченими в атаках кібершпигунства[245]. США звинувачують Китай у тому, що з його боку часто здійснюються кібератаки з метою втручання в бізнес-інтереси й різні комерційні справи, такі як крадіжка комерційної таємниці, інтелектуальної власності для нових технологій та іншої інформації, щоб отримати комерційну вигоду. І навпаки, Китай часто звинувачує Сполучені Штати в тому, що вони домінують в інтернеті й використовують своє становище в світі кіберпростору для пошуку вигідних ситуацій і збору розвідданих[246].

Якщо розглянуті в розділі І сучасні випадки кібератак поки що достеменно не ідентифіковані з конкретною країною, то в тих, що здійснені в попередні роки, США мають підстави звинувачувати Китай, — на підставі проведених розслідувань. Компанія Mandiant, що базується в Сполучених Штатах, виявила кілька так званих розширених постійних загроз (APT), які були здійснені з боку Китаю, часто із залученням інших країн, таких як Російська Федерація. У звіті компанії зазначається, що станом на 2013 р. існувало достатньо доказів, які показують, що Китай знає про діяльність різних груп у сфері кібершпигунства. APT1 — це назва діяльності, яку вели багато членів підрозділу 61398 Народно-визвольної армії Китаю. У звіті показано, що з 2006 р. до 2013 р. в ході APT1 зламано й викрадено сотні терабайтів інформації з понад 141 компанії, з яких 87 % базувалися в англомовних країнах. Найбільшою метою атак були Сполучені Штати, в яких базуються 115 зламаних компаній[247]. Можна припустити, що значна частина цілей хакерських атак у США пов'язана не лише з APT1, але й з багатьма іншими загрозами, які використовував китайський уряд.

У 2014 р. Міністерство юстиції США висунуло звинувачення п'ятьом чиновникам китайської армії в незаконному отриманні та розповсюдженні

[245] Julian Nicholas (2021). United States' and China's Cybersecurity Policies: Collaboration or Confrontation? *Journal of International Relations,* January 24, 2021. URL: http://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation

[246] Brown, G., Yung, C. D. (2017). Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace. *The Diplomat.* URL: https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/

[247] Mandiant Consulting Services, "APT1: Exposing One of China's Cyber Espionage Units". 2013. URL: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

комерційної таємниці зі Сполучених Штатів на користь представників економічної сфери Китаю. Це був один із перших сигналів для КНР про те, що Сполучені Штати мають усе більше підстав звинувачувати Китай в його причетності до кіберзлочинів. Після арешту й пред'явлення звинувачення військовослужбовцям китайської армії в Сполучених Штатах китайські ЗМІ назвали це помстою, щоб зберегти обличчя за витоки інформації через Едварда Сноудена, представника американських інформаційних спецслужб, який втік у невідомому напрямі в 2013 р. Пізніше того ж року Агентство національної безпеки США повідомило, що Китай здійснив величезну кількість кібератак проти Сполучених Штатів за короткий проміжок часу, і сотні з них були успішними[248].

Унаслідок постійного протистояння, яке спостерігалося між Китаєм і Сполученими Штатами, тодішній президент Барак Обама запросив Сі Цзіньпіна відвідати США з державним візитом, з основною темою — скоординувати протидію кібершпигунству. Сполучені Штати хотіли забезпечити захист своїх корпорацій від крадіжки інтелектуальної власності. Зрештою обидві сторони дійшли угоди, яку підписано в 2015 р. й засновано на посиленні комунікації й співпраці між ними. Також у документі підтверджено, що жодна зі сторін не буде свідомо здійснювати крадіжку інтелектуальної власності в іншої сторони. Також було погоджено розробити й запропонувати належні норми поведінки між державами для кіберпростору в міжнародному співтоваристві[249].

Останніми роками відносини між Китаєм і Сполученими Штатами стають усе більш напруженими. На жаль, зазначена вище угода проіснувала недовго, оскільки обидві сторони вчинили дії, які варіюються від загрозливих до незаконних. Протягом двох років після підписання Угоди про кібербезпеку між США й Китаєм у 2015 р. проблема крадіжки інтелектуальної власності не

[248] Brown, G., Yung, C. D. (2017). Evaluating the US-China Cybersecurity Agreement, Part 3: Over a year later, what impact has the 2015 cyber agreement had on U.S.-China relations?. *The Diplomat*. URL: https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/

[249] Brown, G., Yung, C. D. (2017). Evaluating the US-China Cybersecurity Agreement, Part 3: Over a year later, what impact has the 2015 cyber agreement had on U.S.-China relations?. *The Diplomat*. URL: https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/

зменшилась, а набула іншої форми. Хакерські групи з КНР замість того, щоб зосередитися на крадіжці інтелектуальної власності компаній у Сполучених Штатах, як це було раніше, тепер реалізують різні форми шпигунства проти державних структур. Оскільки договір 2015 р. визначив умови, які забороняють крадіжку інтелектуальної власності, за технічними особливостями державні дані виходять за межі положень угоди. Хакери в Китаї також використовували злам, щоб проникнути в американські компанії, такі як Google й Intel[250].

Китайські атаки на фірми зі Сполучених Штатів і урядові ресурси не залишились непоміченими. Адміністрація Трампа вдалася до заборони технологій китайських державних компаній, зокрема Huawei. Піком протистояння з компанією стало затримання її фінансового директора в Канаді. Навіть більше — за твердженнями в китайській пресі, Сполучені Штати почали власну форму пропагандистської війни щодо Huawei у своїх спробах демонізувати корпорацію перед своїми союзниками, зокрема партнерами в рамках кіберугоди Five Eyes [251] . Хоча, як припускають автори подібних публікацій, не виключена ймовірність того, що оскільки Huawei і Китай зараз є світовими лідерами в технології 5G, Сполучені Штати роблять спроби зупинити їх зростання. Зі свого боку Китай звинувачує США в низці кібератак і кібершпигунських інцидентів, про що детальніше йтиметься далі.

Світовими лідерами в сфері кібербезпеки сьогодні є США й Китай — дві найбільші економіки світу. Але Сполучені Штати залишаються, безумовно, найбільш кіберспроможною країною. Такий висновок міститься в доповіді, опублікованій у червні 2021 р. британським аналітичним центром Міжнародного інституту стратегічних досліджень, у якій розглядаються кібер-спроможності п’ятнадцяти найбільших світових гравців у сфері хакерства й цифрового захисту. У звіті оцінюються можливості як уряду, так і приватного сектора. Найбільш

[250] Greenberg, A. (October 13, 2017). “China tests the limits of its U.S. hacking truce,” *Wired*. URL: https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/#

[251] Soo, Z. (April 22, 2019). How Huawei beat America’s anti-China 5G propaganda war in Southeast Asia, years before it even began. *South China Morning Post*. URL: https://www.scmp.com/tech/article/3006935/how-huawei-beat-americas-anti-china-5g-propaganda-war-southeast-asia-years-it

потужних супротивників США, Росію й Китай, віднесено до другого рівня кіберпотужності, так само як Великобританію, Канаду, Австралію, Ізраїль і Францію[252].

Китай досяг значного прогресу в зміцненні своїх кібер-можливостей, але далеко не настільки, щоб скоротити розрив зі США. І головною причиною є відносне становище цифрових економік двох країн, де США залишаються далеко попереду, незважаючи на цифровий прогрес Китаю. Така домінуюча позиція пояснюється багатьма факторами, зокрема[253]:

- домінуючим військовим потенціалом як у наступальних, так і в оборонних кіберспроможностях;
- провідним у світі персоналом американських технологічних компаній і компаній з кібербезпеки;
- системним державним підходом до кібербезпеки й управління ризиками.

Проте швидкий цифровий розвиток Китаю й зростаюча кількість технологічних фірм роблять його "єдиною державою, яка зараз має намір приєднатися до США на першому рівні кіберпотужності"[254]. Найважливішим фактором для загальної кіберспроможності країни є наявність кадрів вітчизняних компаній, зосереджених на інформаційно-комунікаційних технологіях, які можуть розвивати кібер-спроможності. Саме це дає Китаю з його численними технологічними й телекомунікаційними компаніями, що швидко розвиваються, найкращі шанси кинути виклик позиції Сполучених Штатів на вищому рівні.

[252] Cyber Capabilities and National Power: A Net Assessment. *IISS. Research Papers*. 28th June 2021. URL: https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/

[253] Schaffer Aaron (June 28, 2021). The Cybersecurity 202: The United States is still number one in cyber capabilities. *The Washington Post*. URL: https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/

[254] Cyber Capabilities and National Power: A Net Assessment. *IISS. Research Papers*. 28th June 2021. URL: https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/

Китай як джерело кіберзагроз для США

Історія питання

Китай активно розвиває свій кіберпростір, і це дає підґрунтя також для активізації кіберзлочинності й виникнення інших кіберзагроз. Із початком епохи соціальних мереж і масового використання інтернету з метою ведення бізнесу стали з'являтися повідомлення про китайських кібер-злочинців і кібер-шпигунів. Але якщо десятиліття тому більшість виявлених фактів асоціювалася з використанням низькорівневих фішингових електронних листів проти американських компаній і крадіжкою інтелектуальної власності, то до сьогодні хакерські атаки з Китаю перетворились на серйозно організовані операції, а сам Китай сприймається в США як досвідчений і зрілий супротивник[255].

У Сполучених Штатах Китай почали асоціювати з масштабним джерелом кіберзагроз після серії атак на початку другого десятиліття XXI ст. У січні 2010 р. компанія Google заявила, що вона й більше двадцяти інших компаній стали жертвами складної кібератаки, яка пізніше отримала назву Operation Aurora, з боку хакерів із Китаю, яка призвела до крадіжки інтелектуальної власності. Хоча хакери ніколи не були публічно ідентифіковані, інцидент посилив напруженість між Вашингтоном і Пекіном через наявність непрямих доказів того, що значна кількість кібератак на американські інституції походить із Китаю. Представники IT-компанії Symantec повідомили, що хакери, які стоять за операцією "Аврора", зосередились на крадіжці інтелектуальної власності, наприклад, проєктної документації в оборонних підрядників і їхніх постачальників, уключаючи судноплавні, авіаційні, збройні, енергетичні, виробничі, інженерні й електронні компанії. Другою за поширенням групою цілей хакерів були неурядові організації, які займаються питаннями прав людини в Тибеті, а третьою — фінансові фірми й компанії, що займаються програмним забезпеченням[256].

[255] Perlroth Nicole (July 19, 2021). How China Transformed Into a Prime Cyber Threat to the U.S. *The New York Times*. URL: https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html

[256] Finkle Jim (Sept. 12, 2012). Hundreds more cyber attacks linked to 2009 Google breach. *Reuters.* URL: https://www.reuters.com/article/cybersecurity-espionage-idUSL2E8K7A9E20120907

У 2013 р. китайців звинувачено в атаці на New York Times. Хакери, ймовірно з Китаю, здійснювали маршрутизацію через мережу газети протягом щонайменше чотирьох місяців, викрадаючи паролі репортерів у очевидній спробі ідентифікувати джерела й зібрати інші розвідувальні дані про історії, пов'язані з сім'єю прем'єр-міністра Китаю Вен Цзябао. Злам співпав із розслідуванням, опублікованим газетою Times роком раніше, яке розглядало статки, що накопичила сім'я китайського прем'єр-міністра. Хакери зламали мережу, коли газета завершувала опрацювання матеріалів розслідування. Були зламані електронні пошти голови шанхайського бюро газети Девіда Барбози, який проводив розслідування, а також керівника південноазійського бюро газети в Індії Джима Ярдлі, який раніше працював у Пекіні[257].

У 2014 р. президент США Барак Обама назвав кібератаки "реальною загрозою" безпеці й економіці США. Сполучені Штати звинуватили офіцерів китайської армії в кібер-зламі американських компаній приватного сектора задля отримання конкурентної переваги. Генеральна прокуратура США стверджує, що офіцери викрали комерційні таємниці та внутрішні документи у п'яти компаній і профспілки. Проте Китай відкинув звинувачення й попередив, що ця справа зашкодить американо-китайським відносинам[258].

Сполучені Штати, очевидно, мали підстави для таких звинувачень, оскільки на початку 2013 р. компанією Mandiant, що надає послуги в сфері кібербезпеки, опубліковано результати розслідування, в якому стверджується, що за сотні (а за деякими оцінками — тисячі) атак на американські компанії відповідав один шанхайський підрозділ Народно-визвольної армії Китаю (НВАК), відомий як підрозділ 61398. Mandiant відстежила окремих членів найактивніших китайських хакерських груп (таких як "Comment Crew", або "Шанхайська група") до "порога штабу військової частини"[259].

[257] Zetter Kim (01.31.2013). New York Times Hacked Again, This Time Allegedly by Chinese. *WiredI*. URL: https://www.wired.com/2013/01/new-york-times-hacked/

[258] US justice department charges Chinese with hacking. *BBC*. 14 May, 2014. URL: https://www.bbc.com/news/world-us-canada-27475324

[259] Chinese Army unit is seen as tied to hacking against U.S. *Atlantic Council*. February 19, 2013. URL: https://www.atlanticcouncil.org/blogs/natosource/chinese-army-unit-is-seen-as-tied-to-hacking-against-us/

Підрозділ 61398 (формально 3-й відділ Управління Генерального штабу 2-го Бюро НВАК) майже ніде не згадується в офіційних китайських військових описах. Проте аналітики розвідки стверджують, що він є центральним елементом китайського комп'ютерного шпигунства, зосередженим на політичній, економічній та військовій розвідці[260]. У період 2002 — 2012 рр., за висновками американської компанії з кібербезпеки "Fireye", у рамках діяльності цієї групи здійснено понад тисячу кібератак проти великих компаній і відомих політиків. Невдовзі після першого візиту китайського лідера Сі Цзіньпіна до США в 2015 р. укладено угоду про те, що Китай припинить хакерські атаки на американські компанії для своєї промислової вигоди. Відтоді протягом 18 місяців, за часів адміністрації Обами, спостерігалося помітне зменшення інтенсивності китайського хакерства[261].

Сучасний стан

Після того як президент Дональд Трамп вступив на посаду й ініціював торговельні конфлікти й інші напруження з Китаєм, хакерські атаки відновилися. Причому змінилися як їх джерело, так і суть. Хакерів НВАК замінили оперативники, що працюють за дорученням Міністерства державної безпеки, яке керує розвідкою, безпекою й таємною поліцією Китаю. Тепер реалізатори кібер-нападів діють не з НВАК, а з "незалежної" мережі підставних компаній і підрядників, включаючи інженерів, які працювали на деякі з провідних технологічних компаній. Досі недостатньо інформації про те, як саме Китай працював із цими слабо афілійованими хакерами — або їм платили готівкою, або в них не було іншого вибору, окрім як робити все, що просить держава[262].

Особливо активізувалися зловмисники в на початку 2020-х рр. Так, у липні 2021 р. Сполучені Штати звинуватили Китай у кібератаках, відмітивши, що ці атаки були дуже агресивними. Вони є ознакою того, що Китай перетворився на

[260] Cyber Threat Intelligence on Advanced Attack Groups and Technology Vulnerabilities. Threat Intelligence Reports. Fireyes, 2013.

[261] Obama and Xi Jinping of China Agree to Steps on Cybertheft. *The New York Times*. 25 Sept, 2015. URL: https://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html

[262] Wolfe Derek (July 21.2021). How China Became a Digital Adversary and Threat to the U.S. *GSIExchange.* URL: https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/

значно більш витонченого й зрілого цифрового супротивника ніж той, який хвилював американських чиновників десять років тому. Сполучені Штати та їхні союзники звинуватили Китай у глобальній кампанії кібершпигунства, зібравши надзвичайно широку коаліцію країн, до якої приєдналися країни НАТО, Європейського Союзу, Австралія, Великобританія, Японія й Нова Зеландія. Держсекретар США Ентоні Блінкен заявив, що ця атака становить "велику загрозу нашій економічній та національній безпеці"[263].

Одночасно міністерство юстиції США висунуло звинувачення чотирьом громадянам Китаю — трьом співробітникам служби безпеки й одному хакеру-зламнику — в нападі на десятки компаній, університетів і державних установ у Сполучених Штатах і за кордоном[264]. Відповідно до цієї заяви, громадяни Китаю діяли з підставних компаній, таких як Хайнань Сяньдунь, створених Міністерством державної безпеки, щоб дати китайським спецслужбам правдоподібне прикриття. Також звинувачено китайські університети в тому, що вони відіграють важливу роль, набираючи студентів у підсобні компанії та керуючи їхніми ключовими бізнес-операціями, такими як нарахування заробітної плати. Обвинувальний акт вказував і на китайських "пов'язаних з урядом" хакерів, які проводили атаки програм, що вимагають у компаній мільйони доларів. Це свідчить про суттєві зміни в географії кіберзагроз такого типу, оскільки раніше атаки зловмисників-вимагачів походили переважно з Росії, Східної Європи й Північної Кореї.

Звинувачення з боку адміністрації президента США в кібератаках показують, що Китай за останні роки реорганізував свої хакерські операції. Якщо колись практикувались відносно прості хакерські атаки на іноземні компанії, аналітичні центри й державні установи, то сьогодні здійснюються приховані, децентралізовані цифрові напади на американські компанії й інтереси в усьому

[263] @SecBlinken [Secretary Antony Blinken]. United States government official. 19 лип. 2021. URL: https://twitter.com/secblinken/status/1417103602133479 42

[264] U.S. charges four Chinese nationals charged in global hacking campaign. *Reuters*, July 19, 2021. URL: https://www.reuters.com/technology/four-chinese-nationals-charged-global-hacking-campaign-us-justice-department-2021-07-19/

світі. За словами американських чиновників і представників ділових кіл, хакерські дії, які реалізувались підрозділами Народно-визвольної армії Китаю через непрофесійно сформульовані електронні листи (фішинг), тепер здійснюються елітною мережею з підрядних компаній та університетів, які працюють за вказівкою Міністерства державної безпеки Китаю[265].

Хоча фішингові атаки залишаються актуальними, шпигунські кампанії пішли в підпілля, застосовуючи складніші методи. Серед них — використання "нульових днів", або невідомих раніше дір у безпеці в поширеному програмному забезпеченні, як-от служба електронної пошти Microsoft Exchange і пристрої безпеки Pulse VPN, від яких важче захистити та які дають змогу китайським хакерам працювати непоміченими протягом більш тривалого періоду[266]. "Те, що ми спостерігали протягом останніх двох-трьох років, — це зростання Китаю", — сказав Джордж Курц, виконавчий директор компанії з кібербезпеки CrowdStrike. "Вони працюють більше як професійна розвідувальна служба, ніж оператори "розбою й грабежів", яких ми бачили в минулому" (цит. за: Wolfe Derek, 2021[267]).

Китай уже давно є однією з найбільших цифрових загроз для Сполучених Штатів. У квітні 2021 р. найвищі посадові особи американської розвідки надали свою оцінку світових загроз, що зачіпають інтереси США, зосередившись на кібербезпеці й військових загрозах із боку Пекіна й Москви, а також на загрозі внутрішнього й міжнародного тероризму. Директори Національної розвідки, ЦРУ, АНБ, ФБР та Управління оборонної розвідки охарактеризували Китай як близького конкурента, що кидає виклик Сполученим Штатам на багатьох аренах, водночас домагаючись перегляду глобальних норм таким чином, щоб сприяти авторитарній китайській системі й що Пекін здійснює "епохальний

[265] Perlroth Nicole (July 19, 2021). How China Transformed Into a Prime Cyber Threat to the U.S. *The New York Times*. URL: https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html

[266] Там само.

[267] Wolfe Derek (July 21.2021). How China Became a Digital Adversary and Threat to the U.S. *GSIExchange.* URL: https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/

геополітичний зсув", який відбувся на його користь за рахунок Сполучених Штатів[268].

Адміністрація Байдена підняла боротьбу з кіберзагрозами на якісно новий рівень, перетворивши кібератаки, включаючи атаки програм-вимагачів, у великий дипломатичний фронт із такими наддержавами, як Росія й Китай. Розвідувальне співтовариство США сформувало свою позицію щодо Китаю як системного джерела потенційних загроз, пов'язаних із реалізацією цією країною власної стратегії, яка "заходить на територію" національних інтересів США. У звіті щодо стану загроз у світовому масштабі, опублікованому в 2021 р., Китай оцінюється як джерело "результативної й ефективної" загрози кібершпигунства, що володіє значними можливостями кібератак і становить зростаючу загрозу впливу. У свою чергу кіберпереслідування Китаю й поширення пов'язаних технологій збільшують загрози кібератак на США.

Сьогодні американська розвідка конкретизує такі основні кіберзагрози з боку Китаю[269]:

- Китай може здійснювати кібератаки, які, як мінімум, можуть спричинити локалізовані тимчасові порушення роботи критичної інфраструктури в Сполучених Штатах;
- Китай є світовим лідером із застосування систем спостереження й цензури для моніторингу свого населення й придушення інакомислення, особливо серед етнічних меншин, таких як уйгури. Пекін проводить кібер-вторгнення, які впливають на громадян США й інших громадян за межами його кордонів — наприклад, хакерство журналістів, крадіжка особистої інформації або атаки на інструменти, які дають змогу вільно висловлюватися в інтернеті — як частину зусиль щодо спостереження за уявними загрозами владі КПК та адаптації зусиль щодо впливу;

[268] Neumann Scott (April 14, 2021). Intelligence Chiefs Say China, Russia Are Biggest Threats To U.S. *NPR*. URL: https://www.npr.org/2021/04/14/987132385/intelligence-chiefs-say-china-russia-are-biggest-threats-to-u-s

[269] Annual Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence. April 9, 2021. URL: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

- Пекін використовує свою участь у глобальних зусиллях із боротьби з COVID-19 для експорту своїх інструментів і технологій спостереження;
- операції з кібершпигунства в Китаї включали компрометацію телекомунікаційних фірм, постачальників керованих послуг і програмного забезпечення, що широко використовується, а також інших цілей, що створює можливості для потенційного збору розвідувальної інформації, атак або операцій упливу.

За останні роки з'явилося достатньо ознак того, що Китай започаткував нову політику у сфері кібератак, змістивши фокус із використання кібершпигунства на користь державним компаніям до орієнтації на цілі національної безпеки. Наприклад китайські спеціалісти в сфері кібербезпеки повинні протягом двох днів повідомляти державу про виявлені ними діри в захисті інформаційних систем, такі як "нульові дні" (недоліки програмного забезпечення, апаратного чи програмного забезпечення, невідомі стороні чи сторонам, відповідальним за виправлення чи інше виявлення недоліків), такі як були використані для атаки на Microsoft Exchange. Вже в 2016 р. влада раптово закрила найвідомішу приватну платформу Китаю для звітності про нульові дні й заарештувала її засновника[270]. Через два роки китайська поліція оголосила, що почне виконувати закони, що забороняють "несанкціоноване розкриття" вразливостей. Того ж року китайські хакери, що регулярно брали участь у великих західних хакерських конгресах, перестали з'являтися навіть на запрошення[271].

Фактично китайська держава взяла хакерську діяльність під повний державний контроль. Із цього приводу згаданий вище Дж. Курц повідомив таке: "Якщо вони продовжуватимуть підтримувати цей рівень доступу з контролем, який у них є, їхня розвідувальна спільнота виграє... Це гонка озброєнь у кіберпросторі"[272].

[270] China's 'White-Hat' Hackers Fear Dark Times After Community Founder Is Detained. *The Wall Street Journal*, 1 Aug. 2016. URL: https://www.wsj.com/articles/BL-CJB-29440

[271] China's government is keeping its security researchers from attending conferences. *Cyberscoop*. Mar. 8, 2018. URL: https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/

[272] Цит. за: Wolfe Derek (July 21.2021.) How China Became a Digital Adversary and Threat to the U.S. *GSIExchange.* URL: https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/

Позиція Китаю

Китай завжди заперечував свою причетність до кібератак, водночас звинувачуючи США в організації злочинності й шпигунства в кіберпросторі. У відповідь на серію виступів американських офіційних осіб, які з початком каденції Дж. Байдена оголосили Китай серед головних джерел кіберзагроз, китайські рупори називають США "провідною світовою шпигунською імперією з масовими злочинами в кіберпросторі" [273]. А нову жорстку американську політику кібербезпеки щодо Китаю в Пекіні пояснюють спробами "стримати Китай і в рамках своїх невпинних зусиль сформувати антикитайський хор серед своїх основних союзників", для чого "адміністрація Байдена прагне перетворити кіберпростір на нове поле бою, об'єднавшись зі своїми союзниками, щоб звинуватити Китай у проведенні кібератак у всьому світі"[274].

Усі американські звинувачення Китаю в сприянні кіберзлочинності й у кібершпигунстві негайно засуджуються китайськими дипломатами, а також певними експертами, які натомість стверджують, що Китай завжди був довгостроковою жертвою кібератак США. У тому ж дусі Китай заперечує звинувачення на свою адресу й з боку НАТО, Європейського Союзу, Австралії, Великої Британії, Канади, Японії, Нової Зеландії, закликаючи США та їхніх союзників припинити критикувати Китай на цю тему, оскільки нібито США самі тривалий час були організатором кібератак.

Звинувачуючи в організації кібератак передусім ЦРУ, китайські посадовці посилаються на певні інтернет-дослідження, які буцімто доводять, що США стоять за хакерською діяльністю, спрямованою на аерокосмічний сектор Китаю, науково-дослідні установи, інтернет-компанії, нафтову промисловість і державні установи. Так, Qihoo, основний постачальник послуг із кібербезпеки, чиї дослідження, як правило, використовують для розуміння цифрової безпеки Китаю, повідомив, що атаку з боку Центрального розвідувального управління

[273] Qingqing Chen, Siqi Cao (Jul 20, 2021). US turns cyberspace into another anti-China battlefield, 'futile to contain Beijing'. *Global Times*. URL: https://www.globaltimes.cn/page/202107/1229168.shtml

[274] Там само.

було спрямовано на авіаційний та енергетичний сектори Китаю, науково-дослідні організації, інтернет-компанії й урядові установи. У компанії додали, що злам міг бути спрямований на відстеження “маршруту подорожей важливих осіб”[275].

Звинувачення, висунуті на адресу Пекіна американськими компаніями, роками викладаються в довгих звітах, що містять велику кількість даних. Зовсім недавно китайські компанії почали робити те ж саме щодо іноземних хакерських груп. Потрібно зазначити, що Сполучені Штати рідко коментують, коли їх звинувачують у кібершпигунстві.

Риторика китайських посадовців у зв’язку з американськими звинуваченнями на адресу їхньої країни різко негативна. Так, речник міністерства закордонних справ Китаю Чжао Ліцзянь заявив, що ці звинувачення ”є абсолютно неприйнятними, оскільки вони виходять із політичних цілей з метою наклепу й стримування Китаю”, і що така позиція США може призвести до погіршення китайсько-американських відносин, які можуть перейти до нового мінімуму[276]. Китайська влада заявляє про те, що протягом багатьох років Китай був основною жертвою кібератак. Згідно зі щорічним звітом Національної технічної групи з реагування на надзвичайні ситуації / координаційного центру Китаю (CNCERT/CC), у 2020 р. близько 5,31 млн хостів на материковій частині Китаю контролювали загалом близько 52000 закордонних серверів керування шкідливими програмами, а трійка найбільших джерел закордонних серверів за кількістю скомпрометованих китайських хостів — усі з країн — членів НАТО[277].

Відома антивірусна компанія Antiy Labs опублікувала документ, у якому стверджує, що з 2000 р. США вже проводили масштабні атаки на глобальному рівні, — Equation, підрозділ Агентства національної безпеки (АНБ), зламав

[275] Satter Raphael (March 3, 2020). Chinese cybersecurity company accuses CIA of 11-year-long hacking campaign. *Reuters*. URL: https://www.reuters.com/article/us-china-usa-cia-idUSKBN20Q2SI

[276] Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on July 29, 2021. 2021/07/29. URL: https://www.mfa.gov.cn/ce/cohk//eng/Topics/fyrbt/t1896083.htm

[277] Spokesperson of the Chinese Mission to the EU Speaks on a Question Concerning the Statements from the EU and NATO on the So-called Chinese Malicious Cyber Activities. 2021/07/20. URL: https://static.poder360.com.br/2021/07/nota-china-ataques-hackers.pdf

важливі інтернет-цілі в усьому світі, й що Сполучені Штати мають найбільший у світі арсенал атак у кіберпросторі, включаючи високорівневий шкідливий код, а також велику кількість нерозкритих інструментів для використання вразливостей і платформ для атак[278]. За даними китайської компанії, США проникають у інформаційні системи й атакують китайського телекомунікаційного гіганта Huawei, а також країни, якщо вони купують продукцію Huawei. Також стверджується, що США використовують масову хакерську діяльність для того, щоб атакувати низку країн, уключаючи Китай, з метою отримання розвідданих.

Китайський технологічний гігант 360 Security Technology повідомляв про серію атак на китайські аерокосмічні, науково-дослідні установи, нафтову промисловість і великі інтернет-компанії, здійснені хакерською організацією, пов'язаною з ЦРУ. Компанія нібито знайшла докази того, що хакерська група, APT-C-39 належить ЦРУ, а злам, простежений з 2008 р., в основному спрямований на організації в Пекіні, провінціях Гуандун і Чжецзян[279].

У Китаї пояснюють загострення конкуренції зі США в сфері кібербезпеки тим, що Америка намагається зберегти свою гегемонію у світі. Особливо це питання загострилось із приходом адміністрації Байдена, коли з боку Китаю розпочалась масштабна й системна інформаційна кампанія, в якій кібер-діяльність і звинувачення Китаю як джерела кіберзагроз розглядаються в якості елемента загальної гри з боку США задля формування антикитайського альянсу, спрямованого на відродження американської гегемонії.

Державні ЗМІ Китаю пояснили перший закордонний візит президента Джо Байдена до Європи в червні 2021 р. так: "старий міжнародний порядок після Другої світової війни, очолюваний США, стає все більш нежиттєздатним, а

[278] The Analysis of Equation Drug —the Fourth Analysis Report of Equation Group. January 26, 2017. URL: https://www.antiy.net/p/the-analysis-of-equation-drug-the-fourth-analysis-report-of-equation-group/

[279] The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China's Critical Industries for 11 Years. 360 Core Security. URL: https://blogs.360.cn/post/APT-C-39_CIA_EN.html

новий світовий порядок ще далекий від установлення, оскільки глобальна система переходить від однополярної до багатополярної”[280].

Фактично можна говорити про наявність у Китаю чіткого власного уявлення про зміну світового порядку, що впливає на зовнішню орієнтацію Пекіна в епоху Байдена. У Китаї фіксують зміни в зовнішньополітичній стратегії США як такі, що становлять загрозу через те, що адміністрація Байдена розширює політичну траєкторію Вашингтона, визначаючи “більш наполегливий і авторитарний Китай” як “єдиного конкурента, потенційно здатного поєднати свою економічну, дипломатичну, військову й технологічну силу, щоб кинути постійний виклик стабільній і відкритій міжнародній системі” [281] . Як зазначають китайські спостерігачі, незважаючи на деякі можливості для співпраці, політика Байдена в Китаї схиляється до ”стратегічної конкуренції й навіть конфронтації“[282].

У Китаї вважають, що на відміну від односторонньої позиції Трампа з відвертими нападами на Компартію Китаю, Байден обрав альтернативні інструменти багатосторонності й взаємодії з союзниками для подальшої мети — обмеження впливу Китаю. За словами держсекретаря Тоні Блінкена, перші американо-китайські переговори в березні 2021 р. продемонстрували зростаючі тертя щодо прав людини, Тайваню, кібербезпеки й “економічного примусу до наших союзників”[283]. Причому така позиція щодо більш жорсткої стратегії в бік Китаю підтримується обома американськими партіями, що засвідчено в Акті

[280] Chen Qingqing, Xu Keyue and Xu Yelu (June 6, 2021). US Turning G7 Into Anti-China, Anti-Russia Chorus ‘Wishful Thinking. *Global Times*. URL: https://www.globaltimes.cn/page/202106/1225524.shtml

[281] The White House, “Renewing America’s Advantages: Interim National Security Strategic Guidance”. March 2021, 20, 8. URL: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

[282] Liu Guozhu, “拜登政府国家安全战略的基本方针与发展方向, (Bài dēng zhèngfǔ guójiā ānquán zhànlüè de jīběn fāngzhēn yǔ fāzhǎn fāngxiàng) [Основна політика та напрям розвитку Стратегії національної безпеки адміністрації Байдена]. Dangdai Shijie 5 (2021): 50—57. URL: https://webcache.googleusercontent.com/search?q=cache:7-mexZ_mX1EJ:https://dysw.cnki.net/kcms/detail/detail.aspx%3Ffilename%3DJSDD202105008%26dbcode%3DCJFD%26dbname%3DCJFD2021%26v%3D+&cd=1&hl=uk&ct=clnk&gl=ua

[283] US Department of State, “Secretary Antony J. Blinken, National Security Advisor Jake Sullivan, Director Yang and State Councilor Wang at the Top of Their Meeting,” Anchorage, March 18, 2021. URL: https://www.state.gov/secretary-antony-j-blinken-national-security-advisor-jake-sullivan-chinese-director-of-the-office-of-the-central-commission-for-foreign-affairs-yang-jiechi-and-chinese-state-councilor-wang-yi-at-th/

Сенату США про стратегічну конкуренцію (2021 р.)[284]. В основі американської стратегії — констатація того, що ”Китайська Народна Республіка використовує свою політичну, дипломатичну, економічну, військову, технологічну й ідеологічну владу, щоб стати стратегічним глобальним конкурентом для Сполучених Штатів. Політика, яку КНР дедалі частіше проводить у цих сферах, суперечить інтересам і цінностям Сполучених Штатів, їхніх партнерів і більшої частини решти світу”, і що така китайська політика ”поставить під загрозу майбутній мир, процвітання й свободу міжнародного співтовариства в найближчі десятиліття”[285].

У такому контексті Пекін інтерпретує посилення американської політики кібербезпеки як “нову зброю США” у формуванні міжнародного фронту задля стримування Китаю. У зв’язку з цим можна навести слова Лі Хайдуна, професора Інституту міжнародних відносин Китайського університету закордонних справ: “Байден знайомий з такою тактикою “формування альянсу” в протистоянні з Китаєм, наприклад раніше він намагався створити альянс щодо вакцин, альянс щодо зміни клімату, альянс безпеки тощо. Звинувачення в кібератаках додають деякі нові елементи до такої тактики” [286]. Цінь Ань, керівник Пекінського Інституту кіберпросторової стратегії, зазначив, що США використовують старі прийоми для стримування Китаю, оскільки Байден хоче показати своїм союзникам, що США все ще лідирують у світі. “Байден також хоче довести американцям, що він кращий за Трампа”[287].

Китай насторожено сприймає поширення такого американського підходу в аспекті кібербезпеки на союзників США. Так, на зустрічі НАТО в червні 2021 р. Джо Байден і партнери країни по НАТО наголосили на загрозах безпеці, які

[284] A BILL To address issues involving the People’s Republic of China (”Strategic Competition Act of 2021”). 117TH CONGRESS 1ST SESSION. URL: https://www.foreign.senate.gov/imo/media/doc/DAV21598%20-%20Strategic%20Competition%20Act%20of%202021.pdf

[285] Там само, с. 5.

[286] Qingqing Chen, Siqi Cao (Jul 20, 2021). US turns cyberspace into another anti-China battlefield, ‘futile to contain Beijing’. *Global Times*. URL: https://www.globaltimes.cn/page/202107/1229168.shtml

[287] US turns cyberspace into another anti-China battlefield, ‘futile to contain Beijing’. *National Cyber Security Ne*ws Today. July 28, 2021. URL: https://nationalcybersecuritynews.today/us-turns-cyberspace-into-another-anti-china-battlefield-futile-to-contain-beijing-cybersecurity-cyberattack/

надходять із боку Китаю й Росії, а в комюніке НАТО містилася теза про стримування Китаю, що розглядається як зміна стратегії Альянсу. МЗС Китаю засудило цей крок як перетворення кіберпростору на нове поле бою шляхом уведення військового альянсу в кіберпростір, — речник зовнішньополітичного відомства заявив, що "це не буде корисним для підтримки власної безпеки, але спровокує гонку озброєнь у кіберпросторі, посилить конфлікти між країнами в інтернеті й поставить під загрозу мир і безпеку"[288].

Кібернетичні загрози зростають випереджаючими темпами порівняно з усіма іншими проблемами, що пов'язані з розвитком кіберпростору. Сьогодні світовими лідерами в кіберсфері й секторі інформаційної (кібер) безпеки є США й Китай. Сторони звинувачують одна одну в кібератаках із економічною метою, в кібершпигунстві, а протягом останніх років — і в політично мотивованих діях проти інформаційних систем. Незважаючи на спроби узгодити політики в цій сфері, напруженість між США й Китаєм, у зв'язку з нарощенням кіберпотенціалу, зростає. І хоча США залишаються безумовним світовим лідером у сфері кібербезпеки, Китай швидко скорочує своє відставання, спираючись на потужний потенціал людських і економічних ресурсів у кіберсфері.

3.3. Взаємодія ЄС і США у сфері кібербезпеки

Європейський Союз і США мають подібні погляди на розвиток міжнародного співробітництва у сфері безпеки кіберпростору від того часу, коли вона стала актуальною в міжнародному вимірі, відзначаючи, що міжнародне співробітництво є центральним елементом кібербезпеки. Головною ознакою спільного для них західного підходу в питанні безпеки кіберпростору є дотримання принципу свободи обміну інформацією в мережі й демократичної концепції організації самого кіберпростору[289].

[288] Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on July 29, 2021. 2021/07/29. URL: https://www.mfa.gov.cn/ce/cohk//eng/Topics/fyrbt/t1896083.htm

[289] Taylor Emily, Hoffmann Stacie (2019). EU–US *Relations on Internet Governance*. Chatham House. URL: https://www.chathamhouse.org/publication/eu-us-relations-internet-governance. [Google Scholar]

Загальна демократична організація суспільства й свобода підприємницької діяльності, висока громадська активність відображаються на кіберпросторі, який не підлягає жорсткому управлінню, а розвивається за значної участі приватного сектора, коли держава забезпечує лише гарантії безпеки функціонування інформаційних систем та інформаційно-телекомунікаційної інфраструктури й боротьбу з кіберзлочинністю. Також держава забезпечує ефективну оборону й, відповідно, кіберзахист у рамках компетенції оборонних структур.

Загальний демократичний підхід, який поділяють країни — члени ЄС, сам Європейський Союз і США, означає, що кібербезпека не повинна забезпечуватися за рахунок основних прав і свобод, а також, що не повинно бути прямого й жорсткого урядового контролю в управлінні мережею, як це пропонують Росія й Китай, — управління інтернетом має регулюватися шляхом поєднання участі держави, промисловості й приватного сектора. Власне саме ці принципи — забезпечення прав і свобод людини й невтручання в управління інтернетом, розділяють демократичні ЄС і США з одного боку, й авторитарні Росію та Китай — з другого. Прихильники східної, російсько-китайської, моделі з домінуванням інтересів держави в питаннях інформаційної безпеки й інформаційним (кібер) суверенітетом, згуртовують частину країн світу в опозиції до прихильників демократичної концепції на основі ініціатив Росії й Китаю в ШОС, а також Росії на рівні ООН. На відміну від американсько-європейської багатосторонньої моделі управління мережею, російсько-китайський підхід толерує міжурядові, багатосторонні процеси, що характерно, наприклад, для Міжнародного телекомунікаційного союзу й сприяє авторитарним режимам. Така авторитарна модель все повніше реалізується в Росії, Китаї, Ірані.

Одним із перших спільних інтересів ЄС і США стала боротьба з кіберзлочинністю. Відповідну ініціативу Ради Європи 2001 р. (Будапештська конвенція) обидві сторони спільно підтримують на рівні ООН, координують свої зусилля на практиці й спільно діють для просування цього стандарту на міжнародному рівні. Конвенцію ратифіковано багатьма країнами, що не є

членами Ради Європи, включаючи Сполучені Штати, які мають статус спостерігача в Раді.

Популяризація Будапештської конвенції про кіберзлочинність і заохочення держав стати учасниками або ратифікувати конвенцію згодом, стали предметом успішної інституційної співпраці між європейською й американською сторонами, зокрема в рамках діяльності створеної в листопаді 2010 р. на спільному саміті Робочої групи ЄС і США з питань кібербезпеки й кіберзлочинності[290]. Групу створено для розробки спільних підходів до широкого кола питань кібербезпеки й кіберзлочинності й, зокрема, для "просування Конвенції Ради Європи про кіберзлочинність, уключаючи програму розширення приєднання всіх держав — членів ЄС, а також співпраці для надання допомоги державам за межами регіону в дотриманні її стандартів і приєднанні до них[291]".

Приєднання до Будапештської конвенції передбачає здійснення низки процедурно-правових заходів, уключно зі змінами до кримінальних і кримінально-процесуальних кодексів. Тому процес приєднання виявився досить тривалим і вимагає участі й підтримки з боку основних послідовників Конвенції, якими є країни ЄС і США. Окрім того, як сказано вище, розширення участі в Будапештській конвенції йде всупереч бажанню окремих держав, що дотримуються російсько-китайського підходу до кібербезпеки, розширювати свої кібер-суверенітети, адже конвенція заохочує обмін критичними електронними доказами між іноземними країнами, щоби правоохоронні органи могли ефективніше розслідувати й боротися з кібер-злочинами.

Також нагадаємо, що Росія, продовжуючи тривалу боротьбу за свою модель міжнародної координації у сфері боротьби з кіберзлочинністю, запропонувала прийняття нового глобального правового акту щодо кіберзлочинності на рівні ООН (одним із аргументів проти Будапештської конвенції її противники вважають

[290] EU-U.S. Summit 20 November 2010, Lisbon - Joint Statement. MEMO/10/597. Brussels, 20 November 2010. URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_10_597

[291] Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats. European Commission. MEMO/11/246 Brussels, 14th April 2011. URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_11_246

недостатньо високий міжнародний рівень, апелюючи до необхідності прийняття відповідного акта на рівні ООН). Під час Генеральної Асамблеї в 2019 р. прийнято відповідну резолюцію про кіберзлочинність і про створення комітету експертів для розгляду нової угоди ООН про кіберзлочинність для підготовки протягом декількох років проєкту такого документа[292]. Ця резолюція актуалізує давню мету Росії замінити Будапештську конвенцію Ради Європи, яка є єдиним міжнародним документом, що вирішує питання міжнародної взаємодії в сфері кіберзлочинності. Росія, яка раніше запропонувала альтернативний проєкт конвенції ООН [293], послідовно стверджує, що Будапештська конвенція є застарілою регіональною угодою й порушує принципи державного суверенітету й невтручання.

Опозицію російській ініціативі склали США, ЄС і багато держав-учасниць Будапештської конвенції, а заступник посла США Черіт Норман Шале заявила асамблеї перед голосуванням, що "ця резолюція підірве міжнародне співробітництво в боротьбі з кіберзлочинністю в той час, коли посилення координації є надзвичайно важливим [294] ". У свою чергу, виступаючи від Європейського Союзу, представник Фінляндії також підкреслив, що наявна міжурядова експертна група ООН із кіберзлочинності вже вирішує питання про те, чи потрібен новий договір[295]. Тобто США і ЄС на найвищому міжнародному рівні координують свої зусилля на практиці й спільно діють для просування стандарту, закладеного Будапештською конвенцією, на міжнародному рівні.

У червні 2021 р. в контексті виконання Резолюції 74/247 Генеральної Асамблеї ООН (27 грудня 2019 р.), якою було створено спеціальний міжурядовий комітет відкритого складу з представників усіх регіонів для розробки всеосяжної міжнародної конвенції про протидію використанню інформаційно-комунікаційних технологій у злочинних цілях, Росія представила

[292] 73/187. Countering the use of information and communications technologies for criminal purposes. UN General Assembly. 14 January 2019. URL: https://undocs.org/en/A/RES/73/187

[293] DRAFT UNITED NATIONS CONVENTION ON COOPERATION IN COMBATING INFORMATION CRIMES. The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Irelan. URL: https://www.rusemb.org.uk/fnapr/6394

[294] Цит. за: Lederer Edith M. (2019) UN gives green light to draft treaty to combat cybercrime. *AP*. December 28, 2019. URL: https://apnews.com/article/79c7986478e5f455f2b281b5c9ed2d15

[295] Там само.

перший проект Конвенції, головними цілями якої є [296] : вжиття кожною державою-учасницею заходів для визнання злочину відповідно до національного законодавства про кіберзлочинність; визначення нових процедур правового співробітництва у сфері кіберзлочинності; створення Міжнародної технічної комісії для боротьби з кіберзлочинністю й надання допомоги державам щодо виконання Конвенції.

Відповідно до давніх прагнень Росії напевно головною особливістю запропонованої Конвенції є акцент на принципі суверенітету. У преамбулі зазначено таке: "кожна держава має суверенітет і здійснює юрисдикцію над своєю територією щодо інформаційного простору відповідно до свого внутрішнього законодавства"[297]. (основною причиною неприєднання Росії до Конвенції про боротьбу з кіберзлочинами 2001 р. було те, що Будапештська конвенція дозволяє транскордонні кібероперації). Відтак забороняються транскордонні операції, які здійснюються комп'ютерними мережами держав без схвалення їх влади. Також потенційно обмежується екстрадиція особи за злочин, передбачений Конвенцією: "запитувана держава-учасниця може відмовити у видачі, якщо така екстрадиція може зашкодити її суверенітету, безпеці, громадському порядку чи іншим суттєвим суспільним інтересам" (ст. 47)[298].

Цю ініціативу позитивно сприйняла коаліція країн, що розвиваються ООН (Група 77) і Китай ("продовжуватимуть брати активну участь у виконанні Резолюції 74/247 ГА ООН щодо розробки всеосяжної міжнародної конвенції про протидію використанню інформаційно-комунікаційних технологій у злочинних цілях в рамках ООН"[299]). Натомість, позицію з цього приводу держав Заходу ще в листопаді 2019 р. чітко сформульовано зі сторони Сполучених Штатів:

[296] Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях. Проект. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf

[297] Там само.

[298] Там само.

[299] STATEMENT OF THE G-77 AND CHINA DURING THE FOURTEENTH UN CONGRESS ON CRIME PREVENTION AND CRIMINAL JUSTICE KYOTO, JAPAN 7-12 MARCH 2021, DELIVERED BY H.E. AMBASSADOR ALEJANDRO SOLANO ORTÍZ, PERMANENT REPRESENTATIVE OF COSTA RICA. URL: https://www.g77.org/vienna/wp-content/uploads/2021/03/G77ChinaKyotoLongVersionFinal_070321.pdf

”Сполучені Штати розчаровані рішенням авторів цієї резолюції винести її сьогодні на розгляд Третього комітету. Прийняття цієї резолюції вб’є клин між державами-членами й підірве міжнародне співробітництво в боротьбі з кіберзлочинністю в той час, коли посилена координація є важливою”[300].

Європейський Союз чітко не заявив про підтримку чи протидію до зазначеної конвенції, але свою позицію сформулював у Спільному повідомленні Європейському парламенту й Раді щодо імплементації Стратегії кібербезпеки ЄС на цифрове десятиліття в такий спосіб, що очевидно очікує з’ясування деталей і наслідків прийняття документа, оскільки покладається на правила процедури Генасамблеї ООН, де за відсутності консенсусу створений резолюцією 74/247 спеціальний комітет прийматиме рішення більшістю в дві третини голосів (“Остаточно прийняті методи включають важливі елементи для забезпечення інклюзивних процедур прийняття рішень і більш активної участі громадянського суспільства в роботі спеціального комітету[301]”). Тобто, по суті, ЄС не відіграє суттєвої ролі щодо запропонованої Конвенції, але пропонує свою візію для держав-членів щодо координації своїх поглядів, не полишаючи оголошеного курсу на підтримку Будапештської конвенції про кіберзлочинність як всеосяжної багатосторонньої правової бази для розвитку національного законодавства й міжнародного співробітництва. На рівні ООН про підтримку Будапештської конвенції заявлено серед пріоритетів ЄС в ООН під час 76-ї Генеральної Асамбле (вересень 2021 – вересень 2022)[302].

Проте з точки зору послідовників демократичного західного підходу до розвитку кіберпростору обов’язковий міжнародний договір у цій сфері має потенціал розширити урядове регулювання щодо вмісту в інтернеті й змінити

[300] Statement on Agenda Item 107 ‘Countering the use of information and communications technologies for criminal purposes’. U.S. Mission to the United Nations. November 18, 2019. URL: https://usun.usmission.gov/statement-on-agenda-item-107-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes/

[301] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Report on implementation of the EU's Cybersecurity Strategy for the Digital Decade. Brussels, 6.8.2021 JOIN(2021) 14 final/2. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2021:14:REV1&rid=1

[302] EU priorities at the United Nations during the 76th United Nations General Assembly, September 2021 - September 2022 - Council conclusions (12 July 2021). Brussels, 12 July 2021. URL: https://data.consilium.europa.eu/doc/document/ST-10393-2021-INIT/en/pdf

доступ правоохоронних органів до даних таким чином, що може криміналізувати свободу вираження поглядів і підірвати конфіденційність. Окремі уряди, передусім ті, що найбільше підтримують глобальний договір, часто використовують такий підхід для переслідування журналістів, правозахисників, опозиційних політиків, розцінюючи такі форми вільного вираження поглядів, як критика й інакомислення, як злочини. Тому договір про кіберзлочинність, який нормалізує цей підхід, потенційно суперечить зобов'язанням із прав людини.

Про підтримку Європейським Союзом Будапештської конвенції сказано в попередньому параграфі. Натомість США також активно працюють щодо її утвердження, вважаючи розширення міжнародної співпраці в цьому напрямі безальтернативним. Із цього приводу Держсекретар Керрі висловився в Корейському університеті (Сеул) 18 травня 2015 р. так: "Сполучені Штати співпрацюють із партнерами на кожному континенті для зміцнення спроможності урядів запобігати кіберзлочинності шляхом удосконалення навчання, відповідних правових рамок, обміну інформацією й залучення громадськості. Найкращий засіб для міжнародної співпраці в цій галузі — це Будапештська конвенція про кіберзлочинність, до якої мій уряд закликає кожну країну розглянути можливість приєднання. Не існує кращої правової бази для транскордонної роботи, щоб визначити, що таке кіберзлочинність і як слід запобігти порушенням закону й притягнути до кримінальної відповідальності[303]".

Ймовірним шляхом виходу з ситуації, що склалася у зв'язку із російськими ініціативами, яким може скористатися ЄС у разі актуалізації питання щодо прийняття Конвенції про протидію використанню інформаційно-комунікаційних технологій у злочинних цілях, може стати внесення у її преамбулу певного захисного застереження, яке б гарантувало не заперечення, а доповнення цим

[303] Cybercrime% Goals and Priorities. US Dept. of State. URL: https://2009-2017.state.gov/documents/organization/255007.pdf

документом вже існуючих міжнародних інструментів співробітництва, включаючи Будапештську конвенцію[304].

США підтримують Будапештську конвенцію в тому числі й фінансово. Внески в сотні тисяч доларів ця держава спрямувала на сприяння зусиллям Ради Європи в наданні порад щодо розробки законодавства країнам, що розвиваються, й підтримці збільшення участі країн, що розвиваються, в засіданнях конференції сторін[305]. Також лише в 2018 р. в рамках проєкту Cybercrime@Octopus на цю мету виділено 500 тис. дол[306].

У площині практичної співпраці в рамках Робочої групи ЄС і США з питань кібербезпеки й кіберзлочинності стали[307]: розширення можливостей реагування на інциденти спільно й у всьому світі за допомогою програм співпраці, спільних навчань між ЄС і США для протидії кібер-інцидентам; широке зобов'язання залучати приватний сектор, обмінюватися передовим досвідом співпраці з промисловістю й здійснювати конкретне залучення до таких ключових проблем, як боротьба з ботнетами, забезпечення систем промислового контролю (наприклад очищення води й виробництво електроенергії), а також підвищення стійкості й стабільність інтернету; реалізація програми негайних спільних заходів із підвищення обізнаності, обміну повідомленнями, а також дорожня карта щодо синхронних щорічних зусиль щодо інформування й конференція з питань захисту дітей в інтернеті; продовження співпраці ЄС і США щодо видалення дитячої порнографії з інтернету, в тому числі через роботу з реєстраторами доменних імен і реєстрами.

[304] Giovannelli D. (2021). Proposal of United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes : Comment on the first draft text of the Convention. *CCDCOE*. URL: https://ccdcoe.org/incyder-articles/proposal-of-united-nations-convention-on-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes-comment-on-the-first-draft-text-of-the-convention/

[305] The United States support efforts against Cybercrime. US Embassy & Consulates in France. 13 September, 2016. URL: https://fr.usembassy.gov/united-states-support-efforts-cybercrime/

[306] US support to the Budapest Convention. *Council of Europe*. Strasbourg, 25 September 2018. URL: https://www.coe.int/en/web/cybercrime/-/us-support-to-the-budapest-convention

[307] Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats. European Commission. MEMO/11/246 Brussels, 14th April 2011. URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_11_246

У рамках останніх пунктів співпраці, як реалізація одного з основоположних принципів західного підходу до кібербезпеки, — співпраця держав у розслідуванні та боротьбі з кіберзлочинністю. Сторони започаткували в 2012 р. "Глобальний альянс проти сексуального насильства над дітьми в інтернеті", який мав на меті посилити боротьбу цих країн проти сексуальної експлуатації дітей в інтернеті. Після об'єднання в 2016 р. із заснованим у 2013 р. американсько-британським альянсом WePROTECT, цей спільний проєкт став одним з найбільших у сфері координації зусиль щодо кібербезпеки й сьогодні об'єднує 98 країн, десятки компаній, громадських і міжнародних організацій[308].

Здійснюється координація між ЄС та США і в практичних напрямах координації мережі, зокрема між спеціалізованими інституціями. Обидві сторони поділяють спільні принципи та візії щодо управління інтернетом, такі як відкритість, свобода й сумісність, а також гарантії прав і свобод людини у сфері кібербезпеки. США і ЄС визнають єдино багатостороннє управління інтернетом, децентралізоване й демократичне в прийнятті рішень. Цей підхід передбачає політику "знизу вгору", в інтересах усіх зацікавлених сторін на рівних умовах.

Європейські політики високо оцінюють значення інституційної співпраці з американськими колегами щодо кібербезпеки, небезпідставно зважаючи на їх великий досвід і високі компетентності в цій сфері. Сесілія Мальмстрьом, у свій час єврокомісар, відповідальний за внутрішні справи ЄС, відзначала, що США і ЄС є головними мішенями для різних видів кіберзагроз: "Наші уряди, підприємства й громадяни опинилися в облозі все більш складних атак. Ці атаки можуть надходити з багатьох різних джерел — від інших держав до організованої злочинності й хакерів. Для подолання цієї зростаючої глобальної загрози співпраця ЄС і США — це не вибір, а необхідність. Створення Робочої групи ЄС — США з кібербезпеки й кіберзлочинності у листопаді 2010 року стало нашим першим кроком для визначення стратегічних цілей і конкретних дій[309]". У цій же промові єврокомісар

[308] The Alliance. URL: https://www.weprotect.org/alliance/

SPEECH/12/315 Cecilia Malmström. European Commissioner responsible for Home Affairs. The European Response to the rising Cyber Threat. *Transatlantic Cyber Conference organised by the Center for Strategic and*

відзначила високий рівень професіоналізму фахівців із кібербезпеки Федерального бюро розслідувань США, що ”підкріпило думку, що ми повинні продовжувати поглиблювати трансатлантичну співпрацю проти кіберзагроз[310]”.

Відомо багато прикладів успішної співпраці з багатьма зацікавленими сторонами між ЄС і США, включаючи перехідний орган Організації з адміністрування доменних імен верхнього рівня (IANA) та Європейського діалогу з питань управління інтернетом (EuroDIG)[311]. У цьому напрямі Робоча група ЄС — США з кібербезпеки й кіберзлочинності також доклала зусиль для координації між ЄС і США, зокрема в питанні укладення рекомендацій для правоохоронних органів щодо неправомірного використання доменних імен та IP-адрес в інтернеті в незаконних цілях[312].

За словами згаданої вище Сесілії Мальмстрьом, майже 50 % даних, наданих претендентами на п’ять найкращих загальних доменів верхнього рівня — .com (dot com), .org, .net, .info та .biz — містять докази фальшивої, неправдивої чи неповної інформації, що засвідчує особу. І ця проблема була розв’язана саме спільними зусиллями: “Після значного тиску з боку ЄС і США ми нарешті побачили зобов’язання Інтернет-корпорації з присвоєння імен та номерів (ICANN) і приватного сектора впроваджувати конкретні рекомендації правоохоронних органів у своїй політиці[313]“.

Ще одним результатом розвитку євро-атлантичної співпраці у сфері кібербезпеки став Кібер-діалог між ЄС і США, який розпочав роботу в грудні 2014 р. У порівняння з Робочою групою ЄС — США з кібербезпеки й кіберзлочинності його мета, окрім утилітарних аспектів протидії кіберзагрозам,

International Studies, the European Security Roundtable and SRA International. Washington, 2 May 2012. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_315

[310] Там само.

[311] Taylor Emily and Hoffmann Stacie (2019) EU–US Relations on Internet Governance. Chatham House. International Security Department. November 2019. URL: https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-14-EU-US-Relations-Internet-Governance2.pdf

[312] EU-US WORKING GROUP ON CYBER-SECURITY AND CYBER-CRIME - CONCEPT PAPER. 13 April 2011. URL: https://www.statewatch.org/media/documents/news/2011/apr/eu-us-2011-04-13-concept-paper-cybersecurity.pdf

[313] Там само.

більше орієнтована також на координацію зовнішньої політики сторін з кібер-питань і стратегічні аспекти глобальної кібербезпеки. Серед сфер інтересів — розбудова кіберпотенціалу, управління інтернетом, заохочення й захист прав людини в інтернеті, боротьба з кіберзлочинністю, кіберстійкість, трансатлантичне співробітництво в галузі кіберполітики, розвиток міжнародного кіберпростору, пропаганда й захисті прав людини в інтернеті, нарощування потенціалу кібербезпеки в третіх країнах. Безпекові питання в полі інтересів Кібер-діалогу поширюються на встановлення норм поведінки й заходів щодо зміцнення довіри в кіберпросторі й застосування існуючих норм міжнародного права в кіберпросторі[314].

Зокрема в напрямі розвитку кібер-стійкості сторони розробили Директиву ЄС 2016/1148 про безпеку мережевих та інформаційних систем, ухвалену в 2016 р[315]., яка впроваджується в усіх державах — членах, а також організували проведення навчань CyberEurope. Вони також обговорили другу ітерацію Стандартів рамок кібербезпеки на добровільній основі, включаючи постійне залучення зацікавлених сторін. За їх участі підготовлено Національний план реагування на кібер-інциденти США[316].

Важливою характеристичною ознакою американсько-європейського підходу до безпеки кіберпростору є активне залучення до управління ним приватного сектора, науки й громадянського суспільства. У цьому напрямі Європейський Союз і США започаткували Трансатлантичну ініціативу з дослідження кіберполітики, що об’єднує академічні, промислові й експертні центри для вирішення ключових проблем кіберполітики й збільшення потенціалу досліджень у сфері кібер-питань.

[314] EU-U.S. Cyber Dialogue Bruxelles, 16/12/2016 - 23:00 - UNIQUE ID: 161223_8. URL: https://www.statewatch.org/media/documents/news/2016/dec/eu-eeas-eu-us-cyber-dialogue-pr-16-12-16.pdf

[315] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[316] EU-U.S. Cyber Dialogue Bruxelles, 16/12/2016 - 23:00 - UNIQUE ID: 161223_8. URL: https://www.statewatch.org/media/documents/news/2016/dec/eu-eeas-eu-us-cyber-dialogue-pr-16-12-16.pdf

На практиці Робоча група ЄС — США з кібербезпеки й кіберзлочинності й Кібер-діалог ЄС — США стали двома ключовими інституціями для обговорення політики й потенційної координації дій у сфері кібербезпеки. Але потрібно відмітити, що взаємодія ЄС і США в цьому аспекті здійснюється не через розвиток систематичних і стійких відносин у визначених цими (або іншими) інституціями рамках, а відповідно до принципу багатосторонньої координації, шляхом добровільного прийняття й наслідування практики один одного. Наприклад Агентство ЄС з інформаційної безпеки й безпеки мереж (ENISA) для відображення взаємозалежностей операторів основних послуг і постачальників цифрових послуг враховує найбільш актуальні й поширені стандарти у сфері управління ризиками, в тому числі міжнароднний ISO/IEC 27002 й американську рамку NIST Cybersecurity Framework. Ця рамка оцінки ризиків і аудиту охоплює різні сфери ризиків і надає конкретні вказівки для планування й реалізації детальної стратегії на основі ризиків у організаціях[317].

Також у ЄС підтримано реалізовану значно раніше в США модель центрів аналізу та обміну інформацією (ISAC), — некомерційних організацій, які надають ресурси для збору інформації про кіберзагрози (в багатьох випадках для критичної інфраструктури), а також здійснюють двосторонній обмін інформацією між приватним і державним сектором про кібер-інциденти й загрози, обмінюються досвідом, знаннями й результатами аналізу. Європейські законодавчі акти, такі як Директива NIS і Закон про кібербезпеку, підтримують розвиток публічно-приватного партнерства й створення галузевих ISAC у межах ЄС. У США галузеві центри обміну й аналізу інформації співпрацюють між собою через Національну раду ISAC (NCI), створену ще в 2003 р., і яка сьогодні об’єднує 25 організацій[318].

[317] Good practices on interdependencies between OES and DSPs. ENISA. NOVEMBER 2018. URL: https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps/view/++widget++form.widgets.fullReport/@@download/WP2018+O.2.2.2+Good+practices+on+interdependencies+between+OES+and+DSPs.pdf

[318] National Council of ISACs. URL: https://www.nationalisacs.org/

Ураховуючи лідерські позиції Америки у сфері ІКТ, ЄС переймає досвід у США, що здійснюється як через інструменти спільної координації, згадані вище, так і отримується безпосередньо з американських інституцій, які зазвичай відкрито публікують і просувають свої підходи й стандарти, а також шляхом взаємодії європейських чиновників і представників американських компаній, які взаємодіють між собою й обмінюються ідеями під час різноманітних форумів. Використовують досвід американської сторони також європейські інституції. Наприклад Європол здійснює успішні операції з протидії кіберзлочинності, у тісній співпраці з інституціями європейських держав і США.

Так, у 2014 р., правоохоронні органи низки країн, за підтримки Європейського центру з кіберзлочинності при Європолі, об'єднали зусилля в скоординованій дії під керівництвом ФБР, яка забезпечила зрив ботнета Gameover Zeus, у реалізації якого влада США підозрює мешканця Росії[319]. У листопаді 2017 р. Федеральне бюро розслідувань у тісній співпраці з Люнебурзькою центральною інспекцією з розслідування кримінальних справ у Німеччині, Європейським центром із питань кіберзлочинності Європолу, Спільною робочою групою з боротьби з кіберзлочинністю (J-CAT), Євроюстом і партнерами з приватного сектора демонтували сімейство шкідливих програм під назвою Andromeda. Статистичні дані, отримані під час розслідування в цій справі правоохоронними органами Німеччини, були передані через Європол до ФБР[320]. Улітку 2021 р. правоохоронні й судові органи з Європи, США й Канади, зокрема Національна поліція Нідерландів у координації з Європолом і Євроюстом, нейтралізували веб-домени й інфраструктуру серверів DoubleVPN, яка надавала притулок кіберзлочинцям для нападу на їхніх жертв. Зі сторони США участь брали Федеральне бюро розслідувань, Секретна служба США (USSS), Міністерство юстиції США. Ця скоординована ліквідація була здійснена в

[319] International action against 'gameover zeus' botnet and 'cryptolocker' ransomware. EUROPOL. Press Release. 02 June 2014. URL: https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[320] Andromeda botnet dismantled in international cyber operation. *EUROPOL*. Press Release. 04 December 2017. URL: https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation

рамках Європейської багатопрофільної платформи проти кримінальних загроз (EMPACT)[321]. Загалом на веб-сайті Європолу повідомляється про десятки подібних прикладів успішної, спільної з американскою стороною, боротьби з кіберзлочинністю, а в його структурі задіяно близько тридцяти фахівців, які репрезентують різні офіційні служби США[322].

Звісно, щодо певних питань безпеки кіберпростору ЄС і США мають різні погляди. Зокрема це стосується захисту персональних даних, де з упровадженням ЄС у 2018 р. Загального регламенту захисту даних (GDPR), розпочато масштабну перебудову в системі відносин між суб'єктами кіберпростору задля забезпечення кращої конфіденційності даних користувачів інтернету. По-перше, американські компанії висловлювали з цього приводу невдоволення через необхідність додаткових витрат для відповідності вимогам GDPR, а по-друге, адміністрація США стверджувала, що норми GDPR перешкоджають обміну необхідними даними для медичних досліджень, кримінальних розслідувань і протидії тероризму[323].

Після упровадження GDPR відбулося декілька подій, які зумовили необхідність розв'язання певних проблем на шляху співпраці сторін у сфері безпеки кіберпростору. Так, Суд ЄС визнав недійсними правовий механізм для забезпечення взаємного транскордонного потоку даних між ЄС і США, чинний з початку 2000 рр., на підставі якого діяли близько 4000 компаній, зокрема й Фейсбук, які використовували його для передачі даних через Атлантику[324]. Окрім того цей суд, у відповідь на звернення Верховного суду Ірландії, розглядав позов австрійського юриста Макса Шремса проти європейського відділення "Фейсбуку" про ймовірне порушення компанією законодавства Союзу й визнав недійсним

[321] Coordinated action cuts off access to vpn service used by ransomware groups. *EUROPOL*. Press Release. 30 June 2021. URL: https://www.europol.europa.eu/newsroom/news/coordinated-action-cuts-access-to-vpn-service-used-ransomware-groups

[322] Statistics & data. Europol staff numbers. URL: https://www.europol.europa.eu/about-europol/statistics-data

[323] EU Data Protection Rules and U.S. Implications. Congressional Research Service. July 17, 2020. URL: https://sgp.fas.org/crs/row/IF10896.pdf

[324] Vittorio Andrea (2021) Surveillance in Spotlight Amid Ongoing EU-U.S. Data Privacy Rift. *Bloomberg Law.* July 16, 2021. URL: https://news.bloomberglaw.com/privacy-and-data-security/surveillance-in-spotlight-amid-ongoing-eu-u-s-data-privacy-rift

механізм під назвою EU-US Privacy Shield (Щит конфіденційності між ЄС і США), який передбачав належний захист при переданні персональних даних із країн ЄС до США. Підставою такого рішення стало встановлення конфлікту між законодавствами США і ЄС, — перше дозволяє спецслужбам здійснювати збір даних на території країни, а другі, згідно з GDPR, вимагають їх захищати[325].

Загалом США і ЄС дотримуються подібних підходів щодо інформаційної (кібер) безпеки. І це зумовлено не лише подібністю їх демократичних систем, але й прагматичними міркуваннями. Адже економіки обох сторін тісно взаємопов'язані, що з одного боку стимулює співпрацю, а з іншого створює умови для розбіжностей у поглядах на чутливі в аспекті конкуренції сфери. Загальна концепція інформаційної (кібер) безпеки в обох сторін однакова, а їх взаємодія на міжнародному рівні формується на фоні протистояння з Росією й Китаєм із питань, пов'язаних із управлінням інтернетом і правами людини в інтернеті. У контексті конкуренції за встановлення глобальних стандартів ЄС і США протистоять зусиллям Росії й Китаю в їх намаганні контролювати й цензурувати вміст інтернету й підривати нинішню модель управління інтернетом (включно з іншими зацікавленими сторонами замінюючи її на міжурядові й державно-центричні структури). Очевидно, що спільні інтереси сприятимуть розвитку співпраці США та ЄС, зміцненню й поширенню західної концепції інформаційної (кібер) безпеки.

3.4. Взаємодія ЄС із іншими країнами

Важливо, що переслідуючи власні цілі, ЄС бере активну участь у поширенні західної концепції розвитку кіберпростору. Але при цьому розробляються й просуваються власні позиції з актуальних для міжнародної взаємодії питань. Це стосується, наприклад, позиції ЄС щодо кібер-стримування, яка ще виробляється й, відповідно до стратегії кібербезпеки 2020 р., "має сприяти відповідальній

[325] Bodoni Stephanie (2020). EU Court Blocks Data Pact Amid Fears Over U.S. Surveillance (4). *Bloomberg Law.* July 16, 2020. URL: https://news.bloomberglaw.com/privacy-and-data-security/eu-court-bans-privacy-shield-data-transfer-pact

поведінці держави й співробітництву в кіберпросторі, а також давати особливі вказівки щодо протидії тим кібератакам, які мають найбільш значний ефект, особливо тим, що впливають на нашу критичну інфраструктуру, демократичні інститути й процеси[326]". Окрім того розглядаються можливості подальших варіантів обмежувальних заходів у рамках набору інструментів у сфері кібер-дипломатії, й режим горизонтальних санкцій проти кібератак.

У стратегії ЄС надалі зміцнить свій набір інструментів ЄС із кібернетичної дипломатії (сукупність дипломатичних практик, що стосуються широко визначеного управління кіберпростором) для забезпечення її функціонування на регулярній основі, подальшого інтегрування інструментарію кібер-дипломатії в кризові механізми ЄС, забезпечення синергії в зусиллях щодо протидії гібридним загрозам, дезінформації й зовнішнього втручання в рамках Спільної рамки протидії гібридним загрозам[327].

Зовнішній вимір нової стратегії кібербезпеки ЄС заснований на традиційно прагматичному підході, що полягає в продовженні співпраці з міжнародними партнерами для просування політичної моделі й свого бачення кіберпростору як заснованого на верховенстві права, правах людини, основних свободах і демократичних цінностях задля соціального, економічного й політичного розвитку. Одним із пріоритетів визначено активізацію діяльності у сфері міжнародних стандартизаційних процесів і лідерство в них. Це пояснюється технологічними й економічними перевагами тих, хто отримує пріоритет у розробці й затвердженні таких стандартів, а також тим, що міжнародна стандартизація все частіше використовується третіми країнами для просування своєї політичної й ідеологічної програми, зокрема спираючись на розробки в таких сферах, як штучний інтелект, хмарні й квантові обчислення й квантова комунікація, що часто не відповідає цінностям ЄС. Наприклад перспективні

[326] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Brussels, 16.12.2020 JOIN(2020) 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

[327] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Joint Framework on countering hybrid threats. European Commission. Brussels, 6.4.2016 JOIN(2016) 18 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

технологічні розробки Китаю в зазначених сферах застосовуються для обмеження свободи слова, громадянських і політичних прав[328].

Стратегія кібербезпеки ЄС передбачає створення Порядку денного розбудови зовнішнього кібер-потенціалу ЄС. Відповідно до прийнятих у 2018 р. керівних напрямів[329] для розробки цього Порядку денного, ”створення кібер-потенціалу стає однією з найважливіших тем у порядку денному міжнародної кібер-політики”. А розбудова кібер-потенціалу третіх країн за участі ЄС передбачає: ”систематичні зусилля з партнерами країн і відповідних організацій для покращення національних, інституційних і організаційних можливостей, які покращують стійкість критичних цифрових послуг і мереж, а також захист критичної інформаційної інфраструктури; підтримку реформ кримінального правосуддя у сфері кіберзлочинності; боротьбу з використанням інтернету з терористичною метою; вдосконалення навичок і компетенцій кібербезпеки; сприяння підвищенню обізнаності й ефективній співпраці з цих питань на національному, регіональному й міжнародному рівнях [330] ”. Також передбачається посиленням цивільних аспектів Спільної політики безпеки й оборони шляхом включення в неї заходів з кібербезпеки з акцентом на зміцнення стійкості й можливості третіх країн.

На відміну від Китаю ЄС орієнтується на підтримку країн не за їх прихильністю до певного курсу (як-от “Пояс і шлях”), а чітко визначає серед пріоритетних, щодо яких буде здійснено підтримку ЄС у справі розбудови кібернетичного потенціалу, країни-сусіди й загалом країни, що розвиваються.

Для практичної реалізації своїх цілей у сфері розвитку зовнішнього кібер-потенціалу ЄС утворює мережу EU CyberNet[331], яка має посилити глобальну реалізацію, координацію й узгодження проєктів Європейського Союзу щодо

[328] Вейкфілд Джейн (2021). "Китай використовує уйгурів як піддослідних щурів". Що відомо про камери розпізнавання емоцій. *BBC News Україна*. 27 травня 2021. URL: https://www.bbc.com/ukrainian/news-57265671

[329] EU External Cyber Capacity Building Guidelines. Council of the European Union. Brussels, 26 June 2018. URL: https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf

[330] Там само.

[331] EU CyberNet – the bridge to cybersecurity expertise in the European Union. URL: https://www.eucybernet.eu/

створення кібер-потенціалу й можливості Європейського Союзу надавати технічну допомогу третім країнам у сфері кібербезпеки й кіберзлочинності. Необхідність такої мережі стала актуальною після безпрецедентних за масштабами глобальних атак зловмисного програмного забезпечення навесні 2017 р. (через віруси WannaCry і New Petya, NotPetya або ExPetr, які встигли заразити сотні тисяч комп'ютерів у більшості країн світу, через що зупинилася робота банків, урядових організацій, аеропортів і завдано шкоди на понад 10 млрд дол.[332]), коли у комюніке "Стійкість, стримування, оборона: створення міцної кібербезпеки для ЄС" Європейська комісія закликала створити мережу ЄС із розбудови кіберпотенціалу, яка підтримуватиме поточні й майбутні зусилля ЄС у сфері кібернетичного потенціалу в третіх країнах: "Розробити нову мережу з розбудови потенціалу для підтримки спроможності третіх країн боротися з кіберзагрозами"[333]. Запущена в 2019 р., EU CyberNet мала намір досягти чотирьох основних результатів за чотири роки: створення мережі експертів і зацікавлених сторін у сфері кібербезпеки, розробка технічної платформи, забезпечення навчання й допомоги й перетворення на центр знань про зовнішні відносини ЄС у сфері кібербезпеки.

Пріоритетними для ЄС у цьому аспекті є країни Західних Балкан, країни сусідства, а також країни-партнери, які демонструють швидкий цифровий розвиток. Зокрема в рамках EU CyberNet розпочато діяльність щодо розбудови потенціалу на африканському континенті й у Латинській Америці для розробки законодавства й політики країн-партнерів у взаємозв'язку з відповідною політикою й стандартами ЄС у сфері кібернетичної дипломатії. Наприклад у 2021 р. в Домініканській Республіці проведено перші національні навчання з кібербезпеки "Кібер-полум'я" й проведено роботу зі створення майбутнього

[332] What can we learn from the "most devastating" cyberattack in history? *CBC News*. August 22, 2018. URL: https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/

[333] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission. Brussels, 13.9.2017 JOIN(2017) 450 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

центру кіберкомпетентності для країн Латинської Америки й Карибського басейну[334].

Важливого значення ЄС надає співпраці з питань безпеки кіберпростору і з регіональними організаціями, такими як Африканський союз, Регіональний форум АСЕАН, Організація американських держав та ОБСЄ, а також з іншими партнерами — із питань, що становлять спільний інтерес. Поставлено мету — за участі представництв ЄС, а також посольств держав — членів у всьому світі, створити неформальну мережу ЄС із кібернетичної дипломатії для популяризації європейського бачення кіберпростору, обміну інформацією й координації щодо подій у кіберпросторі.

Можна помітити, що серед цільових партнерів ЄС є й ті, що знаходяться в полі стратегічних інтересів Китаю в рамках його стратегії кібербезпеки. Крім того ЄС демонструє загалом подібний до китайського підхід у напрямі третіх країн, збільшуючи зусилля щодо розвитку їх кібер-потенціалу. Звісно, ця співпраця розвиватиметься в рамках унійних програм і не матиме наслідком жодної економічної чи політичної залежності.

І основним у стратегії міжнародної співпраці ЄС із питань безпеки кіберпростору є те, що відповідно до своїх цінностей унія рішуче підтримує й пропагує модель управління інтернетом із багатьма зацікавленими сторонами: “Жодна окрема організація, уряд чи міжнародна організація не повинні прагнути контролювати інтернет”[335].

Особливу вагу для ЄС має співпраця в питаннях безпеки з НАТО, організації, яка об’єднує більшість країн — членів унії. У цьому напрямі в липні 2016 р. у Варшаві підписано Спільну декларацію[336] з метою надати нового

[334] EU CyberNet work in Dominican Republic, first national cybersecurity exercise “Cyber llamas”. *EU CyberNet*. 21.05.2021. URL: https://www.eucybernet.eu/eu-cybernet-work-in-dominican-republic-first-national-cyber-llamas-exercise/

[335] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Brussels, 16.12.2020 JOIN(2020) 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

[336] JOINT DECLARATION BY THE PRESIDENT OF THE EUROPEAN COUNCIL, THE PRESIDENT OF THE EUROPEAN COMMISSION, AND THE SECRETARY GENERAL OF THE NORTH ATLANTIC TREATY ORGANIZATION. URL: https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

імпульсу й нової сутності стратегічному партнерству ЄС — НАТО, зокрема й у сферах протидії гібридним загрозам, кібербезпеки й оборони. На основі мандату Спільної декларації Європейський Союз і НАТО створили спільний набір пропозицій щодо її імплементації, який був схвалений Радами ЄС і НАТО в грудні 2016 р.

У сфері кібербезпеки й оборони оголошено про розширення координації, включаючи контекст місій і операцій, навчань і освіти, а також щодо сумісності в сфері кіберзахисту. Також серед напрямів співпраці — підвищення здатності протидіяти гібридним загрозам, у тому числі шляхом посилення стійкості, спільної роботи над аналізом, запобіганням і раннім виявленням шляхом своєчасного обміну інформацією, співпраця в сфері стратегічної комунікації й реагування.

Окремо відмітимо роботу ЄС щодо розвитку напряму кібероборони в царині спільної політики безпеки й оборони (CSDP). У 2014 р. прийнято рамки політики ЄС щодо кібероборони (CDPF), оновлені в 2018 р[337]. Документ містить основи для протидії кіберзагрозам і визначає аспекти кіберзахисту Стратегії ЄС з кібербезпеки, роз'яснює ролі різних європейських суб'єктів і визначає пріоритетні напрями кіберзахисту CSDP, зокрема сприяння цивільно-військовому узгодженню з кіберполітикою ЄС, установами ЄС і приватним сектором і з відповідними міжнародними партнерами, зокрема НАТО. У CDPF кіберпростір визначено областю операцій CSDP, а також наголошено на необхідності забезпечення кібербезпеки критично важливих космічних інфраструктур, що належать до компетенції відповідних програм і відомств.

У Кіберстратегії 2020 р. відмічено необхідність перегляду Рамкової політики у сфері кібероборони (CDPF) для того, щоб “кібербезпека й кіберзахист ще більше інтегрувалися в ширшу програму безпеки й оборони[338]”. Важливим

[337] EU Cyber Defence Policy Framework (2018 update). Council of the European Union. Brussels, 19 November 2018. URL: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

[338] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Brussels, 16.12.2020 JOIN(2020) 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

стратегічним напрямом є покращення співпраці між державами — членами щодо виявлення й реагування на кібер-інциденти, зокрема за допомогою відповідних осередків мережі Military CERT-Network.

Перспективним інструментом для розвитку співпраці між державами — членами з питань кіберзахисту є PESCO, програма Постійного структурованого співробітництва держав — членів ЄС, спрямована на тіснішу співпрацю у сфері безпеки й оборони, в рамках Глобальної стратегії ЄС із зовнішньої політики й політики безпеки. Серед перших сімнадцяти ключових напрямів співпраці, внесених до Декларації про проєкти в рамках PESCO, є створення бази обміну інформацією у відповідь на кібернетичні атаки й загрози й надання взаємодопомоги для забезпечення кібернетичної безпеки й створення кібер-групи швидкого реагування[339]. Інструментом для фінансування потенційних спільних досліджень і розробок у сфері кіберзахисту, спрямованих на зміцнення співробітництва, інноваційного потенціалу й конкурентоспроможності оборонної промисловості є Європейський оборонний фонд (EDF).

[339] Declaration on PESCO projects (2018) Declaration on PESCO projects (bijlage bij 21501-02,nr.1813). URL: https://www.consilium.europa.eu/media/32020/draft-pesco-declaration-clean-10122017.pdf.

ВИСНОВКИ

Сьогодні у сфері міжнародного співробітництва щодо забезпечення інформаційної (кібер) безпеки сформовано два принципово відмінні підходи. Один з них характерний для США, їх партнерів по НАТО й інших провідних держав Заходу, зокрема ЄС. Інший відстоюють Росія, Китай і низка інших країн з відносно менш розвиненою демократією. Послідовники цих підходів по-різному трактують поняття “інформаційна безпека”. Якщо США виступають виключно за технічне регулювання кіберсередовища (захист комп'ютерних мереж і ресурсів) і використовують поняття “кібербезпека”, а не “інформаційна безпека”, то Росія включає в це поняття як технічне забезпечення кібербезпеки систем і мереж, так і політико-ідеологічні аспекти — протидію пропаганді й недопущення інформаційного впливу. Підхід держав Заходу базується на безпечному зв'язку, — інформація безпечна, доки безпечна технологічна інфраструктура, а відповідальність уряду полягає в тому, щоб кожен громадянин міг вільно користуватися безпечними технологіями. Певною мірою російсько-китайський підхід до політики інформаційної безпеки протилежний американському та європейському, орієнтованому на кібербезпеку. Основна відмінність полягає в тому, що уряд (держава) забезпечує безпеку не тільки інфраструктури, але й самої інформації, декларуючи її невід’ємним складником національного суверенітету.

Відмінні позиції в підходах і щодо основних загроз у кіберпросторі. Помітна відмінність у російському підході порівняно зі сприйняттям кібертероризму в демократичних країнах. Якщо на Заході трактують кібертероризм як загрозу інформаційним системам, передусім пов’язаним із критичною інфраструктурою, то в Росії кібертероризм розглядають у числі комплексних загроз особі, суспільству й державі. Такого підходу притримується й китайська влада.

Суттєво відрізняються підходи до розуміння інформаційних упливів із точки зору військово-політичної стратегії. Російська концепція полягає в застосуванні інтегрального впливу всієї державної “машини” включно з силовими структурами й підконтрольним медіа-сектором (концепція “інформаційних війн”). Натомість американський і загалом євроатлантичний підхід полягає в розділенні військових

і цивільних інформаційних упливів (де цивільні як такі, по суті, й не розглядаються в аспекті медійного дискурсу), але у взаємозв'язку з реалізацією стратегічних інтересів уряду. Така модель відповідає реаліям суспільних комунікацій, де держава не втручається в медійну сферу, яка саморегулюється зусиллями незалежних учасників медіаринку. У військових доктринах на переломі XX — XXI ст. використовувалось поняття "інформаційного протиборства" з виокремленням "інформаційних операцій наступального й оборонного характеру. Проте з середини 2000-х рр. його місце заступила концепція "стратегічних комунікацій" у складі компонентів — інформаційних операцій, інформаційно-психологічних операцій, публічної дипломатії, військової й цивільної комунікації.

Суттєвою проблемою в аспекті міжнародного співробітництва є різні підходи до розуміння ролі міжнародного права в аспекті інформаційної (кібер) безпеки (безпеки кіберпростору). По-перше, право jus ad bellum (сфера Статуту ООН) розглядається Росією та її однодумцями в позитивістському ключі, тобто вони наполягають на обмеженні застосування сили державами, а США й інші країни Заходу виступають за більш широкі можливості застосування сили. Це пов'язано, головним чином, із відчутним відставанням перших в інформаційно-технологічному плані. По-друге, у сфері міжнародного гуманітарного права (jus in bello) Росія, Китай, їх союзники по ШОС і низка інших держав (які переважно не характеризуються високим рівнем демократії) виступають за формування в міжнародному праві окремого домена "інформаційної безпеки", створення спеціальних обов'язкових "правил поведінки" держав і просувають російську концепцію "міжнародної інформаційної безпеки" — правового режиму й формату співробітництва в цій сфері. Держави Заходу наполягають на застосовності до сфери кіберпростору діючих норм міжнародного права, спільного реагування на виникаючі кібер-загрози й добровільних і необов'язових нормах поведінки держав у кіберпросторі. Натомість у випадку військових конфліктів, нападів, у всіх передбачених нормами міжнародного гуманітарного права випадках, цілком

можуть застосовуватися діючі норми, що відображено в “Талліннському посібнику” (Tallinn Manual), розробленому в контексті діяльності НАТО.

Сьогодні найбільш активно проявляють себе чотири міжнародні актори у сфері інформаційної (кібер) безпеки — Росія, США, Китай, ЄС. Росія активно й послідовно просуває на рівні ООН і регіональних міжнародних організацій свою концепцію “міжнародної інформаційної безпеки”, з кінця 1990-х рр. пропонуючи порядок денний, суть якого опрацьовується в контексті запропонованих нею проєктів резолюцій ГА ООН “Досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки”. На рівень ООН висунуто проєкти “правил поведінки” держав у кіберпросторі й конвенції про кіберзлочинність. В основі російських пропозицій лежить лідируюча й керівна роль держави в усіх аспектах і процесах інформатизації й телекомунікацій, у тому числі управлінні інтернетом та “інформаційному суверенітеті”. Головним треком розвитку співпраці на рівні ООН за ініціативами Росії є Робоча група відкритого складу. На двох останніх позиціях наполягає також Китай, загалом підтримуючи всі російські ініціативи. Китай також розширює сферу впливу щодо безпеки кіберпростору, розвиваючи співробітництво з державами, що становлять для нього стратегічний інтерес і пропонуючи світові авторитарну модель управління інтернетом (“Уженьські ініціативи”). Головним майданчиком для опрацювання спільних позицій Росії й Китаю в цьому аспекті є ШОС.

Сполучені Штати відстоюють свою концепцію ліберального підходу до розвитку кіберпростору й багатостороннього управління інтернетом, необов’язкових норм поведінки держав у кіберпросторі (проєкт резолюції ГА ООН “Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки”, 2018 р.). США наполягають на доцільності використання результатів, досягнутих у рамках Групи урядових експертів (2010, 2013 і 2015 рр.), запропонувавши однойменний трек у згаданій вище резолюції. Також США активно пропагують розвиток міжнародної співпраці в протидії кіберзлочинності у форматі, визначеному “Будапештською конвенцією”.

Відмінність у підходах до політики кібербезпеки світових лідерів у сфері ІКТ — Китаю та США — ґрунтується на принципово різному розумінні проблеми управління кіберпростором. Обидва актори виступають за упровадження правил кібер-управління всередині країни й міжнародну співпрацю в цій сфері, але Китай зі своєю ідеєю "кіберсуверенітету" відстоює право кожної держави на участь в управлінні інтернетом і оголошує протидію американській "кібергегемонії". Ця концепція відкидається Сполученими Штатами, які розглядають китайський підхід як такий, що не відповідає демократичним принципам свободи слова й права на інформацію. Із погляду США китайська модель інформаційної (кібер) безпеки орієнтована на встановлення цензури в Китаї й неконкурентне обмеження доступу до китайського ринку для американських ІТ-компаній.

США проводять активну роботу щодо утвердження в глобальному масштабі своєї моделі інформаційної (кібер) безпеки передусім на рівні Організації Об'єднаних Націй, конкуруючи в цьому контексті з Росією. США беруть активну участь в роботі Груп урядових експертів ООН і запропонували власний проєкт резолюції щодо відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки.

Китай проводить активну міжнародну роботу поки що на рівні регіональних організацій і серед своїх партнерів, постійно розширюючи їх коло. Протягом 2015—2020 рр. КНР чітко систематизувала свою міжнародну політику в сфері кібербезпеки, прийнявши міжнародну стратегію для кіберпростору й активізувавши діяльність у відповідному напрямі в колі країн, що розвиваються. Також Китай підтримує ініціативи Росії.

Європейський Союз загалом підтримував ініціативи США у сфері кібербезпеки, реалізував власні проєкти щодо кібербезпеки й розвивав міжнародну співпрацю з партнерами переважно у формі "кібердипломатії", проте починаючи з 2020 р. почав проявляти значну активність у цій сфері, прийнявши відповідну стратегію й ініціювавши принципово новий формат взаємодії зацікавлених сторін на рівні ООН — ініціативу щодо реалізації Програми дій з відповідальної поведінки держав у кіберпросторі.

ДЖЕРЕЛА

1. 29 家网站签署《跟帖评论自律管理承诺书》. 2014 年 11 月 06 日 22:36 新华网 (29 Jiā wǎngzhàn qiānshǔ “gēn tiē pínglùn zìlǜ guǎnlǐ chéngnuò shū”. 2014 Nián 11 yuè 06 rì 22:36 Xīnhuá wǎng) [29 веб-сайтів підписали "Зобов'язання щодо самодисциплінованого менеджменту публікації коментарів". Сіньхуа, 06 листопада 2014]. URL: http://news.sina.com.cn/c/2014-11-06/223631106669.shtml
2. @IDF. URL: https://twitter.com/IDF/status/1125066395010699264
3. @SecBlinken [Secretary Antony Blinken]. United States government official. 19 Ju;y 2021. URL: https://twitter.com/secblinken/status/141710360213347942
4. 2006–2020 年国家信息化发展战略 (2006-2020 Nián guójiā xìnxī huà fāzhǎn zhànlüè) [Державна стратегія із розвитку інформатизації на період з 2006 до 2020 р.]. 08.05.2005. URL: https://baike.baidu.com/item/2006-2020%20%E5%B9%B4%E5%9B%BD%E5%AE%B6%E4%BF%A1%E6%81%AF%E5%8C%96%E5%8F%91%E5%B1%95%E6%88%98%E7%95%A5/16956741?fr=aladdin.
5. 2007 cyber attacks on Estonia. STRATCOMCOE. URL: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf
6. 73/187. Countering the use of information and communications technologies for criminal purposes. UN General Assembly. 14 January 2019. URL: https://undocs.org/en/A/RES/73/187
7. 73/266. Advancing responsible State behaviour in cyberspace in the context of international security. Resolution adopted by the General Assembly on 22 December 2018. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266
8. 73/27. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27&Lang=R
9. 74/247. Противодействие использованию информационнокоммуникационных технологий в преступных целях. Резолюция, принятая Генеральной Ассамблеей 27 декабря 2019 года. URL: https://undocs.org/ru/A/RES/74/247
10. A BILL To address issues involving the People’s Republic of China (”Strategic Competition Act of 2021”). 117TH CONGRESS 1ST SESSION. URL: https://www.foreign.senate.gov/imo/media/doc/DAV21598%20-%20Strategic%20Competition%20Act%20of%202021.pdf
11. A Bill to amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes. URL: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text
12. Andromeda botnet dismantled in international cyber operation. EUROPOL. Press Release. 04 December 2017. URL: https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation
13. Annual Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence. April 9, 2021. URL: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf
14. Aruna Viswanatha, Del Quentin Wilber (2 November 2017). U.S. Prosecutors Consider Charging Russian Officials in DNC Hacking Case. The *Wall Street Journal*. URL: https://www.wsj.com/articles/prosecutors-consider-bringing-charges-in-dnc-hacking-case-1509618203

15. Balzacq T., Cavelty M. D. (2016). A theory of actor-network for cyber-security, *European Journal of International Security*. №. 2. P. 176–198.
16. Basu Arindrajit, Hickok Elonnai and Chawla Aditya Singh (26 March 2019). Unpacking Policy Moves For Sovereign Control Of Data In India. *Cyberbricks*. URL: https://cyberbrics.info/unpacking-policy-moves-for-sovereign-control-of-data-in-india/
17. Biden Says Russia Has 'Some Responsibility' In Pipeline Ransomware Attack (10 May 2021). *Radio Free Europe*. Archived from the original on May 12, 2021.URL: https://web.archive.org/web/20210512233023/https:/www.rferl.org/a/fbi-confirms-darkside-hacker-group-pipeline-cyberattack-russia/31248174.html
18. Blake Andrew (24 September 2016). Ardit Ferizi, hacker who aided Islamic State, sentenced for helping terror group with 'kill list'. *The Washington Times*. Sept. URL: https://www.washingtontimes.com/news/2016/sep/24/ardit-ferizi-hacker-who-aided-islamic-state-senten/
19. Bodoni Stephanie (2020). EU Court Blocks Data Pact Amid Fears Over U.S. Surveillance (4). *Bloomberg Law*. July 16, 2020. URL: https://news.bloomberglaw.com/privacy-and-data-security/eu-court-bans-privacy-shield-data-transfer-pact
20. Brasília Declaration 11th BRICS Summit. 14 November 2019 in Brasília, Brazil. URL: http://brics2019.itamaraty.gov.br/images/documentos/Braslia_Declaration_-_hiperlinks_como_est_no_site_28-11.pdf
21. BRICS Leaders Xiamen Declaration. Xiamen, China. 9.04.2017. URL: https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/BRICS+Leaders+Xiamen+Declaration+9-4-17.pdf
22. Broad William J., Markoff John, Sanger David E. (15 January 2011). Israel Tests on Worm Called Crucial in Iran Nuclear Delay. *New York Times*. URL: https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&ref=general&src=me&pagewanted=all
23. Brown G., Yung C. D. (2017). Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace. *The Diplomat.* URL: https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/
24. Brown G., Yung C. D. (2017). Evaluating the US-China Cybersecurity Agreement, Part 3: Over a year later, what impact has the 2015 cyber agreement had on U.S.-China relations? *The Diplomat*. URL: https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/
25. Bucharest-based Cybersecurity Competence Centre gets green light from Council. *European Council.* 20 April 2021. URL: https://www.consilium.europa.eu/en/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/
26. Cadell Cate (4 November 2021). China launches hotline for netizens to report 'illegal' history comments. *Reuters.* URL: https://www.reuters.com/world/china/china-launches-hotline-netizens-report-illegal-history-comments-2021-04-11/
27. Centre of Excellence Defence Against Terrorism, ed. (2008). *Responses to Cyber Terrorism*. NATO science for peace and security series. Sub-series E: Human and societal dynamics, ISSN 1874-6276. 34. Amsterdam: IOS Press. p. 119.
28. Charlie Savage (July 26, 2016). Assange, Avowed Foe of Clinton, Timed Email Release for Democratic Convention. *New York Times*. URL: https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html?_r=0
29. Chen Abby (14 July 2021). A Close Reading of China's Data Security Law, in Effect Sept. 1, 2021. *China Briefing*. URL: https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021/

30. Chen Qingqing, Xu Keyue and Xu Yelu (June 6, 2021). US Turning G7 Into Anti-China, Anti-Russia Chorus 'Wishful Thinking. *Global Times*. URL: https://www.globaltimes.cn/page/202106/1225524.shtml
31. China Delivers Midnight Internet Declaration — Offline (21 November 2014). *The Wall Street Journal*. Nov. URL: https://www.wsj.com/articles/BL-CJB-24963
32. China Security GB Standarts List. URL: http://www.gbstandards.org/index/Standards_Search.asp?word=security
33. China's 'White-Hat' Hackers Fear Dark Times After Community Founder Is Detained. *The Wall Street Journal*, 1 Aug. 2016. URL: https://www.wsj.com/articles/BL-CJB-29440
34. China's foreign investment regime. Pinsent Masons. *OUT-LAW GUIDE*. 26 Nov., 2020. URL: https://www.pinsentmasons.com/out-law/guides/chinas-foreign-investment-law
35. China's government is keeping its security researchers from attending conferences (8 March 2018). *Cyberscoop*. URL: https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/
36. Chinese Army unit is seen as tied to hacking against U.S. *Atlantic Council*. February 19, 2013. URL: https://www.atlanticcouncil.org/blogs/natosource/chinese-army-unit-is-seen-as-tied-to-hacking-against-us/
37. Chipman Koty Alexander (13 May 2021). Personal Data Regulation in China: Personal Information Protection Law, Other Rules Amended. *China Briefing*. URL: https://www.china-briefing.com/news/personal-data-regulation-in-china-personal-information-protection-law-other-rules-amended/
38. Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010. URL: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
39. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 2030 Digital Compass: the European way for the Digital Decade. COM/2021/118 final. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118
40. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe /* COM/2015/0192 final */. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192
41. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Agenda on Security. Strasbourg, 28.4.2015 COM(2015) 185 final. URL: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
42. Communication from the Commission to the Council, the European parliament, the European Economic and Social Committee and the Committee of the Regions "Network and Information Security: Proposal for A European Policy Approach". Brussels, 6.6.2001. COM (2001)298 final.
43. Convention on International Information Security. The Ministry of Foreign Affairs of the Russian Federation. URL: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666
44. Coordinated action cuts off access to vpn service used by ransomware groups. *EUROPOL. Press Release*. 30 June 2021. URL: https://www.europol.europa.eu/newsroom/news/coordinated-action-cuts-access-to-vpn-service-used-ransomware-groups
45. Cyber Capabilities and National Power: A Net Assessment. IISS. Research Papers. 28th June 2021. URL: https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/

46. Cyber Policy and the 19th Party Congress. CSIS. October 26, 2017. URL: https://www.csis.org/analysis/cyber-policy-and-19th-party-congress
47. Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats. European Commission. MEMO/11/246 Brussels, 14th April 2011. URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_11_246
48. Cyber Threat Intelligence on Advanced Attack Groups and Technology Vulnerabilities. Threat Intelligence Reports. Fireyes, 2013.
49. *Cyber Warfare and Cyber Terrorism* (2008). Edited by Lech J. Janczewski and Andrew M. Colarik. Hershey, PA. Information Science Reference.
50. Cyberbricks. About us. URL: https://cyberbrics.info/about-us/
51. Cybercrime: Goals and Priorities. US Dept. of State. URL: https://2009-2017.state.gov/documents/organization/255007.pdf
52. Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU'. Publication 19 September 2017. URL: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu
53. Cyberspace PolIcy RevIew. Assuring a Trusted and Resilient Information and Communications Infrastructure. URL: https://fas.org/irp/eprint/cyber-review.pdf
54. Cyberwar. Bratannica. URL: https://www.britannica.com/topic/cyberwar
55. Declaration on PESCO projects (2018) Declaration on PESCO projects (bijlage bij 21501-02,nr.1813). URL: https://www.consilium.europa.eu/media/32020/draft-pesco-declaration-clean-10122017.pdf.
56. DEEP: Cybersecurity – A Generic Reference curriculum. NATO. URL: https://www.nato.int/cps/en/natohq/topics_157591.htm
57. Dickinson Steve (30 September 2019). China's New Cybersecurity Program: NO Place to Hide. *Harrais/Bricken*. URL: https://harrisbricken.com/chinalawblog/chinas-new-cybersecurity-program-no-place-to-hide/
58. Dingli Shen (23 April 2014). Framing China's National Security. China/US Focus. URL: https://www.chinausfocus.com/peace-security/%20%20framing-chinas-national-security
59. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
60. Draft United Nations Convention on Cooperation in Combating Information Crimes. The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Irelan. URL: https://www.rusemb.org.uk/fnapr/6394
61. Efrony Dan (16 July 2021). The UN Cyber Groups, GGE and OEWG – A Consensus is Optimal, But Time is of the Essence. *Just Security*. URL: https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/
62. EU Action Plan on Human Rights and Democracy 2020–2024. Council of the European Union. Brussels, 18 November 2020. URL: https://www.consilium.europa.eu/media/46838/st12848-en20.pdf
63. EU Cyber Defence Policy Framework (2018 update). Council of the European Union. Brussels, 19 November 2018. URL: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf
64. EU Cyber Security strategy: An open, safe and secure Cyberspace. 7 February, 2013. URL: https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en

65. EU CyberNet – the bridge to cybersecurity expertise in the European Union. URL: https://www.eucybernet.eu/
66. EU CyberNet work in Dominican Republic, first national cybersecurity exercise “Cyber llamas”. EU CyberNet. 21.05.2021. URL: https://www.eucybernet.eu/eu-cybernet-work-in-dominican-republic-first-national-cyber-llamas-exercise/
67. EU Data Protection Rules and U.S. Implications. Congressional Research Service. July 17, 2020. URL: https://sgp.fas.org/crs/row/IF10896.pdf
68. EU External Cyber Capacity Building Guidelines. Council of the European Union. Brussels, 26 June 2018. URL: https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
69. EU Human Rights Guidelines on Freedom of Expression Online and Offline. Council of the European Union. Brussels, 12 May 2014. URL: https://www.consilium.europa.eu/media/28348/142549.pdf
70. EU priorities at the United Nations during the 76th United Nations General Assembly, September 2021 – September 2022 – Council conclusions (12 July 2021). Brussels, 12 July 2021. URL: https://data.consilium.europa.eu/doc/document/ST-10393-2021-INIT/en/pdf
71. European Parliament resolution of 10 June 2021 on the EU’s Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)). URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_EN.html
72. EU–U.S. Cyber Dialogue Bruxelles, 16/12/2016 – 23:00 – UNIQUE ID: 161223_8. URL: https://www.statewatch.org/media/documents/news/2016/dec/eu-eeas-eu-us-cyber-dialogue-pr-16-12-16.pdf
73. EU–U.S. Summit 20 November 2010, Lisbon – Joint Statement. MEMO/10/597. Brussels, 20 November 2010. URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_10_597
74. EU–US Working Group on Cyber-Security and Cyber-Crime – CONCEPT PAPER. 13 April 2011. URL: https://www.statewatch.org/media/documents/news/2011/apr/eu-us-2011-04-13-concept-paper-cybersecurity.pdf
75. Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities". URL: https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m
76. Executive Order on Improving the Nation’s Cybersecurity. The White House, May 12, 2021. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
77. FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation’s Cybersecurity and Protect Federal Government Networks. The White House, May 12, 2021. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/
78. Farrell H. (2015). Promoting Norms for Cyberspace. New York. Council on Foreign Relations.
79. Final Session of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. UNODA, 28 May 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/05/HR-remarks-at-Final-Session-of-the-Group-of-Governmental-Experts-on-Advancing-responsible-State-behaviour-in-cyberspace-in-the-context-of-international-security.pdf
80. Finkle Jim (12 September 2012). Hundreds more cyber attacks linked to 2009 Google breach. *Reuters.* URL: https://www.reuters.com/article/cybersecurity-espionage-idUSL2E8K7A9E20120907

81. Finnemore M. (2011). Cultivating International Cyber Norms. *America's Cyber Future: Security and Prosperity in the Information Age*. / Ed. by K. Lord, T. Sharp. Washington, DC. Center for a New American Security. P. 89- 101.
82. Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on July 29, 2021. 2021/07/29. URL: https://www.mfa.gov.cn/ce/cohk//eng/Topics/fyrbt/t1896083.htm
83. Full Text: International Strategy of Cooperation on Cyberspace. 2017-03-01. URL: http://www.xinhuanet.com//english/china/2017-03/01/c_136094371_2.htm
84. Géry Aude (6 October 2020). A New UN Path to Cyber Stability. Directions. *Cyber Digital Europe*. URL: https://directionsblog.eu/a-new-un-path-to-cyber-stability/
85. Giovannelli D. (2021). *Proposal of United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes : Comment on the first draft text of the Convention.* CCDCOE. URL: https://ccdcoe.org/incyder-articles/proposal-of-united-nations-convention-on-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes-comment-on-the-first-draft-text-of-the-convention/
86. Global Cybersecurity Market Size to Grow at a CAGR of 12.5% from 2021 to 2028. *Quince Market Insights*, March 17, 2021. URL: https://www.globenewswire.com/en/news-release/2021/03/17/2194254/0/en/Global-Cybersecurity-Market-Size-to-Grow-at-a-CAGR-of-12-5-from-2021-to-2028.html
87. Global Freedom Status. *Freedom House*. URL: https://freedomhouse.org/explore-the-map?type=fiw&year=2021.
88. Good practices on interdependencies between OES and DSPs. ENISA, November 2018. URL: https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps/view/++widget++form.widgets.fullReport/@@download/WP2018+O.2.2.2+Good+practices+on+interdependencies+between+OES+and+DSPs.pdf
89. Greenberg L.T., Goodman S.E., Soo Hoo K.J. (1997). *Information Warfare and International Law*. Washington: National Defense University Press.
90. Greenberg, A. (13 October 2017). China tests the limits of its U.S. hacking truce. *Wired*. URL: https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/#
91. Griffiths James (12 December 2015). Chinese President Xi Jinping: Hands off our Internet. *CNN*. URL: https://edition.cnn.com/2015/12/15/asia/wuzhen-china-internet-xi-jinping
92. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015). UNDOCS. URL: https://undocs.org/A/70/174
93. Haass Richard (2020). Present at the Disruption. How Trump Unmade U.S. Foreign Policy. *Foreign Affairs*. September/October. URL: https://www.foreignaffairs.com/articles/united-states/2020-08-11/present-disruption
94. Hansen L., Nissenbaum H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly* 4. P. 1155–1175.
95. Hao Yeli (2017). A Three-Perspective Theory of Cyber Sovereignty. Belfercenter. URL: https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model
96. Hofmann J. (2005). *Internet Governance: A Regulative Idea in Flux*. Social Science Research Centre. Berlin, 2005. URL: http://duplox.wzb.eu/people/jeanette/texte/Internet%20Governance%20english%20version.pdf
97. Holland Steve, Shalal Andrea (10 July 2021). Biden presses Putin to act on ransomware attacks, hints at retaliation. *Reuters.* URL: https://www.reuters.com/technology/biden-pressed-putin-call-act-ransomware-attacks-white-house-2021-07-09/

98. *HPCR Manual on International Law Applicable to Air and Missile Warfare* (2009). HPCR. URL: https://reliefweb.int/sites/reliefweb.int/files/resources/8B2E79FC145BFB3D492576E00021ED34-HPCR-may2009.pdf
99. Hu Henry L. (2011). The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration. *The China Quarterly*. 207 (207). P. 523–540.
100. ICRC 'How is the Term "Armed Conflict" Defined in International Humanitarian Law?', Opinion paper, March 2008. URL: http://www.icrc.org/eng/assets/files/other/opinion-paper-armed- conflict.pdf
101. International action against 'gameover zeus' botnet and 'cryptolocker' ransomware. EUROPOL. Press Release. 02 June 2014. URL: https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware
102. International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf
103. Internet Governance: A Grand Collaboration (ed. by D. MacLean) (2005). N.Y. UN ICT Task Force Series. 393 p.
104. ISACA. Glossary of terms, 2008 (2008). ISACA. URL: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf
105. ITU estimates that at the end of 2019, a bit more that 51 per cent of the global population, or 4 billion people, are using the Internet. ITU. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
106. *Japan Cybersecurity Strategy.* Information Security policy Council, 2013. URL: http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf
107. Joint Communication to the European Parliament and the Council. Report on implementation of the EU's Cybersecurity Strategy for the Digital Decade. Brussels, 6.8.2021 JOIN(2021) 14 final/2. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2021:14:REV1&rid=1
108. Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Brussels, 16.12.2020 JOIN(2020) 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164
109. Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats. European Commission. Brussels, 6.4.2016 JOIN(2016) 18 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN
110. Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. European Commission. Brussels, 13.9.2017 JOIN(2017) 450 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN1
111. Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. URL: https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf
112. Joint Publication 3-13, Information Operations. 13 February 2006. URL: https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf
113. Joint Statement on Advancing Responsible State Behavior in Cyberspace. URL: https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/
114. Julian Nicholas (24 January 2021). United States' and China's Cybersecurity Policies: Collaboration or Confrontation? *Journal of International Relations*. URL:

http://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation
115. Kelley Michael B (20 November 2013). The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. *Business Insider*. URL: https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013–11
116. Keohane R. Nye J. (1998). Power and interdependence in the information age. *Foreign affairs*. Vol 77, No. 5. P. 81–94.
117. Koh Harold Hongju (2012). International Law in Cyberspace. *Harvard International Law Journal.* 54 (December).
118. Kopiika M. (2020). Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя.* 1–2020. С. 102–109. URL: https://jpl.donnu.edu.ua/article/view/7967/7967
119. Kurbalija Jovan (2014). *An Introduction to Internet Governance*. DiploFoundation. 206 p.
120. Libicki M. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica, CA. RAND Corporation.
121. Liu Guozhu, "拜登政府国家安全战略的基本方针与发展方向, (Bài dēng zhèngfǔ guójiā ānquán zhànlüè de jīběn fāngzhēn yǔ fāzhǎn fāngxiàng) [Основна політика та напрям розвитку Стратегії національної безпеки адміністрації Байдена]. *Dangdai Shijie* 5 (2021): 50–57. URL: https://webcache.googleusercontent.com/search?q=cache:7-mexZ_mX1EJ:https://dysw.cnki.net/kcms/detail/detail.aspx%3Ffilename%3DJSDD202105008%26dbcode%3DCJFD%26dbname%3DCJFD2021%26v%3D+&cd=1&hl=uk&ct=clnk&gl=ua
122. Lederer Edith M. (28 December 2019). UN gives green light to draft treaty to combat cybercrime. *AP*. URL: https://apnews.com/article/79c7986478e5f455f2b281b5c9ed2d15
123. Mandiant Consulting Services, "APT1: Exposing One of China's Cyber Espionage Units". 2013. Fireeye. URL: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
124. Markoff Michele G. (23 June 2017). Explanation of Position at the Conclusion of the 2016−2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. US Department of State. URL: https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm
125. MIT Artificial Intelligence Laboratory, *The JAIR Information Space, MIT Artificial Intelligence Laboratory*, 10 June 1998. URL: http://www.ai.mit.edu/projects/infoarch/jair/jair-space.html
126. Molander Roger C., Riddile Andrew, Wilson Peter A. (1996). *Strategic Information Warfare. A New Face of War*. RAND. MR-661-OSD. URL: https://www.rand.org/pubs/monograph_reports/MR661.html
127. Molander Roger C., Wilson Peter A., Mussington B. David, Mesic Richard (1998). *Strategic Information Warfare Rising*. RAND. MR-964-OSD. URL: https://www.rand.org/pubs/monograph_reports/MR964.html
128. Morgan Steve (2021). *2021 Report: Cyberwarfare in the C-Suite, Cybersecurity Ventures.* URL: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf
129. Nakashima Ellen, Timberg Craig (14 December 2020). Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce. *The Washington Post*. URL: https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

130. National Council of ISACs. URL: https://www.nationalisacs.org/
131. National Cyber Strategy of the United States of America. Trumpwhitehouse. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
132. NATO Standard AJP-3.10.1 Allied Joint Doctrine for Psychological Operations. Edition B Version 1. With UK National Elements. September 2014. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf
133. *NATO, Information Warfare and International Security*. NATO Parliamentary Assembly Science and Technology Committee, Brussels, 6th October, 1999.
134. Neumann Scott (14 April 2021). Intelligence Chiefs Say China, Russia Are Biggest Threats To U.S. *NPR*. URL: https://www.npr.org/2021/04/14/987132385/intelligence-chiefs-say-china-russia-are-biggest-threats-to-u-s
135. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. European Commission. 16 December 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
136. *New PRC Internet Regulation*. A January 1998 report from U.S. Embassy Beijing. URL: https://fas.org/irp/world/china/netreg.htm
137. Newman, Lily Hay (6 May 2019). What Israel's Strike on Hamas Hackers Means For Cyberwar. *Wired*. URL: https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/
138. *NRC Working Group on Defence Reform and Cooperation Special Operations Forces Glossary Russian-English* (2006). NRC WGDRC SOF GLOSSARY (E-R) 08.12.06. URL: https://www.nato.int/docu/other/ru/2006/pdf/SOFglossary(R-E).pdf
139. Obama and Xi Jinping of China Agree to Steps on Cybertheft (25 September 2015) *The New York Times*. URL: https://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html
140. Open-ended working group on developments in the field of information and telecommunications in the context of international security Final Substantive Report. A/AC.290/2021/CRP.2. 10 March 2021. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
141. Oyedele Akin (6 May 2017). BUFFETT: This is 'the number one problem with mankind'. *INSIDER*. URL: https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5
142. Perlroth Nicole (19 July 2021). How China Transformed Into a Prime Cyber Threat to the U.S. *The New York Times*. URL: https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html
143. *Pillars of The International Strategy for Cyberspace*. U.S. Department of State. URL: https://2009-2017.state.gov/s/cyberissues/strategy/index.htm
144. Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities. Brussels, 16.12.2020 COM(2020) 829 final. URL: https://ec.europa.eu/home-affairs/sites/default/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf
145. Qiang, Xiao (18 September 2015). Congressional-Executive Commission on China (CECC) Hearing: Urging China's President Xi Jinping to Stop State-Sponsored Human Rights Abuses. *CECC*. URL: https://www.cecc.gov/sites/chinacommission.house.gov/files/CECC%20Hearing%20-%20Human%20Rights%20Abuses%20-%2018Sept15%20-%20Xiao%20Qiang.pdf
146. Qingqing Chen, Siqi Cao (20 July 2021) US turns cyberspace into another anti-China battlefield, ‘futile to contain Beijing’. *Global Times*. URL: https://www.globaltimes.cn/page/202107/1229168.shtml

147. REGULATION (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015. laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&rid=2
148. Remarks by president biden on america's place in the world. February 04, 2021. The White House. URL: Https://www.Whitehouse.Gov/briefing-room/speeches-remarks/2021/02/04/remarks-by-president-biden-on-americas-place-in-the-world/
149. Renewing America's Advantages: Interim National Security Strategic Guidance. The White House. March 2021, 20, 8. URL: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf
150. Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. 28 May 2021. ADVANCE COPY. URL: https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf
151. Revised Directive on Security of Network and Information Systems (NIS2). European Commission. Publication 16 December 2020. URL: https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2
152. Robertson Jordan, Riley Michael (4 October 2018). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg Businessweek*. URL: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
153. Ross Alec (25 April 2016). Want job security? Try online security. *Wired*. URL: https://www.wired.co.uk/article/job-security-cybersecurity-alec-ross
154. Ruys Tom, Corten Olivier, Hofer Alexandra (2018). *Use of Force in International Law*. Oxford University Press, 2018. URL: https://books.google.com.ua/books?id=MkdiswEACAAJ&printsec=frontcover&hl=uk#v=onepage&q&f=false
155. Ryjov Alexander P., Mikhalevich Igor F. (2020). Hybrid Intelligence Framework for Improvement of Information Security of Critical Infrastructures. In *Handbook of Research on Cyber Crime and Information Privacy*. IGI Global. P. 310–337.
156. Satter Raphael (3 March 2020). Chinese cybersecurity company accuses CIA of 11-year-long hacking campaign. *Reuters*. URL: https://www.reuters.com/article/us-china-usa-cia-idUSKBN20Q2SI
157. Schaffer Aaron (28 June 2021). The Cybersecurity 202: The United States is still number one in cyber capabilities. *The Washington Post*. URL: https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/
158. Schmitt Michael (10 June 2021). The Sixth United Nations GGE and International Law in Cyberspace. *Just Security*, June. URL: https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/
159. Schmitt, Michael N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York. Cambridge University Press. URL: http://www.cambridge.org/tallinnmanual2
160. *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals* (2014) Ed by G. Giacomello. Bloomsbury Publishing USA.
161. Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy. June 2016. URL: https://eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

162. Sink Justin, Parker Mario (5 February 2021). ‘America is back, Diplomacy is back’ – Biden reverses Trump’s foreign policy moves. *ThePrint*. URL: https://theprint.in/world/america-is-back-diplomacy-is-back-biden-reverses-trumps-foreign-policy-moves/599152/
163. Soldatkin Vladimir, Holland Steve (17 June 2021). Far apart at first summit, Biden and Putin agree to steps on cybersecurity, arms control. *Reuters*. URL: https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/
164. Soo Zen (22 April 2019). How Huawei beat America’s anti-China 5G propaganda war in Southeast Asia, years before it even began. *South China Morning Post*. URL: https://www.scmp.com/tech/article/3006935/how-huawei-beat-americas-anti-china-5g-propaganda-war-southeast-asia-years-it
165. Soo Zen (9 December 2020). China orders removal of 105 apps, including TripAdvisor. *Associated Press*. URL: https://apnews.com/article/media-prostitution-china-hong-kong-pornography-84314d74600bd87d6dcea77524e43ed7
166. Spokesperson of the Chinese Mission to the EU Speaks on a Question Concerning the Statements from the EU and NATO on the So-called Chinese Malicious Cyber Activities. 2021/07/20. URL: https://static.poder360.com.br/2021/07/nota-china-ataques-hackers.pdf
167. Statement of Acting Chairwoman Rosenworcel on Department of Justice Decision to Withdraw Lawsuit to Block California net Neutrality Law. URL: https://docs.fcc.gov/public/attachments/DOC-369799A1.pdf
168. Statement of the G-77 and China During the Fourteenth un Congress on Crime Prevention and Criminal Justice Kyoto, Japan 7–12 March 2021, Delivered by H.E. Ambassador Alejandro Solano Ortíz, Permanent Representative of Costa Rica. URL: https://www.g77.org/vienna/wp-content/uploads/2021/03/G77ChinaKyotoLongVersionFinal_070321.pdf
169. Statement on Agenda Item 107 ‘Countering the use of information and communications technologies for criminal purposes’. U.S. Mission to the United Nations. November 18, 2019. URL: https://usun.usmission.gov/statement-on-agenda-item-107-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes/
170. Statistics & data. Europol staff numbers. URL: https://www.europol.europa.eu/about-europol/statistics-data
171. Sternstein Aliya (7 December 2012). Cyber early warning deal collapses after Russia balks. *Nextgov*. URL: https://www.nextgov.com/cybersecurity/2012/12/cyber-early-warning-deal-collapses-after-russia-balks/60035/
172. Summary. DEPARTMENT OF DEFENSE CYBER STRATEGY (2018). URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
173. Szafranski R. (1995). A Theory of Information Warfare: Preparing for 2020. *Airpower Journal*. No. 1.
174. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017). Ed. by M. Schmitt. N.Y. Cambridge University Press. 638 p.
175. Tallinn Manual on the International Law Applicable to Cyber Warfare (2013). Ed. by M.Schmitt. N.Y. Cambridge University Press. 282 p.
176. Taylor Emily and Hoffmann Stacie (2019). *EU–US Relations on Internet Governance.* Chatham House. International Security Department. November 2019. URL: https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-14-EU-US-Relations-Internet-Governance2.pdf
177. Terrorism 2002-2005. U.S. Department of Justice. Federal Bureau of Investigation. URL: https://www.fbi.gov/stats-services/publications/terrorism-2002-2005
178. The Alliance. URL: https://www.weprotect.org/alliance/

179. The Analysis of Equation Drug —the Fourth Analysis Report of Equation Group. January 26, 2017. URL: https://www.antiy.net/p/the-analysis-of-equation-drug-the-fourth-analysis-report-of-equation-group/
180. The CIA Hacking Group (APT-C-39) Conducts Cyber-Espionage Operation on China's Critical Industries for 11 Years. 360 Core Security. URL: https://blogs.360.cn/post/APT-C-39_CIA_EN.html
181. The Comprehensive National Cybersecurity Initiative. URL: https://fas.org/irp/eprint/cnci.pdf
182. *The European Response to the rising Cyber Threat.* SPEECH/12/315 Cecilia Malmström. European Commissioner responsible for Home Affairs. Transatlantic Cyber Conference organised by the Center for Strategic and International Studies, the European Security Roundtable and SRA International. Washington, 2 May 2012. URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_315
183. The EU's Cybersecurity Strategy for the Digital Decade. European Commission. Publication 16 December 2020. URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
184. *The First amendment*. Legal Information Institute. URL: http://www.law.cornell.edu/anncon/html/amdt1afrag1_user.html#amdt1a_hd4
185. The future of discussions on ICTs and cyberspace at the UN. Updated version: 10/08/2020. URL: https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-future-of-cyber-discussions-at-un-10-08-2020.pdf
186. The National Strategy to Secure Cyberspace. February 2003. URL: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf
187. *The Recovery and Resilience Facility*. European Commission. URL: https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en
188. *The United States support efforts against Cybercrime*. US Embassy & Consulates in France. 13 September, 2016. URL: https://fr.usembassy.gov/united-states-support-efforts-cybercrime/
189. Tiede Peter (2021). Neuer Hacker-Angriff aus Russland! *BILD*, 30.06.2021. URL: https://www.bild.de/politik/inland/politik-inland/riesen-hacker-angriff-aus-russland-banken-und-kritische-infrastruktur-im-visier-76930232.bild.html
190. Tikk-Ringas E. (2015). *Evolution of the Cyber Domain: The Implications for National and Global Security*. London. Routledge, for the International Institute for Strategic Studies. 212 p.
191. Triolo Paul, Sacks Samm, Graham Webster, Creemers Rogier (30 November 2017) China's Cybersecurity Law One Year On, An Evolving and Interlocking Framework. *New America*. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/
192. Turton Williams, Jacobs Jennifer (7 July 2021). Russia 'Cozy Bear' Breached GOP as Ransomware Attack. *Bloomberg*. Hit. URL: https://www.bloomberg.com/news/articles/2021-07-06/russian-state-hackers-breached-republican-national-committee
193. U.S. Army Heritage and Education Center (16 February 2018). Who first originated the term VUCA (Volatility, Uncertainty, Complexity and Ambiguity)?. *USAHEC Ask Us a Question*. The United States Army War College. URL: https://usawc.libanswers.com/faq/84869
194. U.S. charges four Chinese nationals charged in global hacking campaign (19 July 2021). *Reuters*. URL: https://www.reuters.com/technology/four-chinese-nationals-charged-global-hacking-campaign-us-justice-department-2021-07-19/

195. UNIDIR. Report of the International Security Cyber Issues Workshop Series. 2016. URL: https://www.unidir.org/publication/report-international-security-cyber-issues-workshop-series
196. US Department of State, “Secretary Antony J. Blinken, National Security Advisor Jake Sullivan, Director Yang and State Councilor Wang at the Top of Their Meeting,” Anchorage, March 18, 2021. URL: https://www.state.gov/secretary-antony-j-blinken-national-security-advisor-jake-sullivan-chinese-director-of-the-office-of-the-central-commission-for-foreign-affairs-yang-jiechi-and-chinese-state-councilor-wang-yi-at-th/
197. US justice department charges Chinese with hacking (14 May 2014). *BBC.* URL: https://www.bbc.com/news/world-us-canada-27475324
198. US support to the Budapest Convention (25 September 2018). *Council of Europe*. Strasbourg, . URL: https://www.coe.int/en/web/cybercrime/-/us-support-to-the-budapest-convention
199. US turns cyberspace into another anti-China battlefield, ‘futile to contain Beijing’ (28 July 2021) *National Cyber Security Ne*ws *Today*. URL: https://nationalcybersecuritynews.today/us-turns-cyberspace-into-another-anti-china-battlefield-futile-to-contain-beijing-cybersecurity-cyberattack/
200. Vittorio Andrea (16 July 2021). Surveillance in Spotlight Amid Ongoing EU-U.S. Data Privacy Rift. *Bloomberg Law*. URL: https://news.bloomberglaw.com/privacy-and-data-security/surveillance-in-spotlight-amid-ongoing-eu-u-s-data-privacy-rift
201. Wendt A. (1995). Constructing International Politics. *International Security*. No. 1(20). P. 71–8.
202. Wenger A. (2001). The Internet and the Changing Face of International Relations and Security. *Information and Security*. No. 7. P. 5–11.
203. What can we learn from the "most devastating" cyberattack in history? (22 August 2018). *CBC News*. August. URL: https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/
204. Wolfe Derek (21 July 2021). How China Became a Digital Adversary and Threat to the U.S. *GSIExchange.* URL: https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/
205. Xi Jinping calls for 'cyber sovereignty' at internet conference (16 December 2015). *BBC*. https://www.bbc.com/news/world-asia-china-35109453
206. Xinmin Ma (2013). 马新民，The Law of Use of Force: Development and Challenges. *China International Law Yearbook. 1,* 中国国际法年刊 (2013), 93.
207. Yan Luo, Zhijing Yu, Nicholas Shepherd (2021). Cybersecurity risk classification under China's multi-level protection scheme. Practical Law. Thomson Reuters. URL: https://uk.practicallaw.thomsonreuters.com/w-022-3160?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true
208. Zetter Kim (31 January 2013). New York Times Hacked Again, This Time Allegedly by Chinese. *WiredI*. URL: https://www.wired.com/2013/01/new-york-times-hacked/
209. Zhong Raymond, Mozur Paul, Krolik Aaron, Kao Jeff (19 December 2020). Leaked Documents Show How China's Army of Paid Internet Trolls Helped Censor the Coronavirus. *ProPublica.*
210. Zhu Shenshen (29 December 2015). Wuzhen initiative on Internet future. *Shanghai Daily*. URL: https://archive.shine.cn/business/it/Wuzhen-initiative-on-Internet-future/shdaily.shtml
211. Zunyou Zhou (21 December 2015). China’s Draft Cybersecurity Law. *China Briefing*. 15. No. 24. URL: https://jamestown.org/program/chinas-draft-cybersecurity-law/.
212. Аничкина Т.Б. (2007). О некоторых приемах информационной войны США. *США-Канада: экономика, политика, культура*. № 7. С. 123–127.

213. Быков А. И. (2008). *Управление Интернетом как одна из проблем современных международных отношений*. Политэкс. URL: http://www.politex.info/content/view/438/30
214. В Москве прошел митинг против изоляции Рунета (10.03.2019). *РБК*. URL: https://www.rbc.ru/politics/10/03/2019/5c851a2d9a7947fefc8e4288
215. Вейкфілд Джейн (27.05.2021). "Китай використовує уйгурів як піддослідних щурів". Що відомо про камери розпізнавання емоцій. *BBC News Україна*. URL: https://www.bbc.com/ukrainian/news-57265671
216. Военная доктрина Российской Федерации. URL: http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf
217. Глобальная безопасность: инновационные методы анализа конфликтов (2011) Под ред. А. И. Смирнова.Москва. Общество «Знание» России. 272 с.
218. Дані ЮНКТАД (UNCTADSTAT. International trade in digitally-deliverable services, value, shares and growth, annual. URL: https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=158358)
219. Дані ЮНКТАД (UNCTADSTAT. International trade in ICT services, value, shares and growth, annual. URL: https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=158359)
220. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 8 червня 1977 року. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text
221. Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895) Совет безопасности РФ. URL: http://www.scrf.gov.ru/documents/5.html
222. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html
223. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. UN. A/RES/53/70. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R
224. Дремлюга Роман Игоревич, Коробеев Александр Иванович, & Федоров Александр Вячеславович (2017). Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты. *Всероссийский криминологический журнал.* 11 (3). С. 607-614. URL: http://cj.bgu.ru/reader/article.aspx?id=21722
225. Закон України Про основні засади забезпечення кібербезпеки України (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
226. Заявление глав государств-членов ШОС по международной информационной безопасности (г. Шанхай, 15 июня 2006 года). Russian.People. URL: http://russian.people.com.cn/31857/102574/102589/7409849.html
227. Заявление Совета глав государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2020/11/10. URL: http://ru.china-embassy.org/rus/zgxw/t1831178.htm
228. Зиновьева Е. (2014). Международное сотрудничество по обеспечению информационной безопасности. *Право и управление. XXI век*. № 4.
229. Иванов Станислав, Томилов Олег (14.03.2013). Кибертерроризм: угроза национальной и международной безопасности. *ИА "Оружие России"*. URL: https://bit.ly/2UFEJl6
230. Информационное противоборство. Справочник МО РФ. URL: https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary

231. Канев Сергей (0.05.2014). Чебурашка, или Хорошими делами прославиться нельзя. *Новая Газета*. URL: https://novayagazeta.ru/articles/2014/05/05/59473-cheburashka-ili-horoshimi-delami-proslavitsya-nelzya
232. Кісілевич-Чорнойван О. М. (2009). Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика*. № 8. С. 11–18. URL: http://nbuv.gov.ua/UJRN/utp_2009_8_2
233. Конвенція про кіберзлочинність. Офіційний переклад. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
234. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. 2011. URL: https://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle
235. Коротков А. В. (2011). Безопасность критических информационных инфраструктур в международном гуманитарном праве. *Вестник МГИМО-Университета*. № 4. С. 154–162.
236. Крутских А. В. (2007). К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы*. № 1(5). С.28–37.
237. Кучерявый М. М. (2013). Глобальное информационное общество и проблемы безопасности. *Власть. Общенациональный научно-политический журнал*. № 9 (сентябрь). С. 89–92.
238. Манойло А. В. (2003). *Государственная информационная политика в особых условиях: Монография.* Москва. МИФИ, 2003. 388 с.
239. Манойло А.В. (2003). Объекты и субъекты информационного противоборства. *Пси фактор*. URL: http://psyfactor.org/lib/psywar24.htm
240. Макаренко Є.А., Рижков М.М., Ожеван М.А., Кучмій О.П., Фролова О.М. (2016). Міжнародна інформаційна безпека: теорія і практика. Підручник. Київ. Центр вільної преси. 418 с.
241. Настюк В. Я., Бєлєвцева В. В. (2014). Правові засади міжнародного співробітництва щодо протидії інформаційним правопорушенням. *Правова інформатика*, № 2(42). URL: http://ippi.org.ua/sites/default/files/14nvypip.pdf
242. Носов С. (2021). Система кибербезопасности в Китае (2021). *Зарубежное военное обозрение*. 2021. №2. С. 17–24. URL: http://factmil.com/publ/strana/kitaj/sistema_kiberbezopasnosti_v_kitae_2021/59-1-0-1833
243. Основы государственной политики в области международной информационной безопасности на период до 2020 года. URL: http://www.consultant.ru/document/cons_doc_LAW_178634/
244. Основы государственной политики Российской Федерации в области международной информационной безопасности (Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213). URL: http://www.scrf.gov.ru/security/information/document114/
245. Правила поведения в области обеспечения международной информационной безопасности, Документ ООН A/69/723/, 13 января 2015. URL: https://bit.ly/31dRCX0
246. Правительство РФ не видит необходимости в законодательном закреплении сетевого нейтралитета (29.10.2018). Роскомсвобода. URL: https://roskomsvoboda.org/42667/
247. Приложение к письму Постоянного представителя Российской Федерации при Организации Объединенных Наций от 11 октября 2017 года на имя Генерального секретаря Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности. : URL: https://namib.online/wp-content/uploads/2020/04/Проект-Конвенции-Организации-Объединенных-Наций-о-сотрудничестве-в-сфере-противодействия-информационной-преступности.pdf

248. Принят закон о ”суверенном интернете”. Государственная Дума Федерального собрания Российской Федерации. 16.04.2009. URL: http://duma.gov.ru/news/44551/
249. Проект. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях. 29.06.2021. UNDOC. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf
250. Рекомендация о развитии и использовании многоязычия и всеобщем доступе к киберпространству. Принята 15 октября 2003 года. URL: https://www.un.org/ru/documents/decl_conv/conventions/multilingualism_recommendation.shtml
251. Романчук Ю. В. (2009). *Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти.* Автореф. дис... канд. політ. наук: 23.00.04. НАН України. Ін-т світ. економіки і міжнар. відносин. Київ. 20 с.
252. Ромашкина Наталья, Задремайлова Вероника (2020). Эволюция политики КНР в области информационной безопасности. *Пути к миру и безопасности*. № 1(58). С. 122–138. URL: https://www.imemo.ru/publications/periodical/pmb/archive/2020/1-58/in-focus-east-asia/security-policies-of-east-asian-states/evolution-of-chinas-information-security-policy
253. Россия и США перетягивают всемирную паутину. В ООН представлены конкурирующие резолюции по кибербезопасности (12.11.2018). *Коммерсантъ*. № 207. С. 6. URL: https://www.kommersant.ru/doc/3797617
254. Соглашение между правительствами государств—членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Екатеринбург, 16 июня 2009 года. URL: https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreementRussian.pdf
255. Солодка О. М. (2020). Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. № 1(32). URL: http://il.ippi.org.ua/article/view/200311
256. "Таллинское руководство" о войне в интернете встревожило Россию – этот документ сам по себе опасен. *NEWSru.com*. 27.05.2013. https://www.newsru.com/hitech/27May2013/cyber.html
257. Туронок С. Г. (2003). Информационно-коммуникативная революция и новый спектр военно-политических конфликтов. *Политические исследования*. № 1. С. 24–38.
258. Указ Президента Российской Федерации от 05.12.2016 г. № 646. Об утверждении Доктрины информационной безопасности Российской Федерации. URL: http://kremlin.ru/acts/bank/41460/page/1
259. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №121/2021. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України». URL: https://www.president.gov.ua/documents/1212021-37661
260. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №392/2020. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». URL: https://www.president.gov.ua/documents/3922020-35037
261. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: https://www.president.gov.ua/documents/472017-21374
262. Федоров А. В., Зиновьева Е. С. (2017). *Международная информационная безопасность: политическая теория и дипломатическая практика*. Москва. МГИМО. 360 с.
263. Фролова О. (2019). Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. *Вісник Львівського університету. Серія: Міжнародні*

відносини. Вип. 46. С. 123–136. URL: http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_13
264. Фролова О. М. (2018). Роль ООН в системі міжнародної інформаційної безпеки. *Електронне видання Інституту міжнародних відносин "Міжнародні відносини. Серія: Політичні науки"*, №18. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468
265. Швец Д. Ю. (2005). *Информационная безопасность Российской Федерации в современных международных отношениях*. Дисс. … кандидата социологических наук. Москва. МГИМО (У) МИД России. 153 с.
266. Якушев М. В. (1999). Информационное общество и правовое регулирование: новые проблемы теории и практики. *Информационное общество*. № 1. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/2be96a4e09339699c32568b1003ab653
267. **中**华人民共和国反恐怖主义法 (Zhōnghuá rénmín gònghéguó fǎn kǒngbù zhǔyì fǎ) [Закон Китайської Народної Республіки про боротьбу з тероризмом]. 27.12.2015. URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-06/12/content_2055871.htm
268. **中**华人民共和国网络安全法(Zhōnghuá rénmín gònghéguó wǎngluò ānquán fǎ) [Закон Китайської народної республіки про кібербезпеку]. 07.11.2016. URL: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm
269. **中**华人民共和国网络安全法. URL: https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95/16843044?fr=aladdin
270. **中国共**产党领导是中国特色社会主义最本质的特征. 来源：《求是》2020/14 作者：习近平 (Zhōngguó gòngchǎndǎng lǐngdǎo shì zhōngguó tèsè shèhuì zhǔyì zuì běnzhí de tèzhēng. Láiyuán:"Qiú shì"2020/14 zuòzhě: Xíjìnpíng) [Лідерство Комуністичної партії Китаю є найважливішою ознакою соціалізму з китайськими особливостями. Джерело: "Пошук правди" 2020/14 Автор: Сі Цзіньпін]. Qishi. http://www.qstheory.cn/dukan/qs/2020-07/15/c_1126234524.htm
271. **全面**贯彻落实总体国家安全观 为全方位推进高质量发展超越筑牢安全屏障 (Quánmiàn guànchè luòshí zǒngtǐ guójiā ānquán guān wèi quán fāngwèi tuījìn gāo zhìliàng fāzhǎn chāoyuè zhù láo ānquán píngzhàng) [Повністю реалізувати загальну концепцію національної безпеки, щоб всебічно сприяти високоякісному розвитку та вийти за межі створення міцного бар'єру безпеки]. 17.04.2021. URL: http://www.cac.gov.cn/2021-04/17/c_1620246064486609.htm
272. **公安机关互**联网安全监督检查规定 (Gōng'ān jīguān hùliánwǎng ānquán jiāndū jiǎnchá guīdìng) [Положення про нагляд та перевірку безпеки в Інтернеті органами громадської безпеки, Наказ Міністерства громадської безпеки КНР від 15 вересня 2018 р. № 151]. URL: http://www.gov.cn/gongbao/content/2018/content_5343745.htm
273. **国**务院关于大力推进信息化发展和切实保障信息安全的若干意见 (2012) 23 **号** (Guówùyuàn guānyú dàlì tuījìn xìnxī huà fāzhǎn hé qièshí bǎozhàng xìnxī ānquán de ruògān yìjiàn (2012) 23 hào) [Кілька думок Державної ради щодо енергійного сприяння розвитку інформатизації та ефективної гарантії інформаційної безпеки, 2012)]. 17.07.2012. URL: http://www.gov.cn/gongbao/content/2012/content_2192395.htm.
274. **国家互**联网信息办公室关于《网络安全审查办法（修订草案征求意见稿）》**公开征求意**见的通知 (Guójiā hùliánwǎng xìnxī bàngōngshì guānyú "wǎngluò ānquán shěnchá bànfǎ (xiūdìng cǎo'àn zhēngqiú yìjiàn gǎo)" gōngkāi zhēngqiú yìjiàn de tōngzhī)

[Повідомлення Державного інформаційного офісу Інтернету про "Заходи з огляду кібербезпеки (переглянутий проект збору коментарів, 10 липня 2021)" Публічне звернення за коментарями]. URL: http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm

275. **国家网信**办启动 2020“**清朗**”专项行动，为期 8 **个月**. URL (Guójiā wǎng xìn bàn qǐdòng 2020“qīnglǎng” zhuānxiàng xíngdòng, wéiqí 8 gè yuè) [Управління кіберпростору Китайської Народної Республіки розпочало спеціальну кампанію «чистий» 2020 рік на 8 місяців]. URL: http://politics.people.com.cn/n1/2020/0522/c1001-31719589.html

276. **汪玉**凯: **中央网**络安全与信息化领导小组的由来及其影响 (Wāngyùkǎi: Zhōngyāng wǎngluò ānquán yǔ xìnxī huà lǐngdǎo xiǎozǔ de yóulái jí qí yǐngxiǎng) [Ван Юкай. Походження провідної малої групи з інформатизації та безпеки в мережі інтернет]. *Baidu.com*. 06.03.2014. URL: https://wenku.baidu.com/view/0c29475252d380eb62946d86.html.

277. 计算机信息系统安全管理制度 (Jìsuànjī xìnxī xìtǒng ānquán guǎnlǐ zhìdù) [Система управління безпекою комп'ютерної інформаційної системи]. URL: https://wenku.baidu.com/view/8814c60716fc700abb68fc31.html.

Для нотаток

Наукове електронне видання на CD-ROM

Федонюк Сергій Валентинович

МІЖНАРОДНІ АСПЕКТИ БЕЗПЕКИ КІБЕРПРОСТОРУ

Монографія

Друкується в авторській редакції

Один електронний оптичний диск (CD-ROM). Об'єм даних 4,72 Мб. Тираж 300 прим.
Зам. 30. Видавець і виготовлювач – Вежа-Друк,
м. Луцьк, вул. Шопена, 12, тел. (0332) 29-90-65.
E-mail: vezhaprint@gmail.com
Свідоцтво Держ. комітету телебачення та
радіомовлення України ДК № 4607 від
30.08.2013 р.

ISBN 978-966-940-406-0