



МІЖНАРОДНА ПОЛІТИКА ІНФОРМАЦІЙНОЇ (КІБЕР) БЕЗПЕКИ

СЕРГІЙ ФЕДОНЮК

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЛЕСІ УКРАЇНКИ

Сергій Федонюк

**МІЖНАРОДНА ПОЛІТИКА ІНФОРМАЦІЙНОЇ (КІБЕР) БЕЗПЕКИ.
87 ПИТАНЬ І ВІДПОВІДЕЙ**

Навчальний посібник

Електронне видання на CD-ROM

Луцьк
Вежа-Друк
2023

УДК 351.746:004.9.056

Ф 32

*Рекомендовано до друку вченою радою
Волинського національного університету імені Лесі Українки
(протокол № 3 від 23 лютого 2023 р.)*

Рецензенти:

Тодоров І. Я. – доктор історичних наук, професор кафедри міжнародних студій та суспільних комунікацій Ужгородського національного університету;

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

Вознюк Є. В. – кандидат політичних наук, доцент кафедри міжнародних відносин і регіональних студій Волинського національного університету імені Лесі Українки.

Федонюк Сергій

Ф 32 Міжнародна політика інформаційної (кібер) безпеки. 87 питань і відповідей [Текст]: навч. посіб. / Сергій Валентинович Федонюк. – Луцьк : Вежа-Друк, 2023. – 1 електрон. опт. диск (CD-ROM). – Об'єм даних 3,55 Мб.

ISBN 978-966-940-515-9

Книга стосується вивчення політики у сфері інформаційної (кібер) безпеки, її витоків і цілей провідних міжнародних акторів із погляду міжнародного співробітництва. Розкрито підходи в реалізації політики й міжнародної діяльності основних міжнародних акторів у сфері інформаційної (кібер) безпеки США, Росії, Китаю, Європейського Союзу переважно в період від кінця 1990-х рр. до початку 2022.

Для здобувачів вищої освіти в галузі міжнародних відносин та всіх, хто цікавиться питаннями розвитку кіберпростору в міжнародних і безпекових аспектах.

УДК 351.746:004.9.056

ISBN 978-966-940-515-9

© Федонюк С. В., 2023

ЗМІСТ

ВСТУП	10
1. Де витоки кіберзагроз?	11
2. Інформаційна безпека чи кібербезпека?	12
3. Які є наукові підходи до проблеми управління інтернетом?	13
4. Які основні підходи до проблеми інформаційної безпеки з погляду міжнародного права?	14
5. Як по-різному розглядають інформаційні загрози воєнного характеру представники країн Заходу та Росії?	15
6. Яких позицій щодо проблем інформаційної безпеки дотримуються українські науковці?.....	16
КІБЕРПРОСТІР: ЗАГРОЗИ Й КОНЦЕПЦІЇ БЕЗПЕКИ	18
Масштаби кіберзагроз	18
7. Як сучасні ринкові процеси й розвиток інтернету впливають на виникнення потенційних кіберзагроз?	18
8. Про що свідчить зростання витрат на кібербезпеку?	19
9. У чому проявляються новітні кіберзагрози?	20
Кіберзлочинність	21
10. Що таке «кіберзлочинність»?	21
11. Чи можуть кібернападники мати політичні цілі? Чи відомі вам кібератаки такого виду?.....	23
Кібертероризм	25
12. Що таке «кібертероризм»? У чому полягають відмінності в трактуванні цього поняття?	25
13. Які є прояви кібертероризму?	27
Воєнні загрози, пов'язані з інформаційними впливами	28
14. Які є види інформаційних загроз воєнного характеру?	28

15. У чому суть основних позицій держав із приводу міжнародно-правового регулювання інформаційної (кібер) безпеки?.....	29
16. Чи інформація й програмне забезпечення можуть безпосередньо спричиняти руйнування або пошкодження фізичних об'єктів і завдавати шкоди людям? Поясніть це з погляду міжнародних відносин.....	30
17. Чи є підстави трактувати вплив кіберзасобами з погляду міжнародного гуманітарного права?.....	31
Інформаційне протиборство.....	32
18. Що таке «інформаційна війна»? А «кібервійна»?	32
19. У чому суть концепції інформаційного протиборства (Information Warfare)?.....	33
20. Які зміни відбуваються в західній концепції стратегічних інформаційних впливів?	34
21. Якого підходу у військовій сфері інформаційної- та кібербезпеки дотримується Україна?	37
22. Як взаємопов'язані військові й невійськові впливи в російській (східній) моделі інформаційної безпеки?	38
Інформаційна (кібер) безпека.....	42
23. На чому ґрунтуються демократичний та авторитарний підходи у сфері інформаційної безпеки?.....	42
24. Які історичні передумови сучасної концепції інформаційної безпеки в США?	42
25. На яких принципах ґрунтується політика Європейського Союзу у сфері інформаційної безпеки?.....	44
26. Яка концепція інформаційної безпеки реалізується в Японії?.....	45
27. У чому суть інформаційної безпеки з позицій Росії? Як це стосується свободи слова й інформації?.....	46
28. Що таке інформаційний- і кіберсуверенітет із погляду Росії й Китаю?.....	47

29. Що таке «мережевий нейтралітет»? Яке ставлення до нього характерне для різних політичних систем?	51
30. У чому суть відмінностей у трактуванні поняття «інформаційна безпека»?	53
Кібервійни й міжнародне право	53
31. У чому полягає проблемність застосування міжнародного права у сфері кібервоєн?	53
32. Як співвідносяться поняття інформаційних- і кібервійн?	56
33. У чому полягає проблемність ідентифікації сторін конфлікту в умовах інформаційного протистояння з погляду міжнародного права? ..	57
34. Яка роль «Таллінського посібника» в питанні застосування міжнародного права у сфері кібервійн?	60
НАЦІОНАЛЬНІ Й РЕГІОНАЛЬНІ ПІДХОДИ ДО БЕЗПЕКИ КІБЕРПРОСТОРУ	64
Авторитарні держави	64
Підхід Росії	64
35. Що таке «міжнародна інформаційна безпека»?.....	64
36. Що, із позиції Росії, розглядається в якості «загроз миру й безпеці в інформаційному просторі»?	65
37. У яких офіційних документах РФ відображено офіційні погляди на «міжнародну інформаційну безпеку»?.....	66
38. Що в Росії розглядають як «загрози міжнародній інформаційній безпеці»?.....	66
39. У чому суть зовнішньої політики Росії у сфері інформаційної безпеки?	68
40. У чому суть російського підходу до міжнародного співробітництва у сфері інформаційної безпеки?.....	69
41. У чому відмінність між поняттями «інформаційний простір» і «кіберпростір»?.....	71

Діяльність Росії в ООН	73
42. Які головні напрями діяльності Росії на рівні ООН щодо просування своїх інтересів у сфері інформаційної (кібер) безпеки?	73
43. Як можна коротко окреслити сферу й обставини діяльності Групи урядових експертів у сфері інформатизації й телекомунікації в контексті міжнародної безпеки (UN GGE)?	75
44. У чому суть позиції Росії у сфері протидії інформаційній злочинності?.....	77
45. Яка причина особливої позиції РФ у сфері інформаційної (кібер) безпеки?	78
Китай	79
46. На яких засадах ґрунтується політика у сфері інформаційної (кібер) безпеки Китаю?	79
47. Яка інституційна основа політики інформаційної (кібер) безпеки КНР?.....	80
48. Як регулюється кіберпростір у КНР?.....	81
49. Як розвивалася нормативна основа кібербезпеки КНР?.....	83
50. У чому полягають головні виклики закону КНР про кібербезпеку з погляду іноземних компаній?.....	85
51. У чому полягає системність підходу китайської влади до регулювання кіберпростору?	87
Демократичні держави	90
Розвиток політики кібербезпеки США	90
52. Які характерні риси були притаманні політиці кібербезпеки США у 2000-х рр.?	90
53. Які виклики визначали політику США у сфері кібербезпеки в період президентства Барака Обами?.....	92
54. Які цілі визначено в «Міжнародній стратегії для кіберпростору» США (2011 р.)?	95

55. Які характерні риси притаманні політиці адміністрації Д. Трампа у сфері кібербезпеки?.....	96
56. Які позиції у сфері міжнародної політики характеризують кіберстратегію Д. Трампа?	98
57. Як змінилася політика США у сфері кібербезпеки з приходом адміністрації Джозефа Байдена?.....	103
Діяльність США в ООН.....	106
58. Яка роль США в роботі Групи урядових експертів UN GGE?	106
59. Які наслідки діяльності Групи урядових експертів UN GGE та прийнятих нею рішень?	107
60. У чому суть ініційованої США Резолюції ГА ООН «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки» (2018 р.)?	108
61. На яких засадах і з якою метою функціонує Робоча група відкритого складу, створена відповідно до Резолюції ГА ООН «Досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки» (2018 р.)?	111
62. Які рішення прийнято UN GGE у період одночасної роботи з OEWG?.....	114
Підхід ЄС	116
63. Які засади політики ЄС у сфері інформаційної (кібер) безпеки?	116
64. Яку роль відіграє політика кібербезпеки в Глобальній стратегії ЄС?	117
65. Як розвивається політика кібербезпеки ЄС?.....	119
66. Які головні положення Стратегії кібербезпеки ЄС для цифрового десятиліття (2020 р.)?.....	121
67. Які пріоритети в політиці кібербезпеки ЄС актуалізуються з прийняттям стратегії «Цифровий компас: європейський шлях до Цифрового десятиліття»?	123

68. На яких концептуальних підходах засновано сучасну стратегію ЄС у сфері кібербезпеки?.....	125
69. У чому суть пропозиції Програми дій для просування відповідальної поведінки держав у кіберпросторі? Яка роль ЄС у її просуванні?	127
ВЗАЄМОДІЯ МІЖ ДЕРЖАВАМИ У СФЕРІ ІНФОРМАЦІЙНОЇ (КІБЕР) БЕЗПЕКИ.....	131
Міжнародна діяльність Китаю у сфері кібербезпеки.....	131
70. Із якою метою проводиться Всесвітня інтернет-конференція й започатковано Уженську ініціативу?	131
71. Які головні напрями міжнародної стратегії Китаю в кіберсфері?.....	132
72. Які головні напрями реалізації кіберстратегії Китаю в регіональних відносинах?.....	134
73. У чому полягають принципові відмінності між підходами до безпеки кіберпростору в Китаї та США?.....	135
74. У діяльності яких міжнародних організацій проявляється узгодження позицій Китаю та Росії в питаннях безпеки кіберпростору?.....	136
Проблеми взаємодії США й Китаю у сфері кібербезпеки.....	139
75. У чому суть протистояння між США й Китаєм у сфері кібербезпеки?	139
76. Який характер має конкуренція між США й Китаєм в аспекті кіберможливостей?.....	143
77. Як формувалося розуміння Китаю як джерела кіберзагроз для США?.....	144
78. Як сьогодні розглядається Китай стосовно кібербезпеки США?.....	147
79. Із яких позицій влада Китаю розглядає США в аспекті кібербезпеки?	152
Взаємодія ЄС і США у сфері кібербезпеки.....	158

80. Яка концептуальна позиція Європейського Союзу щодо політики у сфері безпеки кіберпростору?	158
81. Як узгоджуються зусилля ЄС і США у сфері міжнародної взаємодії щодо боротьби з кіберзлочинністю?	159
82. Які інституції функціонують у сфері співпраці ЄС і США щодо протидії кіберзагрозам?	165
83. Як відбуваються практична взаємодія ЄС і США й запозичення досвіду у сфері протидії кіберзагрозам?	169
84. Які розбіжності існують у підходах ЄС і США до політики безпеки кіберпростору?	172
Взаємодія ЄС з іншими країнами	173
85. Які проблеми безпеки кіберпростору покликана розв'язати кіберстратегія ЄС за допомогою міжнародної взаємодії?	173
86. Які головні регіональні напрями міжнародної співпраці ЄС у сфері розвитку потенціалу протидії кіберзагрозам?	176
87. Які головні напрями співпраці держав ЄС у сфері кібербезпеки й оборони?	178
ВИСНОВКИ	181
ДЖЕРЕЛА ТА ЛІТЕРАТУРА	185
ГЛОСАРІЙ	219

ВСТУП

Шановний читачу, перед тобою – сукупність питань, над якими можеш подумати, знайти допомогу в тексті, скористатися ресурсами з інтернету й активними гіперпосиланнями, що додаються. Звісно, проблема інформаційної (кібер) безпеки складна й динамічна, тому пропонований текст – це лише спроба допомогти в пошуку адекватних розв’язань на конкретний момент часу та в стосунку до конкретної ситуації. Зміст книги розподілено на 88 питань і відповідей, але текст упорядковано так, що його зручно читати від початку й до кінця, міркуючи над логікою викладу.

Ми розглядаємо низку 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 та 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 держав) – це сила, що ґрунтується на тотальному управлінні інформацією та її контролі, домінуюча участь держави в суспільному житті й економіці. На цих підходах ґрунтується внутрішня та 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 у сферах державного суверенітету, управління інтернетом, застосування міжнародного права в кіберсфері, доступності інформаційних технологій та ін.

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

Скільки людей, стільки й думок. І стільки ж досвідів. Тому звертаюся до тебе, читачу, із пропозицією взяти участь у розвитку й покращенні цієї книги. Запропонуй власні судження, поділися критичними зауваженнями, подай додаткові важливі факти – і вони обов’язково будуть розглянуті й ураховані в наступних виданнях посібника. А до моменту включення твоїх доповнень і пропозицій у текст усі вони будуть викладені на вебсайті видання в розділі «Дискусія». Творімо інтелектуальний продукт разом!

<https://internationalcybersecuritybook.wordpress.com>

1. Де витоки кіберзагроз?

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 у створенні, зберіганні та поширенні контенту, дає змогу краще реалізувати персональний потенціал. З одного боку, це нові перспективи для підприємництва й розвитку громадянського суспільства, а з іншого – спокуса для потенційних злочинців, терористів і політиків, котрі мислять категоріями війн та конфліктів. Кіберпростір дає кращі можливості для розвитку особистості, бізнес-проектів і суспільного прогресу загалом. Але в цих умовах також загострюється конкуренція серед учасників ринку й на міжнародній арені.

Період становлення моделі суспільних відносин, заснованої на експлуатації переваг глобальної мережі, знаменував собою початок XXI ст. Його

характерними рисами стали як стрімкі господарські та 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.

2. Інформаційна безпека чи кібербезпека?

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 та міжнародної безпеки. Такий підхід характерний для представників наукових кіл, що репрезентують як країни з розвинутою демократією (А. Вендт¹, Р. Кьохан і Дж. Най²), так і ті, що відстоюють авторитарний підхід до проблеми інформаційної безпеки (наприклад О. Зінов'єва³). Але відмінності є й вони суттєві. Наприклад, у західному академічному дискурсі переважно використовується термін «кібербезпека», визнається наявність терористичних, злочинних загроз та акцентується наявність загроз воєнного характеру винятково в галузі технічних засобів впливу, заперечуючи наявність політико-ідеологічного компонента (А. Венгер⁴, Г. Джакомелло⁵, М. Хансен⁶, Е. Тік-Рінгас⁷ й ін.). Репрезентанти іншої думки, переважно російські автори, натомість використовують термін «інформаційна безпека», виходячи з концепції чотирьох головних загроз міжнародній і

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

² Keohane R., Nye J. Power and interdependence in the information age. *Foreign affairs*. 1998. 83. P. 81–94.

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

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

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

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

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

національній безпеці в інформаційній сфері, – військової, терористичної, злочинної та загрози порушення громадського порядку й стабільності через вплив на громадську думку в державі (М. Кучерявий⁸, А. Смирнов⁹, Д. Швець¹⁰ та ін.).

3. Які є наукові підходи до проблеми управління інтернетом?

У концепціях управління інтернетом спостерігаємо помітну дихотомію, що відображається в працях науковців із різних країн. Тут також виокремлюються особливим поглядом саме представники російських дослідницьких кіл, які, вочевидь, прямують 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. Бикова¹¹, М. Якушева¹² та праці таких авторів, як І. Курбалія¹³, Т. Бальзак і М. Данн-Кавелті¹⁴, Д. Маклін¹⁵, Д. Хоффман¹⁶).

⁸ Кучерявий М. М. Глобальное информационное общество и проблемы безопасности. *Власть. Общественно-политический журнал*. 2013. № 9 (сентябрь). С. 89–92.

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

¹⁰ Швец Д. Ю. Информационная безопасность Российской Федерации в современных международных отношениях: дис. ... канд. социол. наук: Москва: МГИМО (У) МИД России, 2005. 153 с.

¹¹ Быков А. И. Управление Интернетом как одна из проблем современных международных отношений. *Политэкс*. 2008.

¹² Якушев М. В. Информационное общество и правовое регулирование: новые проблемы теории и практики. *Информационное общество*. 1999. № 1.

¹³ Kurbalija Jovan. An Introduction to Internet Governance. DiploFoundation, 2014. 206 p.

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

¹⁵ MacLean D. (ed.) (2005). *Internet Governance: A Grand Collaboration*. New York: UN ICT Task Force Series, 393 p.

¹⁶ Hofmann J. *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>

4. Які основні підходи до проблеми інформаційної безпеки з погляду міжнародного права?

Зважаючи на характер кіберзагроз, із позиції країн Заходу концептуально проблема кіберзагроз в аспекті міжнародного права опрацьована у виданнях «Талліннський посібник¹⁷» і «Талліннський посібник 2.0¹⁸», підготовлених Центром дослідження та моніторингу кіберзагроз НАТО. Головним у цих публікаціях є прийняття концепції застосування у сфері кібербезпеки чинного правового доробку (детальніше це розглянуто в розділі 2 посібника). Існують суттєві відмінності в позиціях науковців, які 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, у той час як інші виступають за необхідність вироблення правил застосування вже наявних норм. До перших належать майже винятково російські автори (що збігається в часі з періодами активної діяльності Росії в цьому напрямі на рівні ООН – у середині 2000-х рр., початок роботи UN GGE (О. Крутських¹⁹) й у наступні роки (А. Коротков²⁰, А. Федоров²¹)). А іншу групу репрезентують представники країн Заходу, причому впродовж тривалого часу (пор. наприклад, Л. Грінберг, С. Гудман, К. Су Ху²² (кінець 1990-х рр.) і Дж. Коссефф²³ (2017) та ін.). Той, хто вивчає проблему безпеки кіберпростору, може дотримуватися домінуючої в репрезентантів країн Заходу позиції,

¹⁷ Schmitt M. (ed.). Tallinn Manual on the International Law Applicable to Cyber Warfare. New York: Cambridge University Press, 2013. 282 p.

¹⁸ Schmitt M. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. New York: Cambridge University Press, 2017. 638 p.

¹⁹ Крутских А. В. К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы*. 2007. № 1(5). С. 28–37.

²⁰ Коротков А. В., Зиновьева Е. С. Безопасность критических информационных инфраструктур в международном гуманитарном праве. *Вестник МГИМО-Университета*. 2011. № 4. С. 154–162.

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

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

²³ Kosseff J. *Cybersecurity Law*. Wiley, 2017.

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. Фаррелл²⁴, М. Фіннемор²⁵, С. Дж. Шаклфед²⁶.

5. Як по-різному розглядають інформаційні загрози воєнного характеру представники країн Заходу та Росії?

Проблематика загроз воєнного характеру в інформаційній сфері глибоко досліджена в низці праць, серед яких найбільш відомими є роботи М. Лібіцкі²⁷, Р. Моландера²⁸, А. Шафранські²⁹, що побачили світ ще на межі століть. Але є й сучасні книги західних авторів, що стосуються розробки окремих питань із цієї сфери, наприклад діяльності Росії та Китаю в цій сфері (наприклад Д. Вонтр³⁰). Потрібно відзначити, що для країн Заходу характерна суто утилітарна концепція використання кіберпростору у воєнно-політичному контексті. Натомість російські автори наполягають на концепції «інформаційних війн» у найширшому сенсі (С. Расторгуєв³¹, А. Манойло³²). У змісті цієї книги детально презентовано практичні аспекти зазначених підходів.

²⁴ Farrell, H. *Promoting Norms for Cyberspace*. New York: Council on Foreign Relations, 2015.

²⁵ Finnemore M. *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, 2011. Pp. 89–101.

²⁶ Shackelford, S. J. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge University Press, 2014.

²⁷ Libicki M. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.

²⁸ Molander R., Riddile A., Wilson P. *Strategic Information Warfare: A New Face of War*. CA: RAND Corporation, 1996. 115 p.

²⁹ Szafranski R. A Theory of Information Warfare: Preparing for 2020. *Airpower Journal*. 1995. 1.

³⁰ Ventre Daniel. *Information Warfare*. Wiley, 2016.

³¹ Расторгуєв С. П. Введение в формальную теорию информационной войны. Вузовская книга, 2016.

³² Манойло А. В. Информационные войны и психологические операции. Руководство к действию. Москва: Горячая Линия – Телеком, 2022.

6. Яких позицій щодо проблем інформаційної безпеки дотримуються українські науковці?

Серед українських науковців немає однастайності в трактуванні проблем інформаційної (кібер) безпеки в аспекті «демократичного» або «авторитарного» дискурсів, хоча до останнього часу переважали обґрунтування «сильної» позиції держави в питаннях інформаційної безпеки й «інформаційного суверенітету» (О. Солодка³³), 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 домену в міжнародному праві щодо інформаційно-безпекових питань (В. Настюк і В. Белєвцева³⁴, О. Кісілевич-Чорнойван³⁵), позитивного оцінювання відповідних російських ініціатив на рівні ООН у контексті «режиму міжнародної інформаційної безпеки» (О. Фролова^{36, 37}). Сучасні публікації науковців, що досліджують цю сферу, частіше розкривають реальний стан справ у балансуванні підходів основних акторів, країн і міжнародних організацій, до політики інформаційної безпеки

³³ Солодка О. М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. 2020. № 1(32). URL: <http://il.ippi.org.ua/article/view/200311>

³⁴ Настюк В. Я., Белєвцева В. В. Правові засади міжнародного співробітництва щодо протидії інформаційним правопорушенням. *Правова інформатика*. 2014. № 2(42). URL: <http://ippi.org.ua/sites/default/files/14nvypip.pdf>

³⁵ Кісілевич-Чорнойван О. М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика*. 2009. № 8. С. 11–18. URL: http://nbuv.gov.ua/UJRN/utp_2009_8_2

³⁶ Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. *Електронне видання Інституту міжнародних відносин «Міжнародні відносини. Серія: Політичні науки»*. 2018. №18.

³⁷ Фролова О. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. *Вісник Львівського університету. Серія: Міжнародні відносини*. 2019. Вип. 46. С. 123–136. URL: http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_13

(М. Копійка³⁸, Ю. Романчук³⁹, Є. Макаренко, М. Рижков, М. Ожеван та ін.⁴⁰). Також сьогодні потрібно враховувати зовнішньополітичний досвід України щодо співпраці зі стратегічними партнерами, що відображено в документах стратегічного планування й діяльності на головних міжнародних майданчиках.

³⁸ Корііка, М. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя*. 2020. 1. С. 102–109. URL: <https://jpl.donnu.edu.ua/article/view/7967/7967>

³⁹ Романчук Ю. В. *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, 2009. 20 с.

⁴⁰ Макаренко Є. А. [та ін.]. *Міжнародна інформаційна безпека: теорія і практика*: підручник / Макаренко Є. А., Рижков М. М., Ожеван М. А., Кучмій О. П., Фролова О. М. Київ: Центр вільної преси, 2016. 418 с.

КІБЕРПРОСТІР: ЗАГРОЗИ Й КОНЦЕПЦІЇ БЕЗПЕКИ

Масштаби кіберзагроз

7. Як сучасні ринкові процеси й розвиток інтернету впливають на виникнення потенційних кіберзагроз?

Сьогодні, у третьому десятилітті ХХІ ст., інформаційне суспільство – це реальність, 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. Й у 2019 р., за даними Міжнародного телекомунікаційного союзу (ITU), кількість користувачів інтернету перевищила 4 млрд, що становить 51 % від усього населення Землі⁴¹. До 2030 р. світ досягне показника 7,5 млрд користувачів глобальної мережі. «Інтернетизація» ґрунтується на впровадженні популярних форматів і засобів обробки інформації та 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 становить інформація – від невеликої дещиці у вигляді штрихового коду GS1 для сканування й обробки в системах рітейлу до майже ста відсотків у цифрових послугах, передаванні

⁴¹ ITU estimates that at the end of 2019, a bit more than 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>

даних, мультимедійному контенті для комерційного використання. Обсяг світового ринку послуг, що постачаються цифровим способом, у 2019 р. становив 3 192 586 млн дол. США, що у 2,65 раза більше в порівнянні з 2005 р.⁴². Світовий ринок ІКТ-послуг за той самий час зріс у 2,55 раза й становив у 2019 р. 635 734 млн дол. США⁴³.

Для такого динамічного ринку характерні просторова неоднорідність і неузгодженість підходів та засобів регулювання – від м'якого спрямування його операторів у США і Європейському Союзі до тотальних обмежень у Китаї й Росії. Властивою йому рисою є поява та 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 VUCA⁴⁴), зокрема процесів на інформаційному ринку, провокують інтересантів із різними мотивами, насамперед економічними й політичними. А їхні методи й засоби не завжди відповідають правовим нормам.

8. Про що свідчить зростання витрат на кібербезпеку?

Про випереджаючі темпи розвитку кіберзлочинності опосередковано свідчить зростання світового ринку кібербезпеки, який у 2004 р. оцінювався в 3,5 млрд доларів, у 2011 – у 64, у 2015 – у 78, а у 2017 р. – уже у 120 млрд (приріст

⁴² UNCTADSTAT. International trade in digitally-deliverable services, value, shares and growth, annual. URL:

<https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=158358>)

⁴³ UNCTADSTAT. International trade in ICT services, value, shares and growth, annual.

URL: <https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=158359>

⁴⁴ 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>

у більш як 34 рази)⁴⁵. І ця динаміка стає все виразнішою. У 2020 р. обсяг світового ринку кібербезпеки становив 162,5 млрд дол. із перспективою зростання до понад 418 млрд у 2028⁴⁶, що відповідає сукупному середньорічному темпу приросту 12,5 %, і більш як у 10 разів перевищує темпи приросту ринків ІКТ та послуг, що постачаються цифровим способом.

Таке швидке зростання витрат на кібербезпеку – відповідь на все більшу загрозу кіберзлочинності, яка у 2021 р. оцінювалась у близько 6 трлн дол. США, збільшившись удвічі з 2015 р., а до 2025 р. досягне 10,3 трлн дол. за рік, що більше за збитки, заподіяні стихійними лихами, та перевищить масштаби глобальної торгівлі всіма основними незаконними наркотиками разом⁴⁷. Мільярдер і меценат Уоррен Баффет називає кіберзлочинність проблемою номер один для людства, а кібератаки – більшою загрозою, ніж ядерна зброя⁴⁸. Сьогодні кібератака може потенційно вивести з ладу інформаційну систему компанії, економіку міста чи цілої країни.

9. У чому проявляються новітні кіберзагрози?

За останні роки відбулися наймасштабніші в історії кібератаки. Кіберзагрози стали ще більш актуальними з початком пандемії SARS-CoV-2 у 2020 р. у зв'язку з масовою перебудовою комунікацій у всіх сферах суспільного життя й суттєвим збільшенням попиту на цифрові та ІТ-послуги. 2020 р. був рекордним за кількістю кібернападів й обсягом утрачених даних. Зростає також

⁴⁵ Ross Alec. Want job security? Try online security. *Wired*. 25.04.2016. URL: <https://www.wired.co.uk/article/job-security-cybersecurity-alec-ross>

⁴⁶ 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>

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

⁴⁸ Oyedele Akin. BUFFETT: This is 'the number one problem with mankind'. *INSIDER*. 2017. May 6, 2017. URL: <https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5>

складність кіберзагроз, що пояснюється застосуванням нових технологій, таких як машинне навчання й штучний інтелект, а також посиленням тактичної співпраці між хакерськими групами та державними акторами. Фіксується різке збільшення масштабів активності зловмисних груп, що фінансуються державами й організованою злочинністю⁴⁹. Безпосередніми наслідками кіберзлочинності є пошкодження та знищення даних, викрадення грошей, утрата продуктивності, крадіжка інтелектуальної власності й персональних та фінансових даних, шахрайство, загроза бізнес-комунікаціям і діловій репутації й ін.

У травні 2021 р. через атаку шкідливого програмного забезпечення зупинено роботу найбільшої американської трубопровідної системи Colonial Pipeline, у результаті чого президент США Джозеф Байден оголосив надзвичайний стан, а компанія заплатила хакерам 4,4 млн дол. у криптовалюти за відновлення роботи. Імовірно, атаку проведено хакерською групою DarkSide, з приводу чого Байден заявив, що хоча не було доказів того, що російський уряд відповідальний за напад, наявні дані про те, що група DarkSide розміщується в Росії й що російська влада «має певну відповідальність за це»⁵⁰.

Кіберзлочинність

10. Що таке «кіберзлочинність»?

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 й/або яке визнано злочином міжнародними договорами України. Зі свого боку, кіберпростором вважається

⁴⁹ Morgan Steve. 2021 Report: Cyberwarfare in the C-Suite, Cybersecurity Ventures. 2021. URL: <https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf>

⁵⁰ «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>

«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 із використанням мережі “Інтернет” та/або інших глобальних мереж передачі даних»⁵¹. Натомість Конвенція Ради Європи про кіберзлочинність («Будапештська конвенція»), прийнята у 2001 р., яку Україна ратифікувала у 2005 р., не містить прямого визначення кіберзлочинності, але встановлює певні стандарти для держав-учасниць, зокрема у сфері матеріального кримінального права впроваджено поділ на ⁵² : 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, у документі представлено відповідні стандарти у сферах процедурного права та юрисдикції. Але одним із головних досягнень Конвенції стало встановлення порядку міжнародного співробітництва з метою розслідування або переслідування кримінальних правопорушень, пов'язаних із комп'ютерними системами й даними або з метою збирання доказів в електронній формі, котрі стосуються кримінальних правопорушень. Загалом Будапештську конвенцію позитивно сприйнято у світі, але окремі держави вже понад двадцять років протидіють її утвердженню як глобального стандарту, що пов'язано з особливостями їхніх концепцій інформаційної безпеки.

⁵¹ 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>

⁵² Конвенція про кіберзлочинність. Офіційний переклад. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

11. Чи можуть кібернападники мати політичні цілі? Чи відомі Вам кібератаки такого виду?

Окрім суто економічних цілей, кібернападники можуть мати й політичні, атакуючи ресурси політичних партій та об'єкти критичної інфраструктури під проголошення політичних вимог або декларацій. За допомогою таких атак роблять також спроби впливу на перебіг демократичних процесів, які мають найбільше значення. Вплив такого рівня мала кібератака на Національний комітет Демократичної партії США, про яку стало відомо в червні 2016 р. Інформаційну систему комітету зламали два угруповання російських хакерів – *Cozy Bear* і *Fancy Bear*, котрі викрали скриньки електронної пошти, а також компромат, зібраний на конкурента демократів на виборах президента – Дональда Трампа. Згодом викрадені матеріали використано в передвиборчій боротьбі, зокрема опубліковано на сайті організації *Вікілікс*, засновник якої, Джуліан Ассанж, визнав, що цим витоком намагався зашкодити претендентці від Демократичної партії Гіларі Клінтон виграти вибори⁵³. У підсумку переможцем виборів став, імовірно, 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 шести російських високопосадовців, причетних до хакерської атаки на комітет Демократичної партії⁵⁴. У липні 2021 р. ті самі хакерські об'єднання атакували сервери Республіканської партії США⁵⁵.

⁵³ CHARLIE SAVAGE. Assange. Avowed Foe of Clinton, Timed Email Release for Democratic Convention. *New York Times*. July 26. 2016. URL: https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html?_r=0

⁵⁴ Aruna Viswanatha, Del Quentin Wilber. U.S. Prosecutors Consider Charging Russian Officials in DNC Hacking Case. *The Wall Street Journal*. 2.11.2017. URL: <https://www.wsj.com/articles/prosecutors-consider-bringing-charges-in-dnc-hacking-case-1509618203>

⁵⁵ Turton Williams, Jacobs Jennifer. 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>

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 у США, зокрема Міністерство фінансів, Національне управління з телекомунікацій та інформації, Міністерство торгівлі, Міністерство внутрішньої безпеки. Існують підозри також у 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 Росії⁵⁶.

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 таким чином помстилися за політику санкцій проти Росії, зробили спробу запобігти жорстким санкціям проти Білорусі та її очільника Олександра Лукашенка⁵⁷. Російські хакери неодноразово атакували об'єкти німецької

⁵⁶ Nakashima Ellen, Timberg Craig. 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

⁵⁷ Tiede Peter. 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>

критичної інфраструктури. Зламували інформаційні системи Бундестагу й викрадали дані про політиків.

У січні та лютому 2022 р. здійснено масштабні кібератаки на вебсайти державних установ України й банківські інституції. Це передувало заздалегідь спланованій збройній агресії Росії проти України.

Кібертероризм

12. Що таке «кібертероризм»? У чому полягають відмінності в трактуванні цього поняття?

Є достатньо підстав стверджувати, що суттєво зростають 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»⁵⁸. Американське Федеральне бюро розслідувань (ФБР) подає 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»⁵⁹. 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.

⁵⁸ Centre of Excellence Defence Against Terrorism, ed. *Responses to Cyber Terrorism*. 2008. NATO science for peace and security series. Sub-series E: Human and societal dynamics. Amsterdam: IOS Press.

⁵⁹ Terrorism 2002–2005. U.S. Department of Justice. Federal Bureau of Investigation. URL: <https://www.fbi.gov/stats-services/publications/terrorism-2002-2005>

У праці «Кібервійна й кібертероризм» (ред. Л. Янчевскі й А. Коларик) наведено таке визначення: «Кібертероризм – це політично мотивовані атаки, що здійснюються субнаціональними групами або таємними агентами, або окремими індивідами проти інформаційних і комп'ютерних систем, комп'ютерних програм чи даних, результатом яких є насильство проти некомбатантів»⁶⁰. Це визначення містить два ключові компоненти, котрі дають змогу відокремити кібертероризм від інших форм кіберзлочинів, – доведену політичну мотивацію й трактування з погляду 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 котрим розуміємо «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 під час виконання політичних, економічних або соціальних завдань»⁶¹. Помітна відмінність у російському підході в порівнянні зі сприйняттям кібертероризму в демократичних країнах. Якщо на Заході трактують кібертероризм як загрозу інформаційним системам, передусім пов'язаним із критичною інфраструктурою, то в Росії його розглядають серед комплексних загроз особі, суспільству й, що важливо, державі.

Такого підходу дотримується також китайська влада, здійснюючи контроль інтернету через державну систему «Золотий щит». Із 2006 р. будь-який інтернет-

⁶⁰ Janczewski Lech J., Colarik Andrew M. (eds.). *Cyber Warfare and Cyber Terrorism*. 2008. Hershey, PA. Information Science Reference. P. 13.

⁶¹ Иванов Станислав, Томилов Олег. Кибертероризм: угроза национальной и международной безопасности. *ИА «Оружие России»*. 14.03.2013. URL: <https://bit.ly/2UFELJ6>

користувач, котрий перебуває 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 та також повинна перешкоджати формуванню антисоціальних установок у користувачів інтернету. Але водночас така система дає владі широкі можливості для контролю й суттєво обмежує свободу інформації.

13. Які є прояви кібертероризму?

Кібертероризм має два основні прояви – це, по-перше, застосування специфічних методів і засобів впливу на критичну інфраструктуру й інформаційні системи для їх виведення з 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 йдеться про «звичайний» тероризм за допомогою сучасних ІКТ і рішень, таких як соціальні мережі, даркнет.

Також як окремий випадок можемо розглядати використання кіберзлочинних дій для «звичайного» тероризму. Саме на цій основі у 2016 р. висунуто перше в історії США звинувачення в кібертероризмі – Ардіту Ферізі – у тому, що він зламав військовий вебсайт, викрав імена, адреси й іншу особисту інформацію державного значення⁶², хоча випадки використання інформаційних технологій під час здійснення терористичних актів відомі давно. Рамзі Юзеф, який організував атаки Всесвітнього торгового центру в Нью-Йорку 11 вересня

⁶² Blake Andrew. 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/>

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 насправді встановити реальних організаторів і замовників терористичних кібератак складно. Не виключено, що серед них можуть бути кола, близькі до урядів окремих держав.

Воєнні загрози, пов'язані з інформаційними впливами

14. Які є види інформаційних загроз воєнного характеру?

Окрім розглянутих вище кіберзлочинності й кібертероризму, можемо виокремити також інші сфери загроз, пов'язаних з інформаційною діяльністю та кіберпростором, зокрема пов'язану з воєнними загрозами. Причому потрібно виокремлювати два різні аспекти загроз такого виду. По-перше, це загрози інформаційно-технічного характеру, явно пов'язані із силовим протиборством, де, щоправда, окрім типових для війн впливів кінетичного характеру, також можна простежити 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 здійснюватися 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 набув розвитку в часи загострення протистоянь геополітичного масштабу. Це спостерігали, наприклад, у період «холодної війни» між СРСР і

США, а також яскраво проявляється сьогодні в постаті «війни нового покоління»⁶³, котру Росія веде проти України.

15. У чому суть основних позицій держав із приводу міжнародно-правового регулювання інформаційної (кібер) безпеки?

Мас-медійні й соціально-медійні стратегічні комунікації здійснюються переважно в рамках правового поля та зазвичай на умовах вільної конкуренції, як-от діяльність російських телевізійних медіапроектів *RT* і *Sputnik* або активність спонсорованих російськими державними фондами суб'єктів у громадській сфері в різних країнах світу. Цілеспрямований тривалий інформаційний вплив може створювати потенційні загрози для соціально-політичних процесів і явищ методами пропаганди, дезінформації, постправди, але їм складно протиставити конкретні засоби, не ризикуючи порушенням свободи слова. Натомість більш явні загрозливі інформаційні впливи, котрі піддаються ідентифікації, можуть мати наслідком застосування щодо їхніх виконавців, учасників чи ініціаторів певних легальних інструментів і засобів протидії. Тому сьогодні спостерігаємо розділення позицій із приводу міжнародно-правового регулювання інформаційної (кібер) безпеки. Одна думка полягає в можливості й необхідності застосування наявних правових норм та підходів, а друга – у потребі вироблення спеціального правового режиму щодо цієї сфери. Імовірно, прихильники першої концепції воліють легально забезпечити себе від усіх наявних 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, постправда, дезінформація й маніпуляція. А послідовниками цього

⁶³ Bowman Andrew S. Russian Armed Forces: Military Doctrine and Strategy (PDF). *Congressional Research Service*. 20 August 2020. No. IF11625. URL: <https://sgp.fas.org/crs/row/IF11625.pdf>

підходу, звісно, є ті, хто вже практикує ці речі та почувається у виграшній позиції перед своїми конкурентами.

16. Чи інформація й програмне забезпечення можуть безпосередньо спричиняти руйнування або пошкодження фізичних об'єктів і завдавати шкоди людям? Поясніть це з погляду міжнародних відносин.

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

Із погляду використання кіберпростору задля здійснення силового впливу потрібно враховувати, що інформація чи програмне забезпечення безпосередньо не можуть спричинити 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 широковідомі приклади застосування інструментів і засобів шкідливого кібервпливу 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 впливом цієї програми у 2010 р. отримали неадекватні керуючі сигнали й зазнали фізичного руйнування газові центрифуги

для відділення ядерного матеріалу в Ірані⁶⁴. Це була перша масштабна кібератака на фізичну інфраструктуру, що призвела до важливих наслідків і в політичному плані, вплинувши на реалізацію ядерної програми Ірану. Про спеціальну розробку Stuxnet як кіберзброї свідчать його прецизійне цільове спрямування й вплив на пристрої моніторингу з метою маскуванню від обслуговуючого персоналу. Були припущення, що його розроблено в рамках спецоперації відповідних служб Ізраїлю та США⁶⁵.

17. Чи є підстави трактувати вплив кіберзасобами з погляду міжнародного гуманітарного права?

Уже відомі випадки застосування кінетичної зброї проти кіберзасобів, що призвело до руйнування інфраструктури й загибелі людей, наприклад коли в травні 2019 р. Сили оборони Ізраїлю зруйнували будівлю, пов'язану з триваючою кібератакою⁶⁶. Із 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 кібероперативники ХАМАС»⁶⁷.

Як бачимо, впливи кіберзасобами можуть бути пов'язані з фізичним пошкодженням і руйнуванням певних об'єктів та потенційно – із 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 важливі

⁶⁴ Kelley Michael B. 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>

⁶⁵ Broad William J., Markoff John, Sanger David E. 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

⁶⁶ Newman Lily Hay. 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/>

⁶⁷ @IDF. URL: <https://twitter.com/IDF/status/1125066395010699264>

саме стратегічні питання, сформульовані в процесі розробки державами концепцій інформаційної безпеки.

Інформаційне протиборство

18. Що таке «інформаційна війна»? А «кібервійна»?

Існують різні підходи до трактування інформаційних- і кібернападів. Поширеним є вживання термінів «інформаційна війна» й «кібервійна», що характерно також і для мас-медійного дискурсу. У журналістській практиці та популярному сегменті соціальних комунікацій терміни «кібернапад» або «кібервійна» вживаються, коли мають на увазі незаконний збір інформації чи інші кіберзлочини, а «інформаційна війна» – щодо пропагандистського впливу телеканалів і спільнот у соціальних мережах. Звісно, зв'язки з громадськістю, публічна дипломатія й психологічні операції щодо 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 у 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»⁶⁸.

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.

19. У чому суть концепції інформаційного протиборства (Information Warfare)?

У звіті «Стратегічне інформаційне протиборство. Нове обличчя війни» американської «фабрики думки» RAND (1996 р.) уперше 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»⁶⁹. А вже за два роки по тому вийшов новий звіт «Розвиток стратегічного інформаційного протиборства», у якому наведено поділ інформаційного протиборства на перше та 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 низку інших областей (передусім

⁶⁸ СОГЛАШЕНИЕ между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 2012. URL: <https://docs.cntd.ru/document/902289626>

⁶⁹ Molander Roger C., Riddile Andrew, Wilson Peter A. Strategic Information Warfare. A New Face of War. RAND. 1996. MR-661-OSD. URL: https://www.rand.org/pubs/monograph_reports/MR661.html

економіку) та триває довгий час: тижні, місяці й роки»⁷⁰. У 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 заходи, ужиті для впливу на інформацію й інформаційні системи супротивника під час захисту власної інформації та інформаційних систем, які застосовуються в усьому діапазоні військових операцій і на всіх рівнях війни. А «інформаційне протиборство» («information warfare») – це ІО, проведена під час кризи або конфлікту (уключаючи війну) для досягнення або просування конкретних цілей над конкретним противником або противниками. Тобто американські військові чітко визначають можливість застосування інформаційних засобів у рамках, охоплених міжнародним гуманітарним правом.

20. Які зміни відбуваються в західній концепції стратегічних інформаційних упливів?

Загалом простежено певну еволюцію в західній концепції інформаційних упливів зі стратегічною метою. У період становлення сучасної моделі інформаційного суспільства й кіберпростору, у 1990-х рр. ХХ ст., військові доктрини містили поняття «інформаційне протиборство», яке включало не лише кібернетичні та спеціальні психологічні засоби, а й певну ширшу сферу 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 військовими й цивільними засобами). Натомість уже в спільній публікації родів військ США «Інформаційні операції» від 2006 р.⁷¹

⁷⁰ Molander Roger C., Wilson Peter A., Mussington B. David, Mesic Richard. Strategic Information Warfare Rising. RAND. 1998. MR-964-OSD. URL: https://www.rand.org/pubs/monograph_reports/MR964.html

⁷¹ Joint Publication 3–13, Information Operations. 13 February 2006. URL: https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf

(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 із суто військового погляду: електронне протиборство, операції в комп'ютерній мережі, психологічні операції, безпека операцій та оперативне маскування й пов'язані з ними допоміжні й супутні можливості»⁷². Також у цьому документі пов'язано оборонну підтримку та публічну дипломатію й указано на адаптацію державних справ і цивільних військових операцій, відповідно до можливостей ІО, додано опис інформаційного середовища та обговорено його стосунок до ІО й інших військових операцій, встановлено взаємозв'язок ІО та стратегічних комунікацій.

Щодо НАТО країни-члени організації застосовують свої внутрішні визначення інформаційного протиборства, але вже у звіті «Information Warfare and International Security» Комітету Альянсу з науки і технологій, прийнятому в 1999 р., термін Information Warfare пояснюється як «наступальне й оборонне використання інформації та інформаційних систем для застосування, пошкодження або знищення інформації й інформаційних систем супротивника під час захисту своїх власних. Такі дії виконуються для досягнення військової або економічної переваги над супротивником»⁷³. 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 цьому словнику міститься термін *psychological operations* – психологічні операції (здійснення

⁷² Там само.

⁷³ NATO, Information Warfare and International Security. NATO Parliamentary Assembly Science and Technology Committee, Brussels, 6th October. 1999.

впливу на установки й поведінку іноземних цільових груп через різні засоби інформаційного протиборства)⁷⁴.

Щодо актуального стану справ, то розглянута вище концепція інформаційних операцій США загалом застосовується й у НАТО. У результаті розширення застосування «м'якої сили» для виконання політичних і військових завдань під час урегулювання кризових ситуацій у різних регіонах світу продемонстровано високу ефективність цілеспрямованого інформаційно-психологічного впливу на активних й 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. засвідчили, що масоване використання інформаційних ресурсів дає змогу впливати на громадську думку й спричиняти революційні зміни в суспільствах.

Відтак у цей період у НАТО формується сучасна концепція стратегічних комунікацій (Strategic Communications), яка, подібно до розглянутої вище американської доктрини, передбачає перехід від відокремленого застосування військових і цивільних інформаційно-пропагандистських структур до координації їхньої діяльності під час підготовки й проведення операцій із врегулювання криз. Стратегічні комунікації розглядаються як поєднання публічної дипломатії, цивільних і військових зв'язків із громадськістю та інформаційних операцій і психологічних операцій на підтримку політики Альянсу, його операцій, діяльності й для досягнення стратегічних цілей НАТО. Таке стратегічне протиборство спроможне 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

⁷⁴ 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](https://www.nato.int/docu/other/ru/2006/pdf/SOFglossary(R-E).pdf)

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 Альянсу⁷⁵.

21. Якого підходу у військовій сфері інформаційної- та кібербезпеки дотримується Україна?

Американський і загалом євроатлантичний підхід полягає в розділенні військових та цивільних інформаційних впливів, 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. З 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 використовувався термін «стратегічні комунікації» відповідно до стандарту НАТО (скоординоване й належне застосування комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних і психологічних операцій, заходів, спрямованих на просування цілей держави)⁷⁶. Це визначення було повторене у прийнятій у 2021 р. Стратегії інформаційної безпеки. А створення ефективної системи стратегічних комунікацій указана серед

⁷⁵ 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

⁷⁶ 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>

стратегічних цілей держави ⁷⁷. Також створення системи стратегічних комунікацій оголошено серед основних напрямів зовнішньої й внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки (Стратегія національної безпеки України)⁷⁸. Відповідно до прийнятої у 2021 р. оновленої воєнної доктрини, узятю курс на запровадження об'єднаного керівництва з підготовки та ведення всеохопної 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 ⁷⁹. Отже, в Україні загалом прийнято західний підхід із виділенням військових і цивільних компонентів у єдиній системі стратегічних комунікацій.

22. Як взаємопов'язані військові й невійськові впливи в російській (східній) моделі інформаційної безпеки?

На відміну від західної моделі, східна тяжіє до втручання влади в усі сфери інформаційного суспільства, у тому числі в аспекті воєнно-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 медіаканалами й створення спеціалізованих державних пропагандистських майданчиків, які працюють у координації з військовим керівництвом.

⁷⁷ Стратегія інформаційної безпеки. Затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069>

⁷⁸ 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>

⁷⁹ 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 терміна «інформаційні війни», який містився в доктрині інформаційної безпеки РФ 2000 р. й відсутній у документі з аналогічною назвою від 2016 р.⁸⁰. Оновлена доктрина, утім, також орієнтує на протидію певним ворогам, серед яких «окремі держави», «окремі / різні організації», або «окремі особи», що здійснюють «інформаційний вплив 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 та порушення територіальної цілісності» й має протидіяти зовнішньому інформаційному впливу на молодь Росії, який відбувається «з метою розмивання традиційних російських духовно-моральних цінностей»⁸¹.

У документі використовується термін «інформаційне протиборство», причому як його суб'єкти вказані, окрім збройних сил, також «інші війська, військові формування й органи». Тобто в порівнянні із західною моделлю інформаційної безпеки Росія, по суті, дотримується концепції «інформаційних війн», де інформаційне протиборство легалізується не лише у військовій, але й у цивільній сфері.

Загалом російська (авторитарна) модель інформаційної безпеки не розділяє військові й невійськові впливи, а отже, по своїй суті непридатна для адаптації до чинних міжнародно-правових норм і вимагає формування окремого режиму на кшталт «міжнародної інформаційної безпеки» (про що йдеться в розділі 2 цієї книги). Очевидно, цим пояснюється, що серед загроз інформаційній безпеці, виділених у згаданій вище російській доктрині, є «відсутність міжнародно-

⁸⁰ 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>

⁸¹ Там само.

правових норм, що регулюють міждержавні відносини в інформаційному просторі, а також механізмів і процедур їх застосування», що «ускладнює формування системи міжнародної інформаційної безпеки»⁸².

Потрібно відзначити й те, що поняття «інформаційного протиборства», зокрема розвиток його сил і засобів, указано серед завдань Воєнної доктрини РФ⁸³. Суть інформаційного протиборства пояснено в словнику, розміщеному на вебсайті Міністерства оборони РФ як інформаційний вплив на інформаційну сферу противника (під час захисту власної), причому цей термін пов'язано з іншим – «інформаційна війна», у якій «політичні, економічні й інші цілі досягаються руйнуванням інформаційного середовища протилежної сторони й оволодінням її інформаційними ресурсами»⁸⁴.

Детально розкрито бачення воєнно-політичної сфери інформаційної безпеки в документі стратегічного значення «Концептуальні погляди на діяльність збройних сил Російської Федерації в інформаційному просторі»⁸⁵, 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 та 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,

⁸² Там само.

⁸³ Военная доктрина Российской Федерации. URL: <http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf>

⁸⁴ *Информационное противоборство*. Справочник МО РФ. URL: <https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary>

⁸⁵ Концептуальные взгляды на деятельность вооруженных сил Российской Федерации в информационном пространстве. 2011. URL: <https://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle>

використанням, зберіганням інформації, що пливає, у тому числі, і на індивідуальну й суспільну свідомість, інформаційну інфраструктуру та власне інформацію». Отже, по суті, військова стратегія РФ принципово охоплює весь цей «простір», уключаючи всю інформацію, індивідуальну й суспільну свідомість, тобто все суспільство, усю 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»⁸⁶.

Підхід російської влади до реалізації військових інструментів, із погляду інформаційної безпеки, стає ще більше зрозумілим із резюмуючого твердження в зазначеному вище документі про те, що «обороздатність Російської Федерації істотно залежить від ефективності діяльності збройних сил в інформаційному просторі й багато в чому визначається їх можливостями щодо стримування, запобігання конфліктам та їх вирішення, 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»⁸⁷.

Тобто сьогодні російська концепція політичного та військового виміру інформаційної безпеки заснована на експлуатації моделі «інформаційних війн» – комплексної сфери забезпечення політичних і геополітичних інтересів держави за допомогою військових та цивільних інформаційних- і кіберзасобів. Причому офіційно пропагується екстраполяція цієї моделі на сферу міжнародних відносин із формуванням спеціального режиму «міжнародної інформаційної безпеки», що, вочевидь, передбачає необхідність формування спеціального домену в

⁸⁶ Там само.

⁸⁷ Там само.

міжнародному праві. Натомість західна модель побудована на розвитку системи стратегічних комунікацій таким чином, що це дає змогу забезпечити відповідність чинним міжнародно-правовим нормам.

Інформаційна (кібер) безпека

23. На чому ґрунтуються демократичний та авторитарний підходи у сфері інформаційної безпеки?

Загалом є два різних бачення інформаційної безпеки з погляду держави. Назвемо їх демократичним (технократичним) й авторитарним (ідеологічним). Держави, що практикують авторитарний підхід, пропонують норми, які включають сильний урядовий контроль над інформацією, тоді як із позицій західного підходу це сприймається як загроза політичній стабільності.

Демократичне бачення, що сформувалось у США, ґрунтується на розумінні інформаційної безпеки як безпеки даних і, відповідно, інформаційних систем, котрі 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 ХХ ст. і розвивалося згідно з принципами функціонування демократичної соціально-економічної моделі. Головним завданням тут стало гарантування рівних можливостей виробництва й споживання інформації кожному індивіду.

24. Які історичні передумови сучасної концепції інформаційної безпеки в США?

Законодавство США визначає загалом дані як комерційно значущу інформацію, володіння й законне розповсюдження якої дає змогу отримати вигоду або уникнути збитків. Наприклад, отримання, зберігання, обробка та обіг персональних даних у США регулюються законодавством саме з погляду комерційної значущості вказаної категорії інформації. У 1967 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 ставить за мету забезпечення функціонування інформаційних систем задля належного функціонування виконавчої влади та її звітності перед народом. З іншого боку, влада повинна гарантувати недоторканність інформації, що належить особі, так само, як і будь-якої іншої приватної власності. Концепція свободи інформації була розвинута з прийняттям у 1974 р. Закону про конфіденційність (*The Privacy Act*), яким встановлено 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, у США свобода волевиявлення та свобода слова гарантовані першою поправкою до Конституції⁸⁸. 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. Так 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 (у тому числі й критично важливої) передавання, зберігання та обробки даних, й 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 та інформаційних систем від несанкціонованого доступу, використання, розкриття, руйнування, зміни чи знищення з метою забезпечення цілісності (захист від несанкціонованої

⁸⁸ The First amendment. Legal Information Institute. URL: http://www.law.cornell.edu/anncon/html/amdt1afrag1_user.html#amdt1a_hd4

модифікації чи знищення інформації), конфіденційності, а також доступності (забезпечення своєчасного й надійного доступу до інформації)⁸⁹. 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 це потрібно (наявність)»⁹⁰). Тобто це поняття в американській практиці зводиться лише до захисту даних і не містить такого складника, як захист від шкідливого контенту (небажаного інформаційного впливу).

25. На яких принципах ґрунтується політика Європейського Союзу у сфері інформаційної безпеки?

Політика Європейського Союзу у сфері інформаційної безпеки також ґрунтується на принципах, властивих західному підходу. Одне з перших формулювань уміщено в комюніке Європейської комісії «Мережева й інформаційна безпека: пропозиції для підходу європейської політики»⁹¹ у 2001 р. Відповідно до цього документа, «мережева й інформаційна безпека» (*Network and Information Security*) визначається як спроможність мережі або інформаційної системи протистояти на заданому рівні надійності випадковим загрозам або умисним шкідливим діям, котрі ставлять під загрозу доступність, достовірність, цілісність і конфіденційність збережених або переданих даних та пов'язаних із ними служб, доступ до яких відбувається за допомогою цих мереж або систем. Єврокомісією запропоновано такі принципові засади в політиці щодо

⁸⁹ 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>

⁹⁰ ISACA. Glossary of terms. 2008. URL: <http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf>

⁹¹ 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.

забезпечення мережевої й інформаційної безпеки: по-перше, забезпечення прикладного характеру правових норм на основі загального розуміння основних питань безпеки та спеціальних заходів щодо її забезпечення (що властиво загальному західному підходу); по-друге, 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); по-третє, потреба в доповненні ринкових механізмів політичними заходами (відображає важливість проблеми інформаційної безпеки, що розглядається на рівні комунітарної політики ЄС); по-четверте, формування європейського внутрішнього ринку інформаційно-телекомунікаційних послуг (базовий підхід у всіх галузевих і секторальних політиках ЄС).

26. Яка концепція інформаційної безпеки реалізується в Японії?

Підхід японського уряду також відповідає західній, або технократичній, моделі. У Стратегії кібербезпеки Японії, підготовленій і винесеній на обговорення у 2013 р.⁹², можна виокремити 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 та зміцнення співробітництва на основі принципів соціальної відповідальності. Відповідно до цієї стратегії, уряд повинен 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 та забезпечити освіту громадян із питань кібербезпеки.

⁹² Japan Cybersecurity Strategy. Information Security policy Council. 2013. URL: <http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf>

27. У чому суть інформаційної безпеки з позицій Росії? Як це стосується свободи слова й інформації?

Авторитарна концепція значну увагу приділяє питанню захисту держави, суспільства й особистості від негативного інформаційного контенту. Одним із перших документів, у якому сформульовано таке бачення, стала Доктрина інформаційної безпеки Російської Федерації⁹³, затверджена у вересні 2000 р. У 2016 р. прийнято нову доктрину⁹⁴, що була 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 погляду національної безпеки. Наприклад, для згаданої доктрини 2000 р. ключовими проблемами були «розкладання моральних цінностей молоді», відтік фахівців у сфері безпеки. Під інформаційною безпекою країни тоді розуміємо стан захищеності її національних інтересів в 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; популяризацію тенденцій, котрі 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 впливів.

⁹³ Доктрина информационной безопасности Российской Федерации (утверждена президентом Российской Федерации в. путиным 9 сентября 2000 г., № Пр-1895) Совет безопасности РФ.

⁹⁴ Доктрина информационной безопасности Российской Федерации Утверждена Указом президента Российской Федерации от 5 декабря 2016 г. № 646.

Авторитарний підхід не передбачає безумовного гарантування свободи слова й масової інформації, відкриваючи шлях до цензури та 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 та держави в інформаційній сфері». Той самий документ дає підстави й для суб'єктивної цензури, оскільки до загроз інформаційній безпеці країни віднесено, зокрема, такі, як «девальвація духовних цінностей, пропаганда зразків масової культури, заснованих на культурі насильства, на духовних і моральних цінностях, що суперечать цінностям, прийнятим у російському суспільстві; зниження духовного, морального й творчого потенціалу населення Росії».

28. Що таке інформаційний- і кіберсуверенітет із погляду Росії й Китаю?

Фактично йдеться про реалізацію державного контролю в інформаційній сфері, що сьогодні часто подають як «інформаційний суверенітет» або «кіберсуверенітет». Поняття «інформаційного суверенітету» не нове, воно розробляється та втілюється в практику з часів початку масового поширення інтернет-технологій у країнах, що тяжіють до авторитарного типу організації суспільства. У Китаї на державному рівні кіберсуверенітет формується, починаючи з початку 2000-х. У Росії у квітні 2014 р. Максим Кавджарадзе, член верхньої палати російського парламенту, запропонував створити повністю недоступну з-за кордону національну внутрішню мережу Росії. Тоді й з'явилася назва – «ЧебурашкаNet» на честь російського мультиплікаційного героя

Чебурашки, персонажа з відомого анімаційного фільму⁹⁵. А у 2019 р. прийнято зміни до федерального законодавства, які отримали неформальну назву «Закону про суверенний інтернет»⁹⁶. Мета закону – створення автономних систем управління інтернетом і тим самим створення можливості відокремлення російського інтранету від глобальної мережі «Інтернет».

Згідно із законом, Росія вимагає від національних постачальників послуг інтернету використовувати лише точки обміну інтернетом, затверджені російським регулятором телекомунікацій, а оператори зв'язку зобов'язані встановити державне обладнання на точках обміну трафіком для аналізу та 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 громадськості⁹⁷, що розглядає цю ініціативу як нову форму цензури. На відміну від Китаю, громадяни якого ввійшли в епоху інтернету майже в той самий час, коли уряд почав його регулювати, і звикли до такого способу життя, де інтернет є національною інтрамережею, громадяни Росії завжди мали доступ до глобальної мережі й широкого спектра контенту й послуг із будь-якої країни. Крім того, сьогодні, в порівнянні з періодом становлення масового інтернету, мережа вже міцно «вросла» в економіку, яка залежить від інтернету та безперебійного функціонування певних додатків і послуг. Нині відключення від іноземних цифрових послуг негативно вплине на національну економіку. Тому 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

⁹⁵ Канев Сергей. Чебурашка, или Хорошими делами прославиться нельзя. *Новая Газета*. 5 мая 2014.

⁹⁶ Принят закон о «суверенном интернете». *Государственная дума Федерального собрания Российской Федерации*. 16.04.2009.

⁹⁷ В Москве прошел митинг против изоляции Рунета. *РБК*. 10 марта 2019 года.

суверенітету», відображений в усіх основних законодавчих актах, прийнятих Росією у сфері інформаційної безпеки.

Крім Доктрини інформаційної безпеки, у 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»⁹⁸ й «Основи державної політики Російської Федерації в галузі міжнародної інформаційної безпеки»⁹⁹. У цьому документі вже у 2013 р. закріплювалися 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.), у ході якої активне використання соцмереж забезпечило координацію дій протестного руху.

Певною мірою авторитарний (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 лише 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»¹⁰⁰, у той час як у західній концепції суверенітет в інформаційну епоху – це заохочення глобального обміну інформацією через безпечну технологічну інфраструктуру.

У Національній стратегії розвитку інформатизації на 2006–2020 рр. Національний інформаційний консультативний комітет КНР визначає

⁹⁸ Основы государственной политики в области международной информационной безопасности на период до 2020 года.

⁹⁹ Основы государственной политики Российской Федерации в области международной информационной безопасности / Утверждены Указом президента Российской Федерации от 12 апреля 2021 г. № 213.

¹⁰⁰ Доктрина информационной безопасности Российской Федерации / Утверждена Указом президента Российской Федерации от 5 декабря 2016 г. № 646.

інформаційну безпеку як ключовий компонент системи національної безпеки, необхідний для забезпечення сталого, здорового застосування інформаційних технологій, а також для соціальної й культурної стабільності та ідеологічного розвитку.¹⁰¹

Авторитарна концепція інформаційної безпеки передбачає винятковий пріоритет держави в питаннях, що стосуються «інформаційного суверенітету». Ідеться про контроль усього, що відбувається в інформаційному полі, яке влада вважає належним до своєї юрисдикції. Прикладом такого ревного ставлення до інформації в питанні її захисту є Закон про кібербезпеку КНР, прийнятий у 2016 р.¹⁰² Закон акцентує на зборі, зберіганні й використанні персональних даних китайських громадян та інформації, що стосується національної безпеки. Такі відомості повинні зберігатись усередині країни (також і в Росії у 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 основу законів, що охоплюють цивільну сферу безпеки кіберпростору в Китаї, покладено так звану «класифікацію 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 погляду потенційних наслідків – від шкоди правам громадян, організацій, громадському порядку, до

101 2006-2020 年国家信息化发展战略 (2006–2020 Nián guójiā xīnxi 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%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>.

102 中华人民共和国网络安全法(Zhōnghuá rénmin 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

загрози національній безпеці¹⁰³. 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 та 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, у т. ч. через блокування соціальних мереж і пошукових систем. Наприклад, керівництво КНР вважає, що сама суть інформаційної безпеки полягає в уведенні обмежень на поширення небажаної інформації¹⁰⁴.

29. Що таке «мережевий нейтралітет»? Яке ставлення до нього характерне для різних політичних систем?

Демократичний підхід ґрунтується 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

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

104 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>.

комісією зв'язку США¹⁰⁵ на підставі Закону про комунікації (1934 р.), хоча й піддавався певним обмеженням у період президенства Д. Трампа. Також цей принцип присутній у більшості європейських стратегій кібербезпеки, а на рівні Європейського Союзу його закладено в стратегію Єдиного цифрового ринку ЄС¹⁰⁶ (проголошено у 2015 р.). Основні рамки для забезпечення нейтралітету мережі на території всього Європейського Союзу. Зокрема, встановлено Регламентом ЄС 2015/2120¹⁰⁷.

Країни, де домінує авторитарний підхід, не забезпечують невтручання в роботу мережі. Наприклад, у Росії на початку 2018 р. кабінет міністрів запропонував формально відмовитися від принципу мережевого нейтралітету, який і так не підтримувався в країні¹⁰⁸. Не застосовується принцип мережевого нейтралітету й у Китаї, де уряд використовує інтернет-провайдерів для перевірки та 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 сайти¹⁰⁹.

¹⁰⁵ STATEMENT OF ACTING CHAIRWOMAN ROSEWORCEL ON DEPARTMENT OF JUSTICE DECISION TO WITHDRAW LAWSUIT TO BLOCK CALIFORNIA NET NEUTRALITY LAW. URL: <https://docs.fcc.gov/public/attachments/DOC-369799A1.pdf>

¹⁰⁶ 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>

¹⁰⁷ 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>

¹⁰⁸ Правительство РФ не видит необходимости в законодательном закреплении сетевого нейтралитета. *Роскомсвобода*. 29.10.2018. URL: <https://roskomsvoboda.org/42667/>

¹⁰⁹ Hu, Henry L. «The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration». *The China Quarterly*. 2011. 207 (207). P. 523–540.

30. У чому суть відмінностей у трактуванні поняття «інформаційна безпека»?

Загалом суть відмінностей між американським і російським підходами полягає в самому трактуванні поняття «інформаційна безпека». Якщо в США виступають винятково за технічне регулювання кіберсередовища (захист комп'ютерних мереж і ресурсів) та 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.

Кібервійни й міжнародне право

31. У чому полягає проблемність застосування міжнародного права у сфері кібервоєн?

Ураховуючи 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 чинного міжнародного права у сфері інформаційних загроз, пов'язаних із військовою сферою, розглянемо зв'язок самого предмета дискусії зі сферами права на ведення війни й права під час війни (тобто міжнародного гуманітарного права, МГП).

Jus ad bellum (лат. «право на війну») стосується умов, за яких національні держави можуть удатися до війни або загалом до застосування збройної сили. Хоча історично *jus ad bellum* розуміли 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 потрібно «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 та країни НАТО) зазвичай виступають за широке визначення самооборони, відмову від монополії ООН на санкціонування військових дій і допустимість гуманітарних чи продемократичних утручань¹¹⁰. З іншого боку, 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 й значною мірою – Китаєм силового врегулювання загрозливих на думку 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», а у 2022 р. Росія заперечувала участь у війні проти України, називаючи вторгнення

¹¹⁰ Ruys Tom, Corten Olivier, Hofer Alexandra. *Use of Force in International Law*. 2018. Oxford University Press. URL: <https://books.google.com.ua/books?id=MkdiswEACAAJ&printsec=frontcover&hl=uk#v=onepage&q&f=false>

на її територію «спеціальною військовою операцією». Тобто, на переконання представників авторитарного підходу, кіберсфера – це лише простір для маніпулювання нормами міжнародно-правового регулювання, щоб, з одного боку, не допустити застосування чинних норм для обмеження їхніх протиправних дій, а з другого – щоб обмежити можливості застосування досягнень ІКТ для країн Заходу.

Росія й Китай підкреслюють важкість адаптації міжнародних правил до кіберпростору та зосередилися на просуванні «міжнародного кодексу поведінки» для кіберпростору. Натомість уряд США публічно й неодноразово заявляв, що «кібердіяльність за певних обставин може бути підставою для застосування сили в значенні Статті 2 (4) Статуту ООН та міжнародного звичаєвого права»¹¹¹.

Імовірно, виходячи саме з такої позиції, коментуючи завершення у 2017 р. роботи Групи урядових експертів ООН у сфері інформатизації й телекомунікації в контексті міжнародної безпеки (UN GGE)¹¹², представник США Мішель Маркофф зазначила, що деякі країни (маючи на увазі Росію та Китай) наполягали, що застосування основних принципів *jus ad bellum* (право початку війни) і *jus in bello* (право під час ведення війни) призведе до мілітаризації ІКТ-сфери, а не до запобігання використанню ІКТ у міжнародних конфліктах¹¹³.

Потрібно зазначити, що Росія й Китай разом із партнерами по ШОС, Таджикистаном та Узбекистаном, у 2011 й у 2015 рр. подали Генеральному секретарю ООН проєкт міжнародного Кодексу поведінки з питань інформаційної

¹¹¹ Koh Harold Hongju. International Law in Cyberspace. *Harvard International Law Journal*. 2012. 54 (December 2012).

¹¹² *детальніше про роботу зазначеної Групи урядових експертів див. у наступних розділах (питаннях) навчального посібника.

¹¹³ Markoff Michele G. 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. 2017. US Department of State, June 23, 2017. URL: <https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm>

безпеки¹¹⁴. Документ є важливим індикатором світогляду країн східного підходу щодо міжнародного регулювання кібердіяльності. Членам ООН пропонується зобов'язатися «не використовувати інформацію й комунікаційні технології, включаючи мережі, для виконання ворожої діяльності або актів агресії, або якщо вони становлять загрозу міжнародному миру й безпеці». Але не пропонується жодних указівок щодо того, як ці заборони на застосування сили застосовуватимуться в кіберконтексті.

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

32. Як співвідносяться поняття інформаційних- і кібервійн?

Проблема підходів до розуміння силового військового впливу в інформаційному/кіберпросторі має загальний характер і викликає суперечки на міжнародних майданчиках найвищого рівня. Але, окрім того, предметній сфері кіберпростору властива також низка особливостей, пов'язаних зі специфікою його організації й функціонування, які накладають відбиток на безпекові проблеми. Загалом щодо потенційно загрозливих операцій у кіберпросторі застосовують 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 та військових мереж із метою їх пошкодження, знищення чи

¹¹⁴ Правила поведення в області забезпечення міжнародної інформаційної безпеки. *Документ ООН. А/69/723/*, 13 янв. 2015.

блокування їх використання¹¹⁵. 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 за допомогою інформаційного потоку, коли такі операції в кіберпросторі реалізуються в контексті збройного конфлікту за змістом МГП¹¹⁶. Тобто поняття «кібервійна» є вузьким у порівнянні з «інформаційною війною» й «інформаційними операціями» в різних трактуваннях.

33. У чому полягає проблемність ідентифікації сторін конфлікту в умовах інформаційного протиборства з погляду міжнародного права?

Із погляду застосування міжнародного права кібервійна породжує низку проблем. Насамперед це – ідентифікація сторін конфлікту, адже в умовах інформаційного протиборства засоби враження не прив'язані до території й не мають розпізнавальних знаків, а їх національну належність можливо встановити лише за опосередкованими ознаками. Відповідно, проблематично встановити й ініціатора конфлікту, принаймні це потребуватиме значного часу. Це ж стосується також установлення суб'єкта відповідальності, – узагалі кібероперація може здійснюватись особами, що навіть не підозрюють про їх роль у конфлікті (наприклад цивільними, які працюють на певну інтернет-компанію, що, зі свого боку, виконує підряд екстериторіального замовника), тому, якщо неможливо встановити особу, організацію чи державу-замовника, таку діяльність складно ідентифікувати як операцію воєнного 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

¹¹⁵ Cyberwar. Britannica. URL: <https://www.britannica.com/topic/cyberwar>

¹¹⁶ How is the Term «Armed Conflict» Defined in International Humanitarian Law? ICRC. Opinion paper. March 2008. URL: <http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf>

практично неможливо визначити наявність конфлікту. Також важко своєчасно ідентифікувати сторону конфлікту.

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 питання. Кібердіяльність у контексті інформаційного протиборства може мати як військовий, так і невійськовий прояви, а отже, постає питання про те, чи буде вона сприйнята в ролі «збройної сили». Також, якщо інформаційний вплив і трактуватимуть як «загрозу силою», то, відповідно до ст. 2 Статуту ООН, найімовірніше, він не буде однозначно спрямованим проти «територіальної недоторканності чи політичної незалежності будь-якої держави» й вимагатиметься обґрунтування його дії будь-яким іншим чином, несумісним із цілями Об'єднаних Націй. Загроза силою, згідно зі ст. 2, трактується як така, що повинна мати примусовий характер, і потрібна чітка заява про намір застосувати силу¹¹⁷. 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 утручання в роботу систем протиповітряної оборони в ході конфлікту, то їх ідентифікація може здійснюватися за ознаками останніх. Також і у випадку 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, про що йдеться у відповіді на питання 17 у цьому навчальному посібнику.

¹¹⁷ 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.

Значно складніше ідентифікувати операцію в кіберпросторі, якщо вона є 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 впливом комп'ютерної програми. Імовірно, що комп'ютерний хробак *Stuxnet*, який у 2010 р. спричинив руйнування в центрах збагачення урану в Ірані, був спеціально розроблений із метою кібернападу, який мав суттєві політичні наслідки через підрив іранської ядерної програми. Але відкритим залишається питання про те, 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 погляду *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 за одночасної «непомітності» такого впливу. Тобто виведення з ладу, скажімо, важливого інфраструктурного чи військового об'єкта через блокування керуючих процесорів спеціальною програмою – це не те 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 в процесі оборони, відповідно до

Додаткового протоколу I до Женевських конвенцій (ст. 49), розцінюються як напади, а отже, по суті, їх інструментом можуть бути й кіберзасоби, тим більше, що це стосується «будь-яких військових дій на суші, у повітрі або на морі, які можуть завдати шкоди цивільному населенню, окремим цивільним особам або цивільним об'єктам»¹¹⁸. Проте в цьому випадку може йтися не про фізичне пошкодження таких об'єктів, а про втрату функціональності. Ще одним специфічним моментом є фактична неможливість ідентифікації осіб, які беруть участь у кібернападі (на противагу «звичайному» нападу, коли має місце ідентифікація учасників-комбатантів).

Також тим самим протоколом (ст. 51) заборонено невибіркові напади, що, зі свого боку, викликає проблему, оскільки кібероперації зазвичай реалізуються 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 водночас універсальність інтернету та 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.

34. Яка роль «Талліннського посібника» в питанні застосування міжнародного права у сфері кібервійн?

Питання щодо можливості застосування міжнародного права у сфері кібервійн стало більш актуальним після скоординованої кібератаки на комп'ютерні системи державних установ Естонії у 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

¹¹⁸ 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

НАТО вжито невідкладних заходів, зокрема проведено внутрішню оцінку кібербезпеки й інфраструктурного захисту з оприлюдненням у жовтні того самого року відповідного звіту¹¹⁹. Це стало початком розвитку політики Альянсу в галузі кіберзахисту. Уже 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 наявних норм міжнародного права, зокрема права початку війни й міжнародного гуманітарного права, у контексті кібероперацій та кібервійни. У квітні 2013 р. опубліковано перше видання так званого «Талліннського посібника» (*The Tallinn Manual on the International Law Applicable to Cyber Warfare*)¹²⁰, який противники застосування міжнародного права в кіберпросторі (найбільше – у Росії) називають набором рекомендацій щодо ведення кібервійни й обґрунтуванням застосування фізичної сили у відповідь на кібернапади¹²¹. Проте «Талліннський посібник» не є офіційним документом, а являє собою лише думку учасників робочої групи фахівців, які, зважаючи на відсутність загальновизнаних міжнародних норм із 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 та ракетному протиборстві.¹²²

«Талліннський посібник» – це науково обґрунтована відповідь на низку принципових питань у сфері інформаційної (кібер) безпеки з погляду як

¹¹⁹ 2007 cyber attacks on Estonia. URL: https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

¹²⁰ Schmitt Michael N. (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013.

¹²¹ «Таллинское руководство» о войне в интернете встревожило Россию – этот документ сам по себе опасен. *NEWSru.com*. 27.05.2013.

¹²² HPCR Manual on International Law Applicable to Air and Missile Warfare. Bern. 15 May 2009. URL: <https://reliefweb.int/attachments/1b79f010-abff-3428-9fb7-9608d80e9f1c/8B2E79FC145BFB3D492576E00021ED34-HPCR-may2009.pdf>

міжнародного співробітництва в цій сфері, так і з позиції вироблення національних підходів і політик. Насамперед автори впорядкували низку 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, розміщеної на їхній території, а також діяльності, пов'язаної з цією кіберінфраструктурою («суверенітет, яким володіє держава над територією, дає їй право контролю кіберінфраструктури та кібердіяльності на її території»). Звідси очевидний логічний висновок, що кібероперація держави, спрямована проти кіберінфраструктури, розміщеної в іншій державі, може порушити суверенітет останньої. І критерієм такого порушення є заподіяння 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 кібероперація може кваліфікуватися як «збройний напад», що провокує право особистої або колективної самооборони. А дії, які не є збройним нападом, але все ж порушують норми міжнародного права, можуть дати право державі-цілі вдаватися до контрзаходів. Країна, що стала жертвою «збройного нападу» в кіберпросторі, що спричинило людські жертви або іншу серйозну шкоду, має право відповісти за допомогою сили в кіберпросторі чи фізичному світі.

Важливим моментом є кваліфікація конфліктів, які відбуваються в кіберпросторі. Автори посібника, по-перше, фіксують їх актуальність, а по-друге

– установлюють відповідність цього феномену міжнародному поняттю «збройний конфлікт», що, відповідно, дає підстави для застосування норм МГП. Тому керівництво кіберопераціями, що призвели до жертв серед цивільного населення (або можуть спричинити таку шкоду), класифікується як воєнний злочин.

Звісно, до кібероперацій повинні застосовуватися й інші норми *jus in bello*, зокрема щодо спрямування проти конкретних цілей та 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 їхньої території, навіть якщо такі операції реалізуються 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»¹²³. Перше видання «Талліннського посібника» зосереджене на найбільш руйнівних кіберопераціях, які можна кваліфікувати як «збройні атаки», що дає змогу державам застосовувати заходи захисту, а також на тих, що відбуваються під час збройного конфлікту. Натомість *Таллінн 2.0* охоплює кібероперації, а не кіберконфлікти, як у виданні 2013 р.

¹²³ Schmitt, Michael N. (ed.). Tallinn manual 2.0 on the international law applicable to cyber operations. *NATO Cooperative Cyber Defence Centre of Excellence*. 2017.

НАЦІОНАЛЬНІ Й РЕГІОНАЛЬНІ ПІДХОДИ ДО БЕЗПЕКИ КІБЕРПРОСТОРУ

Авторитарні держави

Підхід Росії

35. Що таке «міжнародна інформаційна безпека»?

Сьогодні національні підходи до інформаційної безпеки суттєво відрізняються, але інформаційні загрози мають глобальний характер й очевидно, що державам потрібно досягти згоди щодо універсальних норм використання кіберпростору. Проте міжнародної згоди поки що досягти не вдалося. Авторитарний підхід не узгоджується з демократичним, 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.)¹²⁴, опублікованому на вебсайті Міністерства закордонних справ РФ. Тут інформаційна безпека розглядається як «стан захищеності інтересів особистості, суспільства й держави від загроз деструктивних та інших негативних впливів в 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.

¹²⁴ CONVENTION ON INTERNATIONAL INFORMATION SECURITY. The Ministry of Foreign Affairs of the Russian Federation.

36. Що, із позиції Росії, розглядається в якості «загроз миру й безпеці в інформаційному просторі»?

У російському проєкті Конвенції про забезпечення міжнародної інформаційної безпеки (2011 р.) 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, а саме¹²⁵:

- використання інформаційних технологій і засобів для реалізації ворожих дій та актів агресії;
- неправомірне використання інформаційних ресурсів іншої держави без узгодження з державою, в інформаційному просторі якої розміщено ці ресурси;
- дії в інформаційному просторі задля підриву політичної, економічної й 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 середовищ суспільства, ерозія традиційних культурних, моральних, етичних та 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.

¹²⁵ Там само.

37. У яких офіційних документах РФ відображено офіційні погляди на «міжнародну інформаційну безпеку»?

Предметно розкриває позицію Росії в аспекті задекларованої нею «міжнародної інформаційної безпеки» документ «Основи державної політики Російської Федерації в галузі міжнародної інформаційної безпеки»¹²⁶, оновлений варіант якого прийнято у 2021 р. Це документ стратегічного планування РФ, який відображає офіційні погляди на сутність того, що в Росії називають міжнародною інформаційною безпекою, і 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 та 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 являти собою сукупність міжнародних і національних інститутів, що регулюють діяльність у глобальному інформаційному просторі з метою запобігання загрозам (їх мінімізації) цій міжнародній інформаційній безпеці.

38. Що в Росії розглядають як «загрози міжнародній інформаційній безпеці»?

У документі «Основи державної політики Російської Федерації в галузі міжнародної інформаційної безпеки» (2021) названо «загрози міжнародній інформаційній безпеці», серед яких¹²⁷:

¹²⁶ 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/>

¹²⁷ 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/>

- використання інформаційно-комунікаційних технологій у воєнно-політичній та інших сферах задля підриву (обмеження) суверенітету, порушення територіальної цілісності держав, виконання в глобальному інформаційному просторі інших дій, що перешкоджають підтриманню міжнародного миру, безпеки й стабільності;
- застосування інформаційно-комунікаційних технологій у терористичних цілях, у тому числі для пропаганди тероризму й залучення до терористичної діяльності нових прихильників;
- використання інформаційно-комунікаційних технологій з екстремістською метою, а також для втручання у внутрішні справи суверенних держав;
- застосування інформаційно-комунікаційних технологій у злочинних цілях, у тому числі для вчинення 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;
- застосування 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 у сфері інформатизації держав та інформаційної нерівності.

Як бачимо, окрім загроз, пов'язаних із кіберзлочинністю, кібертероризмом і враженням критичної інфраструктури, відкриває й замикає список класична пересторога перед потенційними загрозами воєнно-політичного впливу й технологічного відставання, асоційовані із загрозами міжнародному миру,

безпеці та стабільності, відповідно до формату міжнародних майданчиків найвищого рівня. Згідно з такою позицією, Росія намагається врегулювати міжнародний інформаційний простір для мінімізації зазначених загроз для себе.

39. У чому суть зовнішньої політики Росії у сфері інформаційної безпеки?

Сьогодні зовнішня політика Росії в цій сфері ґрунтується на просуванні прийнятої нею ідеї «міжнародної інформаційної безпеки». Росія першою запустила на майданчику ООН дискусію з цієї проблеми, представивши в 1998 р. проєкт резолюції «Досягнення у сфері інформатизації й телекомунікацій в контексті міжнародної безпеки»¹²⁸ на засіданні Першого комітету Генеральної Асамблеї. Проєкт прийнято без голосування й 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 у сфері інформаційної безпеки. Відповідно до «Основ державної політики Росії у сфері міжнародної інформаційної безпеки»¹²⁹, прийнятих у квітні 2021 р., метою державної політики в галузі міжнародної інформаційної

¹²⁸ 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

¹²⁹ Основы государственной политики Российской Федерации в области международной информационной безопасности (Утверждены Указом президента Российской Федерации от 12 апреля 2021 г. № 213).

безпеки є «сприяння встановленню міжнародно-правового режиму, за якого створюються умови для запобігання міждержавним конфліктам (їх урегулювання) в глобальному інформаційному просторі, а також для формування з урахуванням національних інтересів Російської Федерації системи забезпечення міжнародної інформаційної безпеки». Досягнення цієї мети реалізовується за допомогою виконання завдань щодо розвитку співробітництва РФ з іноземними державами з питань формування цієї «системи забезпечення міжнародної інформаційної безпеки», а також сформульованої російськими стратегами «протидії основним загрозам міжнародної інформаційної безпеки на глобальному, регіональному, багатосторонньому й двосторонньому рівнях»¹³⁰.

40. У чому суть російського підходу до міжнародного співробітництва у сфері інформаційної безпеки?

Суть російського підходу до міжнародного співробітництва у сфері інформаційної безпеки полягає в установленні спеціального міжнародно-правового режиму, тобто, по суті, правових важелів впливу на інформаційне суспільство, головними рушіями якого поки що є інформаційно-комунікаційні технології – сфера, у якій традиційно лідирують країни Заходу. Зокрема на рівні ООН РФ діє в напрямі створення умов для прийняття державами – членами представленої нею «Конвенції про забезпечення міжнародної інформаційної безпеки» й вироблення, з урахуванням специфіки інформаційно-комунікаційних технологій, нових принципів та 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 у тексті «Конвенції про забезпечення міжнародної інформаційної безпеки»,

¹³⁰ Там само.

можемо знайти такий: «Загроза в інформаційному просторі (загроза інформаційній безпеці) – чинники, що створюють небезпеку для особистості, суспільства, держави та їхніх інтересів в інформаційному просторі». І далі: у переліку таких загроз – «протидія доступу до новітніх інформаційно-комунікаційних технологій, створення умов технологічної залежності у сфері інформатизації на шкоду іншим державам»¹³¹. Тобто, із 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 таким чином 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 та недоторканності інформації з погляду приватної власності. Також держави Заходу традиційно пропонують підходи, основані на прозорості, що також не підтримується російськими чиновниками через нібито загрозу національному суверенітету. Із цієї причини, наприклад, у 2012 р. РФ заблокувала резолюцію про раннє попередження про кібератаки в ОБСЄ¹³².

¹³¹ CONVENTION ON INTERNATIONAL INFORMATION SECURITY. The Ministry of Foreign Affairs of the Russian Federation.

¹³² Sternstein Aliya. 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/>

41. У чому відмінність між поняттями «інформаційний простір» і «кіберпростір»?

У представленому Росією проєкті «Конвенції про забезпечення міжнародної інформаційної безпеки»¹³³ потрактовано поняття «інформаційний простір» як «сферу діяльності, пов'язану з формуванням, створенням, перетворенням, передаванням, використанням, зберіганням інформації, що впливає, 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 інфраструктури (див., наприклад, у^{134, 135}), тут це поняття відображає політичні погляди російського керівництва на суть міжнародних відносин в інформаційній сфері як спосіб отримати певні вигоди для держави-актора.

Натомість у демократичному баченні переважно наводять концепт кіберпростору – (*Cyberspace*), який визначають у 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»¹³⁶. Наукове визначення інформаційного простору в трактуванні представників демократичних суспільств наближене до

¹³³ CONVENTION ON INTERNATIONAL INFORMATION SECURITY. The Ministry of Foreign Affairs of the Russian Federation.

¹³⁴ 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.

¹³⁵ Манойло А. В. Государственная информационная политика в особых условиях: монография. Москва: МИФИ, 2003. 388 с.

¹³⁶ 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

кіберпростору: «Тип інформаційної конструкції, у якій репрезентації інформаційних об'єктів розташовані в організованому просторі. У такому просторі розташування й напрямки мають значення, а отже, стають можливими створення карт і навігація»¹³⁷.

У відомому дослідженні «Талліннський посібник» (2013) запропоновано визначення кіберпростору як середовища, сформованого з фізичних та нефізичних елементів, яке характеризується використанням комп'ютерів й електромагнітного спектра для зберігання, зміни та обміну даними із застосуванням комп'ютерних мереж¹³⁸.

У типовому навчальному плані НАТО з кібербезпеки (2016 р.)¹³⁹ є модуль «Структура інформаційного простору: опорна мережа інтернету й мережева інфраструктура держав», котрий стосується винятково технічних аспектів інформаційного простору. Основну увагу при цьому приділено глобальній інфраструктурі, а також інформаційним системам, створеним у масштабі держав й окремих підприємств. А інформаційний простір уключає в себе архітектуру інтернету, комп'ютерні й мобільні мережі, де передусім 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).

¹³⁷ 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>

¹³⁸ Schmitt, Michael N. (ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013. URL: <http://www.cambridge.org/tallinmanual2>

¹³⁹ DEEP: Cybersecurity – A Generic Reference curriculum. NATO. URL: https://www.nato.int/cps/en/natohq/topics_157591.htm

Діяльність Росії в ООН

42. Які головні напрями діяльності Росії на рівні ООН щодо просування своїх інтересів у сфері інформаційної (кібер) безпеки?

Починаючи від кінця 1990-х рр., Росія розгорнула системну діяльність на рівні ООН щодо просування своїх інтересів у сфері інформаційної безпеки, зокрема подаючи проєкти резолюцій ГА ООН із питань безпеки інформаційного простору. Суть їх незмінна й серед членів ООН існує група держав, які ці резолюції традиційно підтримують. Це, зокрема, члени БРІКС, ШОС та частина країн, що розвиваються. Наприклад, Резолюцію 73/27 2018 р. «Досягнення у сфері інформатизації й телекомунікацій в контексті міжнародної безпеки»¹⁴⁰, яка просувалася Росією у 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 у цифровій сфері, незалежно від того, на якому рівні технологічного розвитку вони перебувають. У зв'язку з цим наголошено на важливості надання допомоги деяким державам для подолання розриву у сфері інформаційно-комунікаційних технологій, що, на думку авторів документа, має важливе значення для міжнародної безпеки. По-друге, у резолюції представлено перелік правил, норм і принципів поведінки держав в інформаційному просторі з оголошеною метою – закласти основу мирної взаємодії держав в ІКТ-середовищі, забезпечити запобігання війнам, конфронтації й будь-яким агресивним діям.

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, уперше наведено ці норми (усього 13 пунктів). Наприклад, першим пунктом сформульовано те, що, «відповідно до цілей

¹⁴⁰ 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

Статуту Організації Об'єднаних Націй, у тому числі які стосуються підтримання міжнародного миру й безпеки, держави повинні співпрацювати в розробці й здійсненні заходів зі зміцнення стабільності та безпеки у використанні ІКТ і запобігання вчиненню дій у 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 відбуватися обґрунтування цих звинувачень, не уточнено). Також у переліку «норм» є заборона державам дозволяти використовувати свою територію та інфраструктуру для вчинення кібератак і зобов'язання співпрацювати «з метою обміну інформацією, надання взаємодопомоги, переслідування осіб, винних у терористичному й злочинному використанні інформаційно-комунікаційних технологій». Наголошено на забороні країнам здійснювати кібератаки щодо критично важливої інфраструктури та 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 й організаціями громадянського суспільства у сфері здійснення правил відповідальної поведінки держав в інформаційному просторі з урахуванням їх потенційної ролі».

Під час складання цього переліку автори, очевидно, спиралися на документ Шанхайської організації співпраці (ШОС) від 2015 р. «Правила поведінки в галузі забезпечення міжнаціональної інформаційної безпеки»¹⁴¹, 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

¹⁴¹ Правила поведінки в області забезпечення міжнародної інформаційної безпеки, Документ ООН А/69/723/, 13 янв. 2015. URL: <https://bit.ly/31dRCX0>

державної безпеки, громадського порядку, здоров'я чи моральності населення»¹⁴². Проте в підсумковий текст вони не увійшли.

43. Як можна коротко окреслити сферу й обставини діяльності Групи урядових експертів у сфері інформатизації й телекомунікації в контексті міжнародної безпеки (UN GGE)?

Одним із результатів діяльності в контексті резолюцій «Досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки», починаючи з 1999 р., було створення у 2004 р з ініціативи російської сторони Групи урядових експертів у сфері інформатизації й телекомунікації в контексті міжнародної безпеки з метою вивчення наявних 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 та Росії з питання використання інформації й контенту як фактора загрози національній безпеці держави. Потім були скликані ще три групи, які завершили свою роботу консенсусними доповідями у 2010, 2013 і 2015 рр., але робота п'ятої групи у 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 наполягали на включенні в доповідь пункту про право держав на самооборону в кіберпросторі.

Свою роль зіграли й напружені відносини між Росією та США, які є одними з постійних учасників ГУЕ. Як відомо, американська сторона звинуватила Росію у втручанні в американські президентські вибори 2016 р., а також у скоєнні кібератак і проведенні інформаційних кампаній у соціальних мережах. Більше

¹⁴² Россия и США перетягивают всемирную паутину. В ООН представлены конкурирующие резолюции по кибербезопасности. *Коммерсантъ*. № 207. 12.11.2018, с. 6.

того, висловлювалися думки, що формат ГУЕ себе вичерпав і потрібно шукати нові майданчики для обговорення правил відповідальної поведінки держав у кіберпросторі. Проте ГУЕ 2019–2020 рр. успішно завершила свою роботу, прийнявши консенсусний звіт у травні 2021 р.¹⁴³, що свідчить про актуальність такого формату співпраці, хоча у 2018 р. з подання Росії закладено новий майданчик для обговорення проблем інформаційної безпеки – Робочу групу відкритого складу (РГВС, ОЕWG), у якій беруть участь «усі зацікавлені держави» (детальніше про цю групу йтиметься далі).

Потрібно відзначити, що ГУЕ ООН складається на основі «справедливого географічного розподілу». Традиційно беруть участь у всіх ГУЕ п'ять постійних членів Ради Безпеки, а решта місць розподіляється за групами. На заклик до вираження інтересів держави надсилають офіційний запит про місце в 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 сектору чи міжнародних організацій), без оголошення загальнодоступних підсумків засідань. Формат закритих дверей вважається важливим для відвертих дискусій, щоб дати можливість учасникам досягти згоди¹⁴⁴.

Важливим фактом є підпорядкування ГУЕ Першому комітету ГА 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

¹⁴³ 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>

¹⁴⁴ UNIDIR. Report of the International Security Cyber Issues Workshop Series. 2016. URL: <https://www.unidir.org/publication/report-international-security-cyber-issues-workshop-series>

інтернетом, розвиток і конфіденційність у цифровому режимі, технічні питання, не пріоритетними в роботі Групи. Наприклад, неодноразово пропонувалося запросити Міжнародний телекомунікаційний союз (МСЕ, ІТУ), спеціалізоване агентство ООН, відповідальне за розробку технічних стандартів для ІКТ у ролі спостерігача в роботі Групи, що, однак, не підтримано Генеральною Асамблеєю з огляду на те, що робота ГУЕ має бути зосереджена безпосередньо у сфері міжнародної безпеки й роззброєння¹⁴⁵.

44. У чому суть позиції Росії у сфері протидії інформаційній злочинності?

У 2017 р. Росія представила проєкт конвенції ООН «Про співпрацю у сфері протидії інформаційній злочинності»¹⁴⁶. 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, була 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-

¹⁴⁵ UNIDIR. Report of the International Security Cyber Issues Workshop Series. 2016. URL: <https://www.unidir.org/publication/report-international-security-cyber-issues-workshop-series>

¹⁴⁶ 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 у злочинних цілях»¹⁴⁷ «фактично орієнтована на закріплення цифрового суверенітету держав над інформаційним простором, а під егідою Генасамблеї ООН створюється переговорний майданчик для розробки універсальної конвенції з боротьби з кіберзлочинністю – спеціальний комітет у складі експертів з усіх країн світу (подібним чином просувалися конвенції ООН проти корупції та проти транснаціональної організованої злочинності). Разом із Росією співавторами цієї резолюції виступили 47 країн, серед яких – Білорусь, Казахстан, Азербайджан, Таджикистан, Вірменія, Китай, Індія, Сирія, Єгипет, КНДР, Іран, і Венесуела. «Проти» проголосували США, Канада, Франція, Німеччина, Велика Британія, Україна й ще 54 держави.

45. Яка причина особливої позиції РФ у сфері інформаційної (кібер) безпеки?

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 ІТ-сфері російський уряд реагує шляхом посилення інформаційної політики на внутрішньому рівні. Ця тенденція призводить до подальшої фрагментації російського сегменту 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. На міжнародних майданчиках Росія послідовно відстоює свій підхід, зокрема

¹⁴⁷ 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>

вважаючи, що поведінка держав і їхні права в кіберпросторі повинні бути регламентовані міжнародними угодами, подібними до угод про космічний простір і мореплавство.

Китай

46. На яких засадах ґрунтується політика у сфері інформаційної (кібер) безпеки Китаю?

Підхід китайського керівництва до проблематики загроз, пов'язаних із розвитком інформаційно-комунікаційної активності суспільства загалом подібний до підходу Росії, що полягає в широкому трактуванні саме «інформаційної безпеки», а не безпеки в кіберпросторі, і претензіях на управління певним сегментом того самого кіберпростору (а в розумінні місцевої влади – частини всесвітньої мережі й інформаційних ресурсів, котрі належать до юрисдикції Китаю). Китай загалом послідовно підтримує ініціативи Росії щодо формування міжнародного режиму інформаційної безпеки на міжнародних форумах, виступаючи з нею єдиним табором у дискусіях на майданчику ООН і спільно висуваючи ініціативи на форумах у площині спільних інтересів (таких як ШОС).

Але в Китаю є власна траєкторія розвитку й стратегічне бачення національної безпеки, невід'ємною частиною якої політичне керівництво країни вбачає все, що пов'язано з політико-ідеологічними, технічними та економічними аспектами безпеки у сферах інформації й ІКТ. Сучасна політика у 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 винятково в інтересах правлячої Комуністичної партії Китаю (КПК). Провідна роль компартії в китайському суспільстві посилюється, особливо під керівництвом нинішнього лідера країни Сі Цзіньпіна, який декларує, що «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»¹⁴⁸.

47. Яка інституційна основа політики інформаційної (кібер) безпеки КНР?

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, виокремлено й інформаційну¹⁴⁹. Система кібербезпеки в Китаї формується відповідно до Комплексної концепції національної безпеки Сі Цзіньпіна¹⁵⁰, у 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 у сфері високих технологій та контроль ідеології й інформації.

¹⁴⁸ 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 běnzhì 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

¹⁴⁹ 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>

¹⁵⁰ 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 усебічно 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

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 відіграють роль спеціалізованих інститутів, забезпечуючи інформаційну безпеку в інтернет-просторі. У сфері зовнішньої політики Комісія працює спільно з Центральним комітетом з міжнародних справ. 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 кібербезпеки 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.

Центральній комісії з кібербезпеки й інформатизації підпорядковується провідний орган у сфері адміністрування безпеки кіберпростору – Адміністрація кіберпростору Китаю (*Cyberspace Administration of China, SAC*), заснований на тій самій системі, що й Управління з питань зовнішньої пропаганди Комуністичної партії Китаю.

48. Як регулюється кіберпростір у КНР?

Адміністрація кіберпростору Китаю (*Cyberspace Administration of China, SAC*) бере участь у формуванні та реалізації політики з різних питань, пов'язаних із китайським інтернетом. Серед областей, які регулює SAC, – імена користувачів у китайському інтернеті, доречність висловлювань, поширених в інтернеті, віртуальні приватні мережі, уміст інтернет-порталів й ін. Наприклад, у травні 2020 р. оголошено восьмимісячну кампанію з «очищення» політичного й

релігійного онлайн-контенту, який вважається «незаконним». 151 САС також здійснює деякі цензурні функції, уключаючи видання директив медіакомпаніям у Китаї¹⁵². Причому під наглядом перебувають не лише публікації на вебсайтах, а й коментарі до них – під виглядом самодисципліни управління вебсайтами. Наприклад, серед сформульованих категорій заборонених коментарів є 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»¹⁵³. У 2021 р. САС запустила гарячу лінію, щоб повідомляти про онлайн-коментарі проти Комуністичної партії Китаю¹⁵⁴. Крім того, Адміністрація кіберпростору контролює безпеку пристроїв, виготовлених зарубіжними країнами й програмне забезпечення (у грудні 2020 р. із магазинів додатків у Китаї видалено 105 програмних застосунків, які визнано «незаконними», щоб «очистити інтернет у Китаї»¹⁵⁵).

¹⁵¹ 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, wéiqī 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>

¹⁵² 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>

¹⁵³ 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 zìlǚ guǎnlǐ chéngnuò shū». 2014 Nián 11 yuè 06 rì 22:36 Xīnhuá wǎng) [29 вебсайтів підписали «Зобов'язання щодо самодисциплінованого менеджменту публікації коментарів». Сінхуа, 06 листопада 2014]. URL: <http://news.sina.com.cn/c/2014-11-06/223631106669.shtml>

¹⁵⁴ 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/>

¹⁵⁵ 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>

Також повідомлялося про те, що САС систематично встановлює цензурні обмеження для китайських ЗМІ та соціальних мереж, регулюючи масову комунікацію щодо COVID-19, залучаючи фальшивих інтернет-коментаторів, щоб відволікати увагу в соціальних мережах від чутливих, на думку китайської влади, питань¹⁵⁶. Із 2013 р. САС 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, умісту в інтернеті, а також зміцнення китайської індустрії ІКТ.

49. Як розвивалася нормативна основа кібербезпеки КНР?

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

Законодавство Китаю у 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 р¹⁵⁷. Саме тоді повноваження щодо контролю, інспекції й забезпечення національної інформаційної безпеки, розслідування, розкриття та запобігання злочинам у сфері ІКТ надано Міністерству державної безпеки Китаю. Уже в 1997 р. прийнято закон про безпеку мережної інфраструктури й

¹⁵⁶ Zhong, Raymond; Mozur, Paul; Krolík, Aaron; Kao, Jeff. Leaked Documents Show How China's Army of Paid Internet Trolls Helped Censor the Coronavirus. *ProPublica*. December 19, 2020.

¹⁵⁷ 计算机信息系统安全管理制度 (Jìsuànjī xìnxi xitǒng ānquán guǎnlǐ zhìdù) [Система управління безпекою комп'ютерної інформаційної системи]. URL: <https://wenku.baidu.com/view/8814c60716fc700abb68fc31.html>.

мережі «Інтернет», що стало одним із 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 або руйнування суспільного ладу¹⁵⁸»).

Протягом 2000–2015 рр. прийнято низку нормативних актів у сфері регулювання кібербезпеки в Китаї, зокрема документи стратегічного планування, які визначали горизонти інформатизації в країні разом з основними напрямками регулювання. Наприклад, Державна стратегія з розвитку інформатизації на період 2006–2020 рр., серед стратегічних цілей якої – «створити національну систему гарантій інформаційної безпеки»¹⁵⁹. У 2012 р. прийнято документ Держради КНР із просування інформатизації й розвитку чинної 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

¹⁵⁸ New PRC Internet Regulation. A January 1998 report from U.S. Embassy Beijing. URL: <https://fas.org/irp/world/china/netreg.htm>

¹⁵⁹ 2006–2020 年国家信息化发展战略 (2006-2020 Nián guójiā xīn xī huà fāzhǎn zhànlüè) [Державна стратегія із розвитку інформатизації на період із 2006 до 2020 р.]. 08.05.2005. URL: <https://baike.baidu.com/item/2006-2020%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 та інтернет-трафіку під час виникнення загроз безпеці країни¹⁶⁰.

У 2015 р. започатковано дешифрування інтернет-трафіка, застосування адміністративних заходів щодо вилучення в іноземних компаній і підприємств інформації в разі підозри 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 вмістом та технічні запобіжні заходи безпеки для запобігання поширенню інформації, що містить тероризм й екстремізм»¹⁶¹).

Еволюція правил і норм із кібербезпеки з різних рівнів та сфер увінчалася прийняттям структурованого закону щодо кібербезпеки на макрорівні. Закон КНР про кібербезпеку прийнятий у 2016 р. і діє з 1 червня 2017 р.

50. У чому полягають головні виклики закону КНР про кібербезпеку з погляду іноземних компаній?

Головною метою прийняття закону КНР про кібербезпеку (2016 р.) проголошено захист національного «кіберсуверенітету» КНР, а серед найважливіших його положень – 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

¹⁶⁰ 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.

¹⁶¹ 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

уведення 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 їх справді потрібно надати за межами материка, вони повинні виконувати заходи, спільно сформульовані державними департаментами кібербезпеки»¹⁶²). Якщо користувач не надає реальні ідентифікаційні дані, провайдер не має права відкривати доступ до мережі. Від іноземних компаній вимагається проходження спеціальної сертифікації, що, у 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 набув чинності 1 січня 2020 р., виключається будь-який особливий статус, пов'язаний із тим, що фірма має статус компанії з іноземними інвестиціями (спільні підприємства, представництва), а іноземні компанії щодо кіберконтролю розглядаються так само, як і китайські компанії¹⁶³. Відповідно до Закону про

¹⁶² 中华人民共和国网络安全法(Zhōnghuá rénmin 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

¹⁶³ 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>

кібербезпеку, китайський уряд має право на отримання від будь-якої фізичної чи юридичної особи в Китаї будь-якої інформації, яка, як вважатиме китайський уряд, якимось впливає на безпеку Китаю. Китайський закон про кібербезпеку не лише генералізував попередні напрацювання в цій сфері, але й став основою для подальшого розвитку комплексної програми безпеки/спостереження¹⁶⁴ в інтернеті за планом, який уключає низку допоміжних законів і нормативних актів, згідно з рішеннями XIX з'їзду КПК, на якому ІКТ поставлено в центр економічного розвитку й наголошено на важливості кібербезпеки в міру поширення загроз та ризиків¹⁶⁵.

51. У чому полягає системність підходу китайської влади до регулювання кіберпростору?

Із нормативного й технологічного погляду, усі китайські закони, стратегії, нормативні документи й керівні дії у сфері безпеки кіберпростору можна трактувати як чинні в шести системах, які разом становлять еволюційну основу для регулювання використання ІКТ у Китаї¹⁶⁶: 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 комплексного плану повинна 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

¹⁶⁴ Triolo Paul, Sacks Samm, Graham Webster, Creemers Rogier. 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/>

¹⁶⁵ Cyber Policy and the 19th Party Congress. CSIS. October 26. 2017. URL: <https://www.csis.org/analysis/cyber-policy-and-19th-party-congress>

¹⁶⁶ Там само.

охоплення всього підконтрольного китайській владі кіберпростору, кожного району, кожного міністерства, кожного бізнесу, усіх мереж та інформаційних систем, хмарних платформ, інтернету речей, систем управління, великих даних і мобільного інтернету¹⁶⁷.

Технологічним компонентом комплексної програми збору, спостереження та контролю даних є Багаторівнева схема захисту кібербезпеки (*MLPS 2.0*), що функціонує з 1 грудня 2019 р. й забезпечує реалізацію технічного та 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 стандартах¹⁶⁸. Її цілями є спостереження та контроль із боку уряду КНР і 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 безпеки¹⁶⁹). 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 (у тому числі ті, що належать

¹⁶⁷ Dickinson Steve. China's New Cybersecurity Program: NO Place to Hide. *Harris/Bricken*. Sept. 30. 2019. URL: <https://harrisbricken.com/chinalawblog/chinas-new-cybersecurity-program-no-place-to-hide/>

¹⁶⁸ China Security GB Standarts List. URL: http://www.gbstandards.org/index/Standards_Search.asp?word=security

¹⁶⁹ 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

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 зарубіжні розміщення акцій, повинні проходити додаткову перевірку¹⁷⁰. Відомство має намір розглядати потенційні загрози для національної безпеки й оцінювати надійність зберігання компаніями даних китайських користувачів і ризику розкрадання, витоку, ушкодження чи незаконного експорту такої інформації.

Що стосується персональних даних, то формально вони захищені й у цьому напрямі прийнято низку нормативних актів, котрі водночас доповнюють згадану вище комплексну систему державної кібербезпеки Китаю. У 2021 р., зокрема, прийнято Закон про захист особистої інформації (Personal Information Protection Law)¹⁷¹, котрий уперше встановлює вичерпний набір правил щодо збору та захисту персональних даних і може застосовуватися до зарубіжних обробників,

¹⁷⁰ 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 shěncá bānfǎ (xiūdìng cǎo'àn zhēngqiú yìjiàn gǎo)» gōngkāi zhēngqiú yìjiàn de tōngzhī) [Повідомлення Державного інформаційного офісу Інтернету про «Заходи з огляду кібербезпеки (переглянутий проєкт збору коментарів, 10 липня 2021)» Публічне звернення за коментарями]. URL: http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm

¹⁷¹ Chipman Koty Alexander. 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/>

а також Закон про безпеку даних¹⁷², 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, котрі не мають зв'язку з КПК. Із погляду 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, зацікавлена в отриманні доступу до технологій та 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, котра зацікавлена в інформації, знову ж таки, із метою доступу до технологічних і розвідувальних даних, а також у проведенні спеціальних операцій.

Демократичні держави

Розвиток політики кібербезпеки США

52. Які характерні риси були притаманні політиці кібербезпеки США у 2000-х рр.?

Підхід США в політиці інформаційної безпеки екстраполюється на міжнародний рівень як наполягання на добровільному характері норм і правил

¹⁷² Chen Abby. 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/>

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.

Підхід США ґрунтується 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 в аспекті змін у міжнародній обстановці та технологічного прогресу. Уже у 2003 р. прийнято «Національну стратегію захисту кіберпростору»¹⁷³, відповідно до якої координацію роботи щодо забезпечення безпеки кіберпростору, зокрема щодо запобігання збиткам, несанкціонованому доступу й виведенню з ладу інфраструктури, виконує утворене у 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, у тому числі щодо вироблення міжнародних принципів поведінки й обміну інформацією. Роботу із забезпечення безпеки кіберпростору здійснюють агентства й федеральні міністерства, а Державний департамент розвиває співробітництво з усіх питань кібербезпеки на міжнародній арені, формуючи міжнародне середовище передусім із державами, які поділяють спільне бачення зі 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 крізь призму боротьби з тероризмом і, зокрема, наголошувала на таких напрямках роботи, як взаємодія з міжнародними організаціями та з промисловістю для сприяння глобальній культурі безпеки; розвиток безпечних мереж; сприяння

¹⁷³ THE NATIONAL STRATEGY TO SECURE CYBERSPACE. FEBRUARY 2003. URL: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

створенню національних і міжнародних мереж спостереження й попередження для виявлення та запобігання кібератакам у міру їх виникнення; заохочення інших країн приєднатися до Конвенції Ради Європи про кіберзлочинність або забезпечити, щоб їхні закони й процедури були принаймні всеосяжними.

53. Які виклики визначали політику США у сфері кібербезпеки в період президентства Барака Обами?

Адміністрація Б. Обами, урахувуючи нові обставини у сфері кібербезпеки й нові виклики, ініціювала новий етап розвитку системи кібербезпеки, основні положення якої розкрито в документах «Всеосяжна національна ініціатива кібербезпеки»¹⁷⁴ (2008) та «Огляд політики в кіберпросторі»¹⁷⁵ (2009). Саме при Обамі, у 2010 р., створено кіберкомандування, розроблено й затверджено низку документів, якими закріплено основи проведення оборонних і наступальних операцій у кіберпросторі. Кібербезпеку оголошено однією з найсерйозніших проблем економічної та національної безпеки. Незабаром після вступу на посаду президент наказав ретельно переглянути федеральні зусилля щодо захисту інформаційної й комунікаційної інфраструктури США та розробити комплексний підхід до забезпечення цифрової інфраструктури країни. Із метою координації системи кібербезпеки утворено посаду координатора державної політики з кібербезпеки, який має регулярний доступ до президента. Виконавча влада була спрямована на тісну співпрацю з усіма ключовими гравцями кібербезпеки США, включаючи державні й місцеві органи влади та приватний сектор, щоб забезпечити організовану і єдину систему реагування на майбутні кіберінциденти, зміцнити державно-приватне партнерство для пошуку технологічних рішень, котрі забезпечують безпеку й процвітання США,

¹⁷⁴ The Comprehensive National Cybersecurity Initiative. URL: <https://fas.org/irp/eprint/cnci.pdf>

¹⁷⁵ Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. URL: <https://fas.org/irp/eprint/cyber-review.pdf>

інвестувати в передові дослідження та розробки й розпочати кампанію щодо сприяння поінформованості про кібербезпеку й цифрову грамотність, розпочати розвиток цифрової робочої сили XXI ст. І вся ця діяльність розвивалася таким чином, щоб це відповідало забезпеченню прав на конфіденційність і громадянських свобод, гарантованих Конституцією¹⁷⁶. 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 у підготовці доповіді Групи урядових експертів ООН, яка була узгоджена консенсусом і схвалена Генасамблеєю ООН. Для просування політики США у сфері 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»¹⁷⁷. Із погляду національної безпеки виникла актуальна потреба в розв'язанні масштабних проблем, що з'явилися у зв'язку з атаками в мережі, які можуть серйозно загрожувати національній безпеці, що продемонстровано в ході кібератак проти Естонії навесні 2007 р.

За роки президентства Б. Обама потенціал використання ІКТ-інструментів набув значення важливого фактора міжнародних відносин. Із погляду дієвості

¹⁷⁶ The Comprehensive National Cybersecurity Initiative. URL: <https://fas.org/irp/eprint/cnci.pdf>

¹⁷⁷ 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

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 кіберпросторі¹⁷⁸. Президент Обама в цьому документі підкреслює, що «зростання поширеності й серйозності шкідливих дій, пов'язаних із кіберзахистом, які походять від або керуються особами, котрі перебувають повністю або значною мірою за межами Сполучених Штатів, становить надзвичайну загрозу національній безпеці, зовнішній політиці та 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, проте злочинна діяльність у його рамках розуміється надзвичайно широко, хоча указ і не розкриває методики ідентифікації кіберзлочинця.

Потрібно 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 роботі комп'ютера чи мережі комп'ютерів;
- спричинення значного привласнення коштів або економічних ресурсів, комерційної таємниці, особистих ідентифікаторів або фінансової

¹⁷⁸ 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>

інформації задля комерційної чи конкурентної переваги чи приватної фінансової вигоди.

54. Які цілі визначено в «Міжнародній стратегії для кіберпростору» США (2011 р.)?

Як відзначено в «Міжнародній стратегії для кіберпростору» (2011 р.), Сполучені Штати прагнуть до середовища кіберпростору, яке винагороджує 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 оголошено¹⁷⁹:

- досягнення глобального консенсусу щодо відповідальної поведінки держав у кіберпросторі, уключаючи 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, уключаючи сприяння міжнародному співробітництву та 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 сектору;

¹⁷⁹ Pillars of The International Strategy for Cyberspace. U.S. Department of State. URL: <https://2009-2017.state.gov/s/cyberissues/strategy/index.htm>

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

55. Які характерні риси притаманні політиці адміністрації Д. Трампа у сфері кібербезпеки?

Говорячи про зовнішню політику США у сфері інформаційної (кібер) безпеки, мусимо 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 стратегія й 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, у той час, як інфраструктура Америки прийшла в занепад ... Із цього дня на першому місці буде тільки Америка»¹⁸⁰. 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»¹⁸¹.

Фактично в такому дусі й повністю, відповідно до мети «Зробити Америку великою знов», дбаючи винятково про Америку, підготовлено опубліковану у 2018 р. «Національну кіберстратегію Сполучених Штатів Америки»¹⁸². Документ відображає глибинний підхід в оцінці ризиків, пов'язаних із кіберпростором і чи не вперше в американській політиці інтегрує кібердіяльність у систему владних відносин: «Кіберпростір більше не розглядатиметься як окрема категорія політики чи діяльності, відокремлена від інших елементів національної влади. Сполучені Штати будуть інтегрувати використання кіберопцій у всі елементи національної влади». Подібне бачення вже давно було властивим для держав, що дотримувалися російсько-китайського підходу в інформаційній безпеці.

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 їхніх

¹⁸⁰ Haass Richard. Present at the Disruption. How Trump Unmade U.S. Foreign Policy. *Foreign Affairs*. 11.08.2020. September/October 2020. URL: <https://www.foreignaffairs.com/articles/united-states/2020-08-11/present-disruption>

¹⁸¹ Там само.

¹⁸² National Cyber Strategy of the United States of America. URL: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

повноважень). Так, Міністерство оборони отримало власну кіберстратегію¹⁸³, розроблену відповідно до національної, та 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»¹⁸⁴.

Загалом період президентства Д. Трампа характеризується розбудовою стратегії та 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 зі штатами США та покращення захисту держави від дій приватних і національних хакерів). У міжнародному вимірі, незважаючи на ізоляціоністську риторику президента, США послідовно дотримувалися раніше напрацьованих підходів.

56. Які позиції у сфері міжнародної політики характеризують кіберстратегію Д. Трампа?

Із погляду міжнародної політики, у кіберстратегії Трампа закладено позицію захисту національних інтересів перед загрозою чинників, які можуть впливати на інформаційні системи, критичну інфраструктуру й економічні процеси та пов'язані з конкретними акторами, серед яких виокремлено Росію, Китай, Іран, КНДР і міжнародний тероризм: «Адміністрація визнає, що

¹⁸³ Summary. DEPARTMENT OF DEFENSE CYBER STRATEGY (2018). URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

¹⁸⁴ Там само.

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, їхніми союзникам і партнерам, часто з безглуздя, яке вони ніколи не проявляли би в інших сферах діяльності. Ці протиборчі сторони використовують кіберінструменти, щоб підірвати нашу економіку й демократію, украсти 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 проведуть кібератаки проти Сполучених Штатів під час кризи, близької до війни. Ці протиборчі сторони постійно розробляють нову й більш ефективну кіберзброю»¹⁸⁵. Можливо, під час підготовки документа враховано й реакцію суспільства на звинувачення зовнішніх сил у втручанні в перебіг президентських виборів у США у 2016 р., і досвід інформаційної експансії Росії в Україну.

Ураховуючи характер і масштаб конкретних противників, зовнішньополітична лінія у 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 подальшій 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 та, за необхідності, карати тих, хто використовує кіберінструменти на шкідливі цілі»; і «розширити вплив Америки за кордоном, щоб розширити ключові принципи відкритої, сумісної взаємодії, надійний і

¹⁸⁵ National Cyber Strategy of the United States of America. URL: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

безпечний інтернет»¹⁸⁶. Звісно, головним завданням цієї національної стратегії є відстоювання національних інтересів, зокрема в аспекті впливу на функціонування інтернету.

Фактично інтернет, цей американський продукт, будучи демонстративно виведеним з-під державного контролю в США і відданим на саморегуляцію, є спокусливим полем діяльності для суперників і противників Америки. Тому Сполучені Штати наполягають на багатосторонній моделі управління інтернетом та 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 погляду, зокрема, національних економічних інтересів: «Багато країн усе частіше вдаються до різних обмежень для локалізації даних і впроваджують механізми регулювання з метою реалізації політики цифрового протекціонізму під приводом забезпечення національної безпеки. Ці дії негативно впливають на конкурентоспроможність американських компаній»¹⁸⁷. 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»¹⁸⁸.

Сполучені Штати відкрили свої технології для світу та світового ринку. Це інтернет, комп'ютери, глобальна система позиціонування й багато іншого, але натомість залишають за собою право вимагати толерантної та відповідальної поведінки тих, хто цими технологіями користується. Головним завданням американської влади в цьому аспекті на зовнішньополітичному напрямі є

¹⁸⁶ Там само.

¹⁸⁷ Там само.

¹⁸⁸ Там само.

запобігання потенційним загрозам, що походять від політичних і геополітичних суперників, котрі 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 та контролюючи доступ до нього своїх громадян. Для легітимізації такої поведінки вони активно прагнуть підірвати принципи вільного доступу всіх охочих до всесвітньої мережі на міжнародних форумах.

У Національній кіберстратегії США від 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, що застосовуються в мирний час задля зміцнення довіри та зменшення ризику конфліктів, пов'язаних зі шкідливою кібердіяльністю, і підтримка універсальності міжнародного права у сфері інформаційних відносин та 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 ІТ-компаній із 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 монтувались оперативними агентами з підрозділу Народно-визвольної армії Китаю в серверні плати, що використовуються багатьма американськими компаніями, у тому числі

Amazon та Apple¹⁸⁹. Також особливої ваги надано захисту чутливих нових технологій і комерційної таємниці – для запобігання використанню національними державами результатів американських досліджень і розвитку для завоювання несправедливої переваги. І ще одним важливим напрямом стратегії є розвиток боротьби з 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 ідеться про розвиток співпраці з іноземними державами. Прикладом такої діяльності є збір необхідної інформації, що регулюється угодами про взаємну правову допомогу, що реалізуються, у тому числі, у рамках Будапештської конвенції з протидії кіберзлочинності. Натомість прийнятий у 2018 р. «CLOUD Act»¹⁹⁰ дає правоохоронним органам змогу отримувати інформацію, що зберігається на серверах американських компаній, які розміщені за межами США.

Сфера протидії кіберзлочинності є однією з пріоритетних в американській кіберстратегії: тут США планують відігравати провідну роль у розробці сумісних і взаємовигідних механізмів для ефективного транскордонного обміну інформацією у сфері правоохоронних дій, а також просувають використання наявних 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 та дезінформації – у розділі, що стосується

¹⁸⁹ Robertson Jordan, Riley Michael. 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>

¹⁹⁰ 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>

неприпустимої поведінки в кіберпросторі. А на протидію «безвідповідальній поведінці держав у кіберпросторі, що спричиняє збитки США чи американським партнерам», для запобігання, реагування й стримування зловмисної кіберактивності можуть бути використані всі доступні інструменти, у 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, у 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.

57. Як змінилася політика США у сфері кібербезпеки з приходом адміністрації Джозефа Байдена?

Президентство Дж. Байдена розпочалось із його заяви про те, що «Америка повертається, дипломатія повертається»¹⁹¹, 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 займемося світом не для того, щоб відповідати вчорашнім викликам, а сьогоднішнім і завтрашнім. Американське керівництво має зустріти цей новий момент просування авторитаризму,

¹⁹¹ Sink Justin, Parker Mario. '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/>

уключаючи зростаючі амбіції Китаю конкурувати зі США й рішучість Росії завдати шкоди нашій демократії»¹⁹².

Отже, розробка питань кібербезпеки адміністрацією Дж. Буша-молодшого відбувалася на тлі протистояння з міжнародним тероризмом після терактів 2001 р., Б. Обама – після показової масштабної кібератаки проти Естонії, Д. Трамп – з оглядом на приклади національного протекціонізму Китаю й Росії над окремими сегментами інтернету та активної експансії окремих країн у сфері кіберпростору, чутливі для США й 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 загрозової діяльності в кіберпросторі.

У першому виступі президента Байдена про місце Америки у світі відзначено збільшення ваги кібербезпеки з погляду національних інтересів США: «Ми підняли статус кіберпитань у нашому уряді, уключаючи призначення 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»¹⁹³.

Уже в травні 2021 р. на сайті Білого дому опубліковано президентський указ про покращення національної кібербезпеки¹⁹⁴. Документ з'явився невдовзі після масштабних кіберінцидентів, які сталися з американськими компаніями стратегічного значення SolarWinds, Microsoft і Colonial Pipeline, що виявило потребу доопрацювання механізмів взаємодії між державою й приватним

¹⁹² 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/>

¹⁹³ Там само.

¹⁹⁴ 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 в аспекті запобігання кіберзагрозам і реагування на них. Повідомлено, що це лише перший із багатьох амбітних кроків, які адміністрація робить для модернізації національного кіберзахисту¹⁹⁵. У документі детально описано процедурні моменти, що 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 у сфері кібербезпеки, спільно очолювана представниками уряду й приватного сектору, що може збиратися після значного кіберінциденту, щоб проаналізувати те, що сталося, і дати конкретні рекомендації щодо покращення кібербезпеки. Також указом упроваджується стандартизований посібник та набір визначень для реагування на кіберінциденти федеральними департаментами й відомствами.

Очевидно, що, ураховуючи підходи Байдена в зовнішній політиці, США активно реалізуватимуть свої цілі у відносинах із країнами-партнерами та опонентами. У цьому аспекті важливою стала зустріч президентів США й Росії в Женеві в 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 США¹⁹⁶. Натомість обидва лідери домовилися розпочати переговори про кібербезпеку, що, імовірно, матиме суттєве значення для розробки проблеми безпеки кіберпростору / інформаційної безпеки, адже співпраця в цій сфері між США й Росією фактично не відбувалася, крім окремих заяв та декларацій. Тобто сьогодні на певному рівні

¹⁹⁵ 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/>

¹⁹⁶ Soldatkin Vladimir, Holland Steve. 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/>

в обох держав зберігається інтерес до продовження контактів щодо інформаційної безпеки, хоча б тому, що відсутність комунікації в цьому напрямі може призвести до неконтрольованої ескалації з важкопрогнозованими наслідками.

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

Діяльність США в ООН

58. Яка роль США в роботі Групи урядових експертів UN GGE?

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 у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки» і згодом розпочала роботу Група урядових експертів, США брали активну участь у її роботі, дотримуючись своїх принципів у питаннях безпеки кіберпростору. Так, уже 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 та відповідальної поведінки держав у сфері ІКТ. США змогли не лише 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 у сфері інформаційної безпеки Андрій Крутських (Російська Федерація головувала в ГУЕ у 2005 та 2010 рр., Австралія – у 2013 р., Бразилія – у 2015 й 2019–2021 рр., Німеччина – у 2016 р.).

59. Які наслідки діяльності Групи урядових експертів UN GGE та прийнятих нею рішень?

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 є¹⁹⁷ визнання того, що міжнародне право, зокрема Статут ООН і чотири принципи *jus in bello* – гуманності, необхідності, пропорційності й розрізнення (щоправда, без використання терміна МПП), 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 та додані з часом; рекомендовані конкретні заходи щодо зміцнення довіри, потенціалу й співробітництва; залучення регіональних міжнародних організацій, приватного сектору, наукових кіл.

Проте ці звіти не мають обов'язкового характеру. Досі політично та 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 diligence*, 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 задля дотримання відповідного міжнародного зобов'язання). Тому сформульовані заяви, засновані на правилах, та інші норми в списку зазначених одинадцяти норм залишаються малоприматними для виконання.

¹⁹⁷ 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/>

Необов'язковість згаданих норм сьогодні не дає можливостей урегулювати все гостріші проблеми кібербезпеки. Наприклад, правило *due dilligence* мало б застосовуватися в разі виявлення кібератаки, що походить із конкретної країни. Так, за підсумками телефонної розмови з президентом Росії в липні 2021 р., у 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»¹⁹⁸. Байден також повідомив про можливість наслідків, імовірно, якщо попередження не дасть очікуваних результатів.

60. У чому суть ініційованої США Резолюції ГА ООН «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки» (2018 р.)?

Після 2015 р. переговорний процес із питань кібернетичної безпеки застопорився і п'ятий склад ГУЕ у 2016–2017 рр. не зміг прийняти консенсусної доповіді. На цьому тлі у 2018 р. Росія вже вкотре висунула ініціативу, започатковану ще в 1998 р., під гаслом: «Досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки», наполягаючи на формуванні режиму «міжнародної інформаційної безпеки». Але з позиції США в 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

¹⁹⁸ 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/>

грудні 2018 р. Генеральною Асамблеєю ООН схвалено Резолюцію 73/266 «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки»¹⁹⁹, проєкт якої висунули Сполучені Штати спільно з 35 співавторами (139 за, 11 проти, 16 утрималися). Резолюцію підтримали переважно держави – члени ЄС, НАТО й інші союзники США, хоча низка країн (усього 77, уключаючи Індію, ПАР, Казахстан, Індонезію та ін.) голосували за обидві резолюції, американську й російську. Цікаво, що географія підтримки цих резолюцій відповідає розподілу країн за їх демократичним статусом, відповідно до щорічних звітів організації Freedom House²⁰⁰ – «не-вільні» країни підтримали російський проєкт, а «вільні» й переважно «частково-вільні» – американський.

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 країн у кіберпросторі у сфері міжнародної безпеки оголошено «забезпечення відкритого, інтероперабельного, надійного та безпечного інформаційно-комунікаційного середовища, виходячи з необхідності зберегти вільний потік інформації»²⁰¹.

Автори документа посилаються на результативну роботу Групи урядових експертів із досягнень у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки та відповідні доповіді Генерального секретаря за 2010, 2013 і 2015 рр., відповідно до яких міжнародне право й, зокрема, Статут Організації Об'єднаних Націй можуть бути застосовані й мають суттєво важливе значення для підтримки миру та стабільності й створення відкритого, безпечного,

¹⁹⁹ 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

²⁰⁰ Global Freedom Status. Freedom House. URL: <https://freedomhouse.org/explore-the-map?type=fiw&year=2021>.

²⁰¹ Там само.

стабільного, доступного та мирного інформаційно-комунікаційного середовища. Наголошено, що саме «добровільні й необов'язкові норми, правила та принципи відповідальної поведінки держав у сфері використання інформаційно-комунікаційних технологій можуть знизити ризик порушення міжнародного миру, безпеки й стабільності» і що «з урахуванням унікальних особливостей інформаційно-комунікаційних технологій із часом можуть бути розроблені додаткові норми»²⁰².

У преамбулі зазначено, що добровільні заходи зміцнення довіри можуть сприяти підвищенню ступеня довіри й установленню довірливих 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 використанням інформаційно-комунікаційних технологій та 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 наявних і потенційних загроз у сфері інформаційної безпеки, а також застосування міжнародного права 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) із питань інформаційної безпеки, і що мають бути опубліковані національні позиції учасників групи з питання застосування міжнародного права до використання ІКТ державами.

²⁰² Там само.

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

61. На яких засадах і з якою метою функціонує Робоча група відкритого складу, створена відповідно до Резолюції ГА ООН «Досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки» (2018 р.)?

З ініціативи РФ, відповідно до резолюції «Досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки»²⁰³ 2018 р., створено так звану Робочу групу відкритого складу (РГВС). На відміну від ГУЕ, що працює паралельно та 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 сектору, наукових кіл, організацій громадянського суспільства (остання ГУЕ натомість проводила епізодичні консультації з регіональними міжнародними організаціями – АС, ЄС, ОАД, 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, унесення в них виправлень або подання додаткових норм. Група мала вивчити можливість інституціалізації діалогу з питань застосування міжнародного права на регулярній основі під егідою ООН і

²⁰³ 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

досліджувати наявні 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 потенціалу, а також застосування міжнародного права до кіберпростору).

Із моменту заснування у 2019 р. РГВС залучила близько 150 країн і спостерігачів, а в березні 2021 р. представила остаточний проект звіту, що містить рекомендації щодо просування миру та безпеки в кіберпросторі й щодо якого досягнуто консенсусу²⁰⁴. У документі надано рекомендації для подальшого прогресу у сфері 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.

Стосовно 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 стосовно просування їхнього підходу до відповідальності за шкідливу кібердіяльність, яка порушує міжнародні норми: «Добровільні, необов’язкові норми відповідальної поведінки держави можуть зменшити ризики міжнародного миру, безпеки й стабільності та відіграють важливу роль у підвищенні передбачуваності й зменшенні ризиків помилкового сприйняття, сприяючи тим самим запобіганню конфліктів»²⁰⁵.

У звіті повністю підтримано позицію країн Заходу в тому, що міжнародне право, зокрема Статут Організації Об’єднаних Націй, є застосовним і важливим

²⁰⁴ 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>

²⁰⁵ 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>

для підтримки миру й стабільності та сприяння відкритому, безпечному, стабільному, доступному й мирному середовищу ІКТ. Певним компромісом із їхнього боку було включення посилання на можливість «міжнародних юридичних зобов'язань», усунення посилань на міжнародне гуманітарне право та зменшення акценту на правах людини. Також до міжнародного порядку денного внесено 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 для виборчих процесів.

Згадана консенсусна доповідь РГВС 2021 р.²⁰⁶ загалом відповідає позиції, сформульованій в опублікованій у 2019 р. Державним департаментом США «Спільній заяві про просування відповідальної поведінки держави в кіберпросторі»²⁰⁷, яку підтримали 26 інших країн – партнери «П'яти очей», 18 держав ЄС (уключно з Німеччиною та Францією), а також Норвегія, Японія, Південна Корея й Колумбія. У документі з посиланням на основу, закладену у 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 кіберінцидентів». Також підписанти підкреслюють, що вони за необхідності

²⁰⁶ 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>

²⁰⁷ Joint Statement on Advancing Responsible State Behavior in Cyberspace. URL: <https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/>

працюватимуть разом на добровільних засадах, щоб притягнути до відповідальності держави, що діють усупереч цим рамкам, «у тому числі шляхом ужиття заходів, які є прозорими й відповідають міжнародному праву», – «мають бути наслідки поганої поведінки в кіберпросторі»²⁰⁸. Також у документі підтримується цілеспрямоване нарощування потенціалу кібербезпеки для того, щоб відповідальні держави могли краще захистити свої мережі від руйнівної чи іншої дестабілізуючої кібердіяльності. Резолюцією ГА ООН 75/240 від грудня 2020 р. поновлено мандат РГВС на період із 2021 до 2025 рр. і в червні 2021 р. відбулося її організаційне засідання.

62. Які рішення прийнято UN GGE у період одночасної роботи з OEWG?

У травні 2021 р. (після прийняття першого звіту РГВС) прийнято черговий звіт ГУЕ²⁰⁹. У ньому, 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 – із часом деякі норми можуть трансформуватись у звичаєве міжнародне право чи авторитетні тлумачення наявних норм²¹⁰.

Також підтверджено застосовність міжнародного права, зокрема Статуту ООН загалом, до середовища ІКТ. Значним кроком уперед стало визнання того, що міжнародне гуманітарне право застосовується до кібероперацій під час збройного конфлікту. Група уточнила, що МГП застосовується лише в ситуаціях

²⁰⁸ Там само.

²⁰⁹ 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>

²¹⁰ Schmitt Michael. 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/>

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 конфліктів і не спонукає до них). Проте звіт ГУЕ 2021 р. став винятковим у тому сенсі, що досягнуто консенсусу, незважаючи на те, що Група 2016–2017 рр. не змогла опублікувати звіт, попри високу напруженість між ключовими гравцями у зв'язку з частотою й серйозністю кібератак, у яких США, Росія та Китай звинувачують одне одного.

Демократичні країни Заходу (США, Франція, Велика Британія, Канада, Німеччина й ін.) виступили проти резолюції щодо створення РГВСС. У 2018 р. США представили власну резолюцію з безпеки ІКТ (*Advancing responsible State behaviour in cyberspace in the context of international security*), у якій визначено новий мандат дії ГУЕ ООН. На цьому тлі привертає увагу резолюція A/RES/76/19²¹¹ Генеральної Асамблеї ООН, співавторами якої виступили США та Російська Федерація, у якій державам пропонується продовжувати інформувати Генерального секретаря про свої погляди й оцінки «зусиль, що вживаються на національному рівні для зміцнення інформаційної безпеки та сприяння міжнародному співробітництву в цій сфері». Резолюцією визнається діяльність обох форматів переговорів. І загалом це може оцінюватися як свідчення зближення позицій двох держав. Характерно, що певне знаходження позиції, котре допускає обидва погляди, відбулося після зустрічі президентів США й Росії в Женеві в червні 2021 р., де обговорювалися питання початку діалогу щодо кібербезпеки.

²¹¹ A/RES/76/19. Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies. *Resolution adopted by the General Assembly on 6 December 2021*. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/377/48/PDF/N2137748.pdf?OpenElement>

Підхід ЄС

63. Які засади політики ЄС у сфері інформаційної (кібер) безпеки?

Європейський Союз як регіональне інтеграційне об'єднання є найуспішнішим і найамбітнішим проектом міждержавної співпраці. Його специфіка полягає в суто прагматичних підходах до проблем, які мають суттєве й загальне значення для країн-членів. Тому в такому аспекті й розробляються всі комунітарні стратегії та реалізуються політики в розрізі окремих галузей або секторів. У контексті 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 то 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 проекту резолюції ГА ООН «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки»²¹² у 2018 р. Утім, окремі країни мають власні бачення перспектив міждержавного узгодження проблематики кібернетичної / інформаційної безпеки.

Безпека в цій сфері розглядається на рівні ЄС стосовно саме кібербезпеки й актуалізувалася недавно, у порівнянні зі США чи Росією, фактично лише після прийняття документа про стратегію кібербезпеки ЄС у 2013 р.²¹³ Але з того часу відбувається активний розвиток політики ЄС щодо кіберпростору. Починаючи з 2013 р., багато чого досягнули з погляду політики ЄС у сфері кібербезпеки, яка поставлена в центрі політичних пріоритетів Європейської комісії та набула

²¹² 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

²¹³ 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

актуальності в Стратегії єдиного цифрового ринку ЄС²¹⁴. Кібербезпека й боротьба з кіберзлочинністю є одним із трьох стовпів Європейського порядку денного щодо безпеки²¹⁵ (2015 р.), а в Глобальній стратегії ЄС²¹⁶ (2016 р.) вона вже трактується як горизонтальна політика унії, починаючи від загальнодоступного цифрового простору та закінчуючи елементами діяльності Європейського Союзу.

64. Яку роль відіграє політика кібербезпеки в Глобальній стратегії ЄС?

Глобальна стратегія ЄС (2016 р.)²¹⁷ утілює новий підхід до розуміння проблеми безпеки та загроз для громадян і самого Союзу, серед яких виокремлено й кіберзагрози поряд із гібридними загрозами, тероризмом, економічною нестабільністю, змінами клімату й енергетичними загрозами. Також у період, що збігається з часом президентства Трампа в США, у питаннях безпеки з боку ЄС проголошено 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

²¹⁴ 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>

²¹⁵ 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

²¹⁶ 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

²¹⁷ 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

партнера ЄС – США, і несподіваний прецедент виходу зі складу ЄС Великої Британії. Імовірно, ЄС шукатиме й використовуватиме відповідні можливості також на рівні зовнішньої політики. У сфері кібербезпеки Глобальна стратегія ЄС передбачає узгодження захисту комп'ютерних загроз із гарантією збереження «відкритого, вільного й безпечного кіберпростору» за зміцнення 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.

У середині ЄС посилюється спроможність відповіді на кіберзагрози та відновлення критично важливої інфраструктури держав-членів за збереження відкритого, вільного й безпечного кіберпростору. Буде посилено увагу до кібербезпеки, підвищено спроможність унії та забезпечено допомогу державам-членам у захисті від кіберзагроз зі збереженням при цьому відкритого, вільного й безпечного кіберпростору. ЄС підтримуватиме політичне, оперативне та технічне кіберспівробітництво 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 головними партнерами, як США й НАТО. Але основним меседжем для міжнародного співтовариства, уміщеним у тексті стратегії, є чітко висловлена позиція, що цілком відповідає західному (американському) підходу до забезпечення безпеки в кіберпросторі. Це – реалізація своєї прагматичної мети: стати «перспективним кібергравцем, захищаючи свої найважливіші активи й цінності в цифровому світі, зокрема за допомогою 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 наявного міжнародного права. Він підтримуватиме багатостороннє цифрове управління й глобальні рамки співпраці з кібербезпеки, поважаючи вільний потік інформації»²¹⁸. 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.

65. Як розвивається політика кібербезпеки ЄС?

Від початку розробки політики у сфері кібербезпеки ЄС орієнтувався більшою мірою на так звану м'яку безпеку: посилення зовнішнього виміру політики ЄС у сфері 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 у кіберпросторі. У 2016 р. Директивою про безпеку мереж та інформаційних систем (NIS)²¹⁹ 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 та ризики; сприяли розвитку кібербезпеки серед операторів критичної

²¹⁸ Там само.

²¹⁹ 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

інфраструктури. У цій сфері працюють спеціалізоване Агентство ЄС із питань безпеки мережі й інформації (ENISA), Європейський центр кіберзлочинності (EC3) у структурі Європолу, Команда ЄС із питань комп'ютерного реагування на надзвичайні ситуації (CERT-EU) та Європейське оборонне агентство.

Однак концепція стратегічної автономії, помітна в Глобальній стратегії ЄС (2016 р.), у найближчі роки, очевидно, вимагатиме відповідних заходів, підтриманих належним рівнем фінансування. Практичну реалізацію цього нового підходу розпочато з прийняттям у вересні 2017 р. так званого пакету кібербезпеки, із пропозицією низки заходів, які надалі координовано зміцнюватимуть структури та можливості ЄС у сфері кібербезпеки при повній співпраці держав-членів і різних зацікавлених структур ЄС.²²⁰

Наприкінці 2020 р. Європейська комісія й Високий представник Союзу із закордонних справ і політики безпеки презентували нову «Стратегію кібербезпеки для цифрового десятиліття»²²¹, 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 NIS2²²² про заходи щодо високого загального рівня кібербезпеки в усьому Союзі й нову Директиву щодо стійкості критичних організацій²²³. Разом ці документи становлять новий пакет із кібербезпеки. Доповнення європейського вторинного

²²⁰ 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>

²²¹ 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>

²²² 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>

²²³ 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

права у сфері кібербезпеки стало логічним кроком після врахування виявлених недоліків попередніх нормативних актів і викликів, що з'явилися у зв'язку з пандемією COVID-19.

66. Які головні положення Стратегії кібербезпеки ЄС для цифрового десятиліття (2020 р.)?

Стратегія кібербезпеки для цифрового десятиліття (2020 р.)²²⁴ покликана забезпечити відповідь на сучасні й потенційні кіберпов'язані виклики, що виникли з посиленням цифровізації та 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 й «усе частіше використовується в політичних та ідеологічних цілях», а ЄС «не має колективної ситуаційної обізнаності щодо кіберзагроз». Так формулюється складне завдання поліпшення кібербезпеки ЄС для захисту основних прав і свобод та 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 та відкритого кіберпростору.

ЄС планує побудувати мережу Оперативних центрів безпеки на всій своїй території, що працює на основі штучного інтелекту, щоб створити європейський «щит кібербезпеки»²²⁵, розгорнути надзвичайно безпечну інфраструктуру квантового зв'язку для Європи для передачі конфіденційної інформації й

²²⁴ 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>

²²⁵ 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

упровадити низку інших інструментів і заходів, наприклад зміцнити інструменти кібердипломатії, розробити план дій на випадок надзвичайних ситуацій «для вирішення екстремальних сценаріїв, що впливають на цілісність та доступність глобальної кореневої системи DNS», установити стандарти безпеки.

Підвищити безпеку інтернету й інших важливих мереж та інформаційних систем планується шляхом утворення «Європейського центру компетенції з питань промислової, технологічної та дослідницької роботи з кібербезпеки»²²⁶, – для об'єднання інвестицій у дослідження кібербезпеки, технології й промисловий розвиток. Новий орган розмістять у Бухаресті, він працюватиме разом із мережею національних координаційних центрів, призначених державами-членами та ENISA.

Відзначимо, що 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 закликає забезпечити захист пов'язаних продуктів і супутніх послуг, уключаючи ланцюжки поставок, із погляду стійкості до кіберінцидентів, наголошує на необхідності встановлення вимог кібербезпеки щодо програм, програмного забезпечення, убудованого програмного забезпечення (яке контролює різні пристрої й машини, що не є комп'ютерами) та операційних систем (програмне забезпечення, що виконує основні функції комп'ютера) до 2023 р.²²⁷. Цілком імовірно, що реалізація таких вимог матиме наслідки, подібні до обмеження присутності на ринку відповідних продуктів іноземного виробництва, як це було в США.

На перший погляд, європейська стратегія за масштабом нагадує підхід Китаю, що полягає в державному управлінні й спрямовуванні економіки та

²²⁶ 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/>

²²⁷ 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

всього 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 та телекомунікацій.

Нова стратегія передбачає значне збільшення коштів у сфері кібербезпеки, зокрема в рамках програми досліджень й інновацій, стратегічної інвестиційної програми «Цифрова Європа» та програми «Горизонт Європа», а також у рамках Плану відновлення для Європи²²⁸. Мета – залучити до 4,5 млрд євро спільних інвестицій із ЄС, держав-членів та промисловості.

67. Які пріоритети в політиці кібербезпеки ЄС актуалізуються з прийняттям стратегії «Цифровий компас: європейський шлях до Цифрового десятиліття»?

У березні 2021 р. Комісія виклала своє бачення цифрової трансформації Європи до 2030 р. в Комюніке «Цифровий компас: європейський шлях до Цифрового десятиліття»²²⁹, у якому фактично виклала «європейське» бачення цифрового суверенітету, що полягає в амбітному плані щодо проведення цифрової політики, що передбачає усунення вразливих місць і залежностей, а також прискорення інвестицій задля випереджаючого розвитку ЄС у відкритому й узаємопов'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 та надійне онлайн-середовище, цифрові медичні послуги, цифрові

²²⁸ 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 доповняють наявні права, що вже захищають і розширюють можливості європейців в інтернеті, такі як захист особистих даних та конфіденційності, свобода висловлення поглядів, свобода створення й ведення бізнесу в інтернеті й захист інтелектуальної власності.

У середовищі безпеки, що швидко розвивається, Стратегічний компас передбачає необхідність розробки всеохопної політики, що могла б допомогти подолати комплексні загрози проти ЄС, дотримуючись чіткої політичної мети, що може мати форму гібридного інструментарію ЄС, охоплює заходи проти кібератак, дезінформації, а також інших форм утручання, таких як використання міграційних потоків як інструментів гібридних атак проти ЄС²³⁰. Це – доповнення до поточних напрямів роботи в контексті посилення Стратегії кібербезпеки ЄС, уключаючи інструментарій кібердипломатії. У такій ширшій рамці Компас також пропонує розробити подальші заходи для протидії маніпуляції з іноземною інформацією²³¹. Перший проєкт Стратегічного компаса представлено в листопаді 2021 р., а прийнято 21 березня 2022 р.²³²

Прийняття нової стратегії тепер здійснювалося з урахуванням викликів, пов'язаних з ескалацією агресивної політики РФ, – з'явилася гостра необхідність у посиленні позицій ЄС і його партнерів, зокрема України. Мета Стратегічного компаса – зробити ЄС сильнішим та більш спроможним гарантом безпеки. ЄС має бути в змозі захистити своїх громадян і сприяти міжнародному миру й

²³⁰ Questions and answers: a background for the Strategic Compass. *EEAS*. 2021. URL: https://eeas.europa.eu/headquarters/headquarters-homepage/97895/questions-and-answers-background-strategic-compass_en

²³¹ A Strategic Compass for a stronger EU security and defence in the next decade. *Council of the EU. Press release*. 2022. URL: <https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>

²³² A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security URL: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>

безпеці. Це особливо важливо в той час, коли війна повернулася до Європи після невинуватеної та неспровокованої агресії Росії проти України, а також серйозних геополітичних зрушень. Стратегічний компас посилить стратегічну спроможність ЄС і його здатність працювати з партнерами для захисту своїх цінностей та інтересів. Сильніший і більш спроможний ЄС у сфері безпеки й оборони сприятиме глобальній і трансатлантичній безпеці та доповнює НАТО, що залишається основою колективної оборони для його членів. Це також посилить підтримку глобального порядку, заснованого на правилах, ядром якого є Організація Об'єднаних Націй.

68. На яких концептуальних підходах засновано сучасну стратегію ЄС у сфері кібербезпеки?

Європейський Союз орієнтований на західну (американську) концепцію в питаннях розвитку кіберпростору та його безпеки. Відповідно до нової стратегії (2020 р.), унія активізуватиме роботу з міжнародними партнерами щодо зміцнення заснованого на правилах глобального порядку, сприяння міжнародній безпеці й стабільності в кіберпросторі, захисту прав людини та основних свобод в інтернеті, просуватиме міжнародні норми й стандарти, що відображають ці основні цінності ЄС, співпрацюючи зі своїми міжнародними партнерами в ООН та 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 (UN GGE) у галузі інформації та телекомунікацій у контексті міжнародної безпеки, схвалених Генеральною Асамблеєю ООН. Загалом така позиція відповідає й консенсусному звіту Робочої групи відкритого складу 2021 р.

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 та просування прав людини й основних свобод в інтернеті. Із цією метою ЄС повинен сприяти подальшому дотриманню міжнародного законодавства та стандартів у сфері прав людини, зокрема Статуту ООН і Загальної декларації прав людини, а також упроваджувати в життя прийнятий у ЄС у листопаді 2020 р. План дій із прав людини й демократії на 2020–2024 рр²³³. Також у цьому контексті потрібно згадати прийняті в ЄС у 2014 р., але актуальні й у стратегічній перспективі Настанови з прав людини щодо свободи висловлення поглядів у інтернеті та офлайн²³⁴.

Ще одним пунктом, у якому позиція ЄС збігається з американською й протилежна російській, є міжнародна співпраця у сфері протидії кіберзлочинності. ЄС дотримується Будапештської конвенції Ради Європи про кіберзлочинність і заявляє про підтримку третіх країн, котрі 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 та 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 у 2017 р. проекту конвенції ООН «Про співпрацю у сфері протидії інформаційній злочинності», який «ризикує посилити розбіжності й уповільнити

²³³ 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>

²³⁴ 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>

настільки необхідні національні реформи та 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»²³⁵.

69. У чому суть пропозиції Програми дій для просування відповідальної поведінки держав у кіберпросторі? Яка роль ЄС у її просуванні?

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 та 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 потрібно відзначити проактивну позицію окремих держав-членів і самого ЄС. У жовтні 2020 р. Франція, Єгипет та 40 інших держав (Аргентина, Колумбія, Еквадор, Габон, Грузія, Японія, Марокко, Норвегія, Сальвадор, Сингапур, Республіка Корея, Республіка Молдова, Республіка Північна Македонія, Сполучене Королівство, ЄС і його держави-члени) запропонували²³⁶ програму дій (ПД) для просування відповідальної поведінки держав у кіберпросторі²³⁷. У світлі багаторічної конкуренції між російсько-китайським та західним підходами до інформаційної безпеки / безпеки

²³⁵ Там само.

²³⁶ 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>

²³⁷ Там само.

кіберпростору це було 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 Робочої групи відкритого складу. Її основним прихильником, очевидно, є Франція, підтримана ЄС і всіма його членами, а також низкою держав, орієнтованих переважно на реалізацію західного підходу в питаннях кібербезпеки. Ці країни заявляють, що хотіли б, замість розділеної між ГУЕ й РГВС дискусії, бачити один постійний форум, який би займався питаннями використання державами ІКТ у контексті міжнародної безпеки. Як модель вони пропонують узяти формат, власне, програм дій – за аналогією, наприклад, з уже наявними програмами дій – щодо запобігання й викорінення незаконної торгівлі стрілецькою зброєю та легкими озброєннями в усіх її аспектах і боротьби з нею, щодо інвалідів, расизму, найменш розвинених країн, заборони підбурювання до насильства й 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 всеосяжно та ретельно).

Два оформлених раніше треки, ГУЕ (UN GGE) й РГВС (OEWG), є результатом стратегічної конкуренції між Росією та США. За цих обставин дипломатичні спроби досягти успіху одного процесу в конкуренції з іншим, найімовірніше, призведуть до невдачі обох. Тому реалізація Програми дій з кіберпитань – це третій варіант, той, який може створити більш відкритий і всебічний переговорний процес, не потрапляючи в пастку наявної дуополії²³⁸.

²³⁸ Géry Aude. 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/>

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

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

У Стратегії кібербезпеки ЄС 2020 р., яка побачила світ майже відразу після ініціативи щодо ПД, існує 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 наявний 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, що ініціативу ПД не підтримали ні Росія, ні Китай, що зрозуміло з погляду їх просування концепцій міжнародної інформаційної безпеки та 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. Урешті, у досягненні консенсусу на рівні РГВС у березні 2021 р., імовірно, певну роль відіграли 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 із боку провідних кібердержав може бути пов'язана з вичікуванням більш конкретного оформлення цієї нової пропозиції, а також бажанням уникнути поляризації під час дебатів.

ВЗАЄМОДІЯ МІЖ ДЕРЖАВАМИ У СФЕРІ ІНФОРМАЦІЙНОЇ (КІБЕР) БЕЗПЕКИ

Міжнародна діяльність Китаю у сфері кібербезпеки

70. Із якою метою проводиться Всесвітня інтернет-конференція й започатковано Уженську ініціативу?

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 кіберуправлінні, протистояння кібергегемонії²³⁹. Також Китай не схвалює проведення, потурання та підтримку будь-яких дій, які можуть загрожувати кібербезпеці інших держав²⁴⁰.

Віднедавна Китай претендує на роль провідного актора у сфері, пов'язаній із розвитком інтернету, зокрема у 2014 р. ним започатковано Всесвітню інтернет-конференцію, щорічний форум для обговорення глобальних питань і політики інтернету. Уже на першій Всесвітній інтернет-конференції невідома сторона розповсюдила проєкт спільної заяви, що підтверджує право окремих країн розвивати, використовувати й керувати інтернетом (котрий, проте, офіційно не розглядався)²⁴¹. А на другій конференції у 2015 р., у якій узяли участь очільник Китаю та керівники урядів низки держав, Сі Цзіньпін закликав світ «поважати

²³⁹ Hao Yeli. A Three-Perspective Theory of Cyber Sovereignty. 2017. URL: <https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model>

²⁴⁰ Zunyou Zhou. China's Draft Cybersecurity Law. *China Briefing*. 2015. 15. No. 24 (December 21, 2015). URL: <https://jamestown.org/program/chinas-draft-cybersecurity-law/>.

²⁴¹ China Delivers Midnight Internet Declaration – Offline. *The Wall Street Journal*. Nov. 21, 2014. URL: <https://www.wsj.com/articles/BL-CJB-24963>

інтернет-суверенітет кожної країни, поважати право кожної держави вибирати власний шлях розвитку й модель управління інтернетом»²⁴².

Тоді ж започатковано Уженську ініціативу, яка закликає всі країни сприяти розвитку інтернету, ділитися плодами його розвитку й покращувати глобальне управління мережею, сприяти культурному різноманіттю та забезпечувати мир і безпеку в кіберпросторі ²⁴³. Проте із західної позиції ця ініціатива була 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 та нагляд стали нормою скрізь. Це повний напад на свободи інтернету»²⁴⁴.

71. Які головні напрями міжнародної стратегії Китаю в кіберсфері?

Головним на сьогодні документом, у якому розкрито підходи Китаю до інформаційної безпеки на міжнародному рівні, є прийнята у 2017 р. «Міжнародна стратегія співробітництва в кіберпросторі». У цьому документі цілком і повністю відображено китайське розуміння кіберпростору та його безпеки, передусім домінуючої ролі держави в управлінні мережею, відповідно до національного бачення системи міжнародної взаємодії. В основу стратегії покладено чотири принципи – миру, суверенітету, спільного управління й спільної вигоди²⁴⁵. Ці принципи – в основі 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

²⁴² Xi Jinping calls for 'cyber sovereignty' at internet conference. *BBC*. 2015-12-16. URL: <https://www.bbc.com/news/world-asia-china-35109453>

²⁴³ Zhu, Shenshen. Wuzhen initiative on Internet future. *Shanghai Daily*. 29 December 2015. URL: <https://archive.shine.cn/business/it/Wuzhen-initiative-on-Internet-future/shdaily.shtml>

²⁴⁴ Griffiths, James. 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>

²⁴⁵ 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

справедливий і розумний міжнародний порядок у кіберпросторі на основі суверенітету держави», вестиме активну роботу над досягненням міжнародного консенсусу у зв'язку з цим, висловлює незгоду з «тенденцією мілітаризації та стримування в кіберпросторі», яка «не сприяє міжнародній безпеці й стратегічній узаємній довірі», і що «жодна країна не повинна прагнути до кібергегемонії». Очевидним є натяк на американську ініціативу кіберстримування, у якій серед носіїв потенційних кіберзагроз разом із 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 та участь у міжнародному співробітництві, запобіганні великій кіберкризі, у захисті кіберпростору й підтримці національної безпеки й соціальної стабільності».

По-друге, Китай знову послідовно підтверджує свою позицію щодо відходу від нинішньої моделі управління інтернетом, у якій політику мережі формують різні гравці – уряди, компанії й громадянське суспільство, у напрямі багатостороннього прийняття рішень між урядами, зокрема на платформі ООН: «відповідні зусилля повинні відображати широку участь, розумне управління та демократичне прийняття рішень, при цьому всі зацікавлені сторони роблять внесок у свою частку залежно від власних можливостей, а уряди посідають 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»²⁴⁶.

Китай підтримував та брав активну участь у процесі прийняття міжнародних правил і декларує, що продовжуватиме це за допомогою «посилення діалогу й співпраці з міжнародним співтовариством». У цьому

²⁴⁶ Там само.

аспекті наголошено на важливості прийнятого у 2015 р. 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 та 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, у розбудові можливостей кібербезпеки, включаючи передачу технологій, розвиток критичної інформаційної інфраструктури й навчання персоналу.

72. Які головні напрями реалізації кіберстратегії Китаю в регіональних відносинах?

Китай, завжди послідовний у своїй політиці, відповідно до прийнятої у 2017 р. «Міжнародної стратегії співробітництва в кіберпросторі»²⁴⁷, продовжуватиме проводити щорічну Всесвітню 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 та, звісно ж, розвиватиме співпрацю й свою позицію в напрямі кібербезпеки в рамках ШОС і БРІКС.

Відповідно до цієї стратегії, Китай планує закріпити за собою місце лідера й у регіональних відносинах із приводу політики у сфері кібербезпеки. Він заохочуватиме й підтримуватиме в цьому напрямі регіональні організації з

²⁴⁷ 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

різних частин світу, де він має сильні позиції, включаючи Нараду зі взаємодії та зміцнення заходів довіри в Азії (СІСА), Форум китайсько-африканського співробітництва (ФОСАС), Форум співробітництва між Китаєм й арабськими державами, Форум Китаю та 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 та, поза сумнівом, досліджуватиме можливості діалогу щодо кіберпростору з іншими регіональними організаціями.

73. У чому полягають принципові відмінності між підходами до безпеки кіберпростору в Китаї та США?

Головним інтересом китайської політики у сфері інформаційної (кібер) кібербезпеки 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 в питанні розв'язання проблеми управління кіберпростором. І Китай, і США виступають за правила кіберуправління всередині країни й на міжнародному рівні, але їхні 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 кіберуправлінні, 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 та 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.

74. У діяльності яких міжнародних організацій проявляється узгодження позицій Китаю та Росії в питаннях безпеки кіберпростору?

В аспекті міжнародних відносин китайська позиція концептуально збігається з російською, адже КНР послідовно відстоює претензії на виокремлення зі світової інформаційної 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 проекти 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 у 2006 р. прийнято Заяву головних держав-членів із міжнародної інформаційної безпеки²⁴⁸, у якій інформаційну безпеку оголошено важливим фактором забезпечення державного суверенітету, національної безпеки, соціально-економічної стабільності. У рамках угоди між державами у 2009 р. визначено перелік загроз, зокрема такі, що традиційно наголошуються Росією на міжнародних майданчиках, зокрема «використання домінуючого становища в інформаційному просторі на шкоду

²⁴⁸ 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>.

інтересам і безпеці інших країн» та «розповсюдження інформації, що завдає шкоди суспільно-політичній і соціально-економічній системам, духовному, моральному й культурному середовищам інших держав»²⁴⁹.

У рамках ШОС за участі Китаю проведено чимало зустрічей і прийнято низку декларацій, у яких відзначено 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 порушуються 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 виконуваної в ООН діяльності з вироблення правил, норм і принципів відповідальної поведінки держав в інформаційному просторі й підтверджено намір продовжити спільну роботу та 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», у тому числі забезпечення рівних прав держав на участь у процесі управління мережею «Інтернет»²⁵⁰.

Ще одним майданчиком, на якому Китай просуває свої позиції, котрі принципово збігаються з російськими, стала група БРІКС (Бразилія, Росія, Індія, Китай, Південно-Африканська Республіка). Цей форум потужних держав, які концентрують понад сорок відсотків населення планети й характеризуються

²⁴⁹ 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>

²⁵⁰ 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>

швидкими темпами інформатизації суспільства, кожна сторона використовує на свою користь, але в питаннях інформаційної безпеки / безпеки кіберпростору вони мають подібне бачення. Це стосується, зокрема, підходу до вироблення спільних правил для кіберпростору й тяжіння до інформаційного (кібер) суверенітету.

Ці питання порушуються на самітах БРІКС і поступово набувають усе більш виразних формулювань у підсумкових документах. Так, на бразильському (2019 р.) саміті БРІКС прийнято декларацію, у 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 та підтримуємо центральне значення Організації Об'єднаних Націй у їх розвитку»²⁵¹. Ще раніше, на Сяменьському саміті організації, організованому Китаєм на своїй території, у тексті прийнятої декларації розтлумачено позицію держав-членів із питань безпеки кіберпростору, з указівкою на те, що «ООН відіграє центральну роль у розробці загальноновизнаних норм відповідальної поведінки держав у використанні ІКТ для забезпечення мирного, безпечного, відкритого, кооперативного, стабільного, упорядкованого, доступного й справедливого середовища ІКТ»²⁵². 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, прийнятих ШОС в Етеквіні, Форталезі, Уфі та Гоа. Країнами – членами БРІКС утворено Робочу групу з питань безпеки в застосуванні інформаційно-комунікаційних технологій (WGSICT), і Дорожню

²⁵¹ 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

²⁵² 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>

карту практичного співробітництва БРІКС щодо забезпечення безпеки використання ІКТ.

Потрібно зазначити, що країни – члени БРІКС у питаннях кібербезпеки й підходів до політики ІКТ мають дещо відмінні позиції. Так, Росія подає пропозиції 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, але бере участь у всіх відповідних проєктах БРІКС і, урешті, ситуація у сфері безпеки кіберпростору на цьому форумі еволюціонує в потрібному для КНР напрямі. Зокрема, отримала розвиток концепція цифрового суверенітету, активно пропагована Китаєм. Серед його партнерів по БРІКС, окрім Росії, також Індія наполегливо намагається зберігати дані про громадян на комп'ютерах усередині країни, а не за кордоном²⁵³. Робота в напрямі формування узгодженого підходу до кібербезпеки ведеться в рамках БРІКС у різних площинах, зокрема науковій, де ініційовано міжінституційний проєкт CyberBRICS, котрий має на меті передусім «зіставити наявні нормативні документи, визначити найкращі практики й розробити пропозиції щодо політики у сферах управління кібербезпекою (уключаючи регулювання персональних даних), політики доступу до інтернету» в країнах БРІКС²⁵⁴.

Проблеми взаємодії США й Китаю у сфері кібербезпеки

75. У чому суть протистояння між США й Китаєм у сфері кібербезпеки?

Тема кібербезпеки є більш сучасною, ніж численні інші питання в історії відносин між Сполученими Штатами й Китаєм. Проте швидкий розвиток

²⁵³ Basu Arindrajit, Hickok Elonnai and Chawla Aditya Singh. 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/>

²⁵⁴ Cyberbricks. About us. URL: <https://cyberbrics.info/about-us/>

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 та Китаєм ставали більш напруженими. Це результат збільшення кількості проблем кібершпигунства з боку обох країн, що призвело до того, що ці дві держави найчастіше звинувачуються в атаках кібершпигунства²⁵⁵. США винуватять Китай у тому, що з його боку нерідко здійснюються кібератаки з метою втручання в бізнес-інтереси та різні комерційні справи, такі як крадіжка комерційної таємниці, інтелектуальної власності для нових технологій та іншої інформації, щоб отримати комерційну вигоду. І навпаки, Китай часто інкримінує Сполученим Штатам те, що вони домінують в інтернеті й використовують своє становище у світі кіберпростору для пошуку вигідних ситуацій і збору розвідданих²⁵⁶.

У низці кібератак США на підставі проведених розслідувань мають підстави звинувачувати Китай. 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 роботу різних груп у сфері кібершпигунства. АРТ1 – це назва діяльності, яку виконували багато членів підрозділу 61398 Народно-визвольної армії Китаю. У звіті показано, що з 2006 р. до 2013 р. в ході АРТ1 зламано й викрадено сотні терабайтів інформації з більш як 140 компаній

²⁵⁵ Julian Nicholas. 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>

²⁵⁶ Brown, G., Yung, C. D. Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace. *The Diplomat*. 2017. URL: <https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/>

із 20 галузей²⁵⁷. Можна припустити, що значна частина цілей хакерських атак у США пов'язана не лише з АРТ1, але й із багатьма іншими загрозами, що використовував китайський уряд.

У 2014 р. Міністерство юстиції США висунуло звинувачення п'ятьом чиновникам китайської армії в незаконному отриманні та розповсюдженні 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 у його причетності до кіберзлочинів. Після арешту й висунення звинувачення військовослужбовцям китайської армії в Сполучених Штатах китайські ЗМІ назвали це помстою, щоб зберегти обличчя після скандалу з витоком інформації через Едварда Сноудена, представника американських інформаційних спецслужб, який утік у невідомому напрямі у 2013 р. Пізніше того самого року Агентство національної безпеки США повідомило, що Китай здійснив величезну кількість кібератак проти Сполучених Штатів за короткий проміжок часу, і сотні з них були успішними²⁵⁸.

Унаслідок постійного протистояння, яке простежено 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 у 2015 р. й засновано на посиленні комунікації та співпраці між ними. Також у документі підтверджено, що жодна зі сторін не буде свідомо здійснювати крадіжку інтелектуальної власності в іншій стороні. Також

²⁵⁷ Mandiant Consulting Services. *APT1: Exposing One of China's Cyber Espionage Units*. 2013. URL: <https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf>

²⁵⁸ Brown G., Yung C. D. 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*. 2017. URL: <https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/>

погоджено розробити та запропонувати належні норми поведінки між державами для кіберпростору в міжнародному співтоваристві²⁵⁹.

Останніми роками відносини між Китаєм і Сполученими Штатами стають усе більш напруженими. На жаль, зазначена вище угода проіснувала недовго, оскільки обидві сторони вчинили дії, що 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 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, що 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 Intel²⁶⁰.

Китайські атаки на фірми зі Сполучених Штатів й урядові ресурси не залишилися 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 ²⁶¹. Хоча, як припускають автори подібних

²⁵⁹ Brown G., Yung C. D. 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*. 2017. URL: <https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/>

²⁶⁰ Greenberg A. China tests the limits of its U.S. hacking truce. *Wired*. October 13. 2017. URL: <https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/#>

²⁶¹ 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>

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.

76. Який характер має конкуренція між США й Китаєм в аспекті кіберможливостей?

Світовими лідерами у 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 кіберспроможності п'ятнадцяти найбільших світових гравців у сфері хакерства й цифрового захисту. У звіті оцінюються можливості як уряду, так і приватного сектору. Найбільш потужних супротивників США, Росію й Китай, віднесено до другого рівня кіберпотужності, так само, як Великобританію, Канаду, Австралію, Ізраїль і Францію²⁶².

Китай досяг значного прогресу у зміцненні своїх кіберможливостей, 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, зокрема²⁶³:

- домінуючим військовим потенціалом як у наступальних, так і в оборонних кіберспроможностях;

²⁶² Cyber Capabilities and National Power: A Net Assessment. *IJSS. Research Papers*. 28th June 2021. URL: <https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/>

²⁶³ Schaffer Aaron. The Cybersecurity 202: The United States is still number one in cyber capabilities. *The Washington Post*. June 28. 2021. URL: <https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/>

- провідним у світі персоналом американських технологічних компаній і компаній із кібербезпеки;
- системним державним підходом до кібербезпеки й управління ризиками.

Проте швидкий цифровий розвиток Китаю та зростаюча кількість технологічних фірм роблять його «єдиною державою, яка зараз має намір приєднатися до США на першому рівні кіберпотужності»²⁶⁴. Найважливішим фактором для загальної кіберспроможності країни є наявність кадрів вітчизняних компаній, зосереджених на інформаційно-комунікаційних технологіях, які можуть розвивати кіберспроможності. Саме це дає Китаю з його численними технологічними й телекомунікаційними компаніями, що швидко розвиваються, найкращі шанси кинути виклик позиції Сполучених Штатів на вищому рівні.

77. Як формувалося розуміння Китаю як джерела кіберзагроз для США?

Китай активно розвиває свій кіберпростір – і це дає підґрунтя також для активізації кіберзлочинності й виникнення інших кіберзагроз. Із початком епохи соціальних мереж та масового використання інтернету задля ведення бізнесу стали з'являтися повідомлення про китайських кіберзлочинців і кібершпигунів. Але якщо десятиліття тому більшість виявлених фактів асоціювалася з використанням низькорівневих фішингових електронних листів проти американських компаній та крадіжкою інтелектуальної власності, то до сьогодні хакерські атаки з Китаю перетворилися на серйозно організовані операції, а сам Китай сприймається у США як досвідчений і зрілий супротивник²⁶⁵.

²⁶⁴ Cyber Capabilities and National Power: A Net Assessment. *IJSS. Research Papers*. 28th June 2021. URL: <https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/>

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

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 понад двадцять інших компаній стали жертвами складної кібератаки, яка пізніше отримала назву *Operation Aurora*, із боку хакерів Китаю, котра 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 ІТ-компанії *Symantec* повідомили, що хакери, які стоять за операцією «Аврора», зосередилися 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 працюють із програмним забезпеченням²⁶⁶.

У 2013 р. китайців звинувачено в атаці на *New York Times*. Хакери, імовірно з Китаю, здійснювали маршрутизацію через мережу газети протягом щонайменше чотирьох місяців, викрадаючи паролі репортерів в очевидній спробі ідентифікувати джерела та зібрати інші розвідувальні дані про історії, пов'язані із сім'єю прем'єр-міністра Китаю Вен Цзябао. Злам збігся з розслідуванням, опублікованим газетою *Times* за рік до того, яке розглядало статки, котрі 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,

²⁶⁶ Finkle Jim. Hundreds more cyber attacks linked to 2009 Google breach. *Reuters*. Sept. 12. 2012. URL: <https://www.reuters.com/article/cybersecurity-espionage-idUSL2E8K7A9E20120907>

який проводив розслідування, а також керівника південноазійського бюро газети в Індії Джима Ярдлі, котрий раніше працював у Пекіні²⁶⁷.

У 2014 р. президент США Барак Обама назвав кібератаки «реальною загрозою» безпеці й економіці США. Сполучені Штати звинуватили офіцерів китайської армії в кіберзламі американських компаній приватного сектору задля отримання конкурентної переваги. Генеральна прокуратура США стверджує, що офіцери викрали комерційні таємниці та внутрішні документи в п'яти компаній і профспілки. Проте Китай відкинув звинувачення й попередив, що ця справа зашкодить американо-китайським відносинам²⁶⁸.

Сполучені Штати, очевидно, мали підстави для таких звинувачень, оскільки на початку 2013 р. компанією *Mandiant*, що надає послуги у сфері кібербезпеки, опубліковано результати розслідування, у 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»²⁶⁹.

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 і військовій розвідці²⁷⁰. У період 2002–2012 рр., за висновками американської компанії з кібербезпеки *Fireeye*, у рамках діяльності цієї групи

²⁶⁷ Zetter Kim. New York Times Hacked Again, This Time Allegedly by Chinese. *Wired*. 01.31.2013. URL: <https://www.wired.com/2013/01/new-york-times-hacked/>

²⁶⁸ US justice department charges Chinese with hacking. *BBC*. 14 May, 2014. URL: <https://www.bbc.com/news/world-us-canada-27475324>

²⁶⁹ 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/>

²⁷⁰ Cyber Threat Intelligence on Advanced Attack Groups and Technology Vulnerabilities. Threat Intelligence Reports. *Fireeyes*, 2013.

здійснено понад тисячу кібератак проти великих компаній та відомих політиків. Невдовзі після першого візиту китайського лідера Сі Цзіньпіна до США у 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 спостерігали помітне зменшення інтенсивності китайського хакерства²⁷¹.

78. Як сьогодні розглядається Китай стосовно кібербезпеки США?

Після того, як президент Дональд Трамп вступив на посаду й ініціював торговельні конфлікти та інші напруження з Китаєм, хакерські атаки відновилися. Причому змінилися як їх джерело, так і суть. Хакерів НВАК замінили оперативники, котрі працюють за дорученням Міністерства державної безпеки, що керує розвідкою, безпекою й таємною поліцією Китаю. Тепер реалізатори кібернападів 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 слабоафілійованими хакерами: або їм платили готівкою, або в них не було іншого вибору, окрім як робити все, що просить держава²⁷².

Особливо активізувалися зловмисники на початку 2020-х рр. Так, у липні 2021 р. Сполучені Штати звинуватили Китай у кібератаках, відзначивши, що ці атаки були дуже агресивними. Це є ознака того, що Китай перетворився на 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 кібершпиунства, зібравши надзвичайно широку коаліцію країн, до якої приєдналися країни НАТО,

²⁷¹ 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>

²⁷² Wolfe Derek. How China Became a Digital Adversary and Threat to the U.S. *GSIXchange*. July 21.2021. URL: <https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/>

Європейського Союзу, Австралія, Великобританія, Японія й Нова Зеландія. Держсекретар США Ентоні Блінкен заявив, що ця атака становить «велику загрозу нашій економічній та національній безпеці»²⁷³.

Одночасно Міністерство юстиції США висунуло звинувачення чотирьом громадянам Китаю – трьом співробітникам служби безпеки й одному хакеру-зламнику – у нападі на десятки компаній, університетів і державних установ у Сполучених Штатах та за кордоном²⁷⁴. 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 китайські університети звинувачено 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 указував 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 в кібератаках із боку адміністрації президента США свідчать, що Китай за останні роки реорганізував свої хакерські операції. Якщо колись практикувалися відносно прості хакерські атаки на іноземні компанії, аналітичні центри й державні установи, то сьогодні здійснюються приховані, децентралізовані цифрові напади на американські компанії та інтереси в усьому світі. За словами американських чиновників і представників ділових кіл, хакерські дії, що реалізувалися підрозділами Народно-визвольної армії Китаю через непрофесійно сформульовані електронні листи (фішинг), тепер

²⁷³ @SecBlinken [Secretary Antony Blinken]. *United States government official*. 19 лип. 2021. URL: <https://twitter.com/secblinken/status/141710360213347942>

²⁷⁴ 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/>

здійснюються елітною мережею з підрядних компаній та університетів, які працюють за вказівкою Міністерства державної безпеки Китаю²⁷⁵.

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 періоду²⁷⁶. «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*, 2021²⁷⁷).

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 та 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

²⁷⁵ Perlroth Nicole. How China Transformed Into a Prime Cyber Threat to the U.S. *The New York Times*. July 19. 2021. URL: <https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html>

²⁷⁶ Там само.

²⁷⁷ Wolfe Derek. How China Became a Digital Adversary and Threat to the U.S. *GSIXchange*. July 21.2021. 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 Штатів²⁷⁸.

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

Сьогодні американська розвідка конкретизує такі основні кіберзагрози з боку Китаю²⁷⁹:

- Китай може здійснювати кібератаки, що можуть спричинити щонайменше локалізовані тимчасові порушення роботи критичної інфраструктури в Сполучених Штатах;
- Китай є світовим лідером із застосування систем спостереження й цензури для моніторингу свого населення та придушення інакомислення, особливо серед етнічних меншин, таких як уйгури. Пекін проводить кібервтоврнення, які впливають на громадян США й інших громадян за межами його кордонів, наприклад хакерство журналістів, крадіжка особистої інформації або атаки на інструменти, що дають змогу вільно

²⁷⁸ Neumann Scott. Intelligence Chiefs Say China, Russia Are Biggest Threats To U.S. *NPR*. April 14. 2021. URL: <https://www.npr.org/2021/04/14/987132385/intelligence-chiefs-say-china-russia-are-biggest-threats-to-u-s>

²⁷⁹ 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>

- висловлюватися в інтернеті, як частину зусиль щодо спостереження за уявними загрозами владі КПК та адаптації зусиль щодо впливу;
- Пекін використовує свою участь у глобальних зусиллях із боротьби з COVID-19 для експорту власних інструментів і технологій спостереження;
 - операції з кібершпигунства в Китаї включали компрометацію телекомунікаційних фірм, постачальників керованих послуг та програмного забезпечення, що широко використовується, а також інших цілей, що створює можливості для потенційного збору розвідувальної інформації, атак або операцій впливу.

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 у 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 або інше виявлення недоліків), такі як використовувалися для атаки на *Microsoft Exchange*. Уже у 2016 р. влада раптово закрила найвідомішу приватну платформу Китаю для звітності про нульові дні й заарештувала її засновника²⁸⁰. Через два роки китайська поліція оголосила, що почне виконувати закони, котрі забороняють «несанкціоноване розкриття» вразливостей. Того самого року китайські хакери, які регулярно брали участь у великих західних хакерських конгресах, перестали з'являтися навіть на запрошення²⁸¹.

²⁸⁰ 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>

²⁸¹ 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/>

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»²⁸².

79. Із яких позицій влада Китаю розглядає США в аспекті кібербезпеки?

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»²⁸³. А нову жорстку американську політику кібербезпеки щодо Китаю в Пекіні пояснюють спробами «стримати Китай і в рамках своїх невинних 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»²⁸⁴.

Усі американські звинувачення Китаю в сприянні кіберзлочинності та в кібершпигунстві негайно засуджуються китайськими дипломатами, а також певними експертами, які натомість стверджують, що Китай завжди був довгостроковою жертвою кібератак США. У такому самому дусі Китай заперечує звинувачення на свою адресу й із боку НАТО, Європейського Союзу, Австралії, Великої Британії, Канади, Японії, Нової Зеландії, закликаючи США та

²⁸² Цит. за: Wolfe Derek. How China Became a Digital Adversary and Threat to the U.S. *GSIXchange*. July 21.2021. URL: <https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/>

²⁸³ Qingqing Chen, Siqu Cao. US turns cyberspace into another anti-China battlefield, 'futile to contain Beijing'. *Global Times*. Jul 20. 2021. URL: <https://www.globaltimes.cn/page/202107/1229168.shtml>

²⁸⁴ Там само.

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, чий дослідження, зазвичай, використовують для розуміння цифрової безпеки Китаю, повідомив, що атаку з боку Центрального розвідувального управління 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»²⁸⁵.

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 із метою наклепу й стримування Китаю» й що така позиція США може призвести до погіршення китайсько-американських відносин, які можуть перейти до нового мінімуму²⁸⁶. Китайська влада заявляє про те, що протягом багатьох років Китай був основною жертвою кібератак. Згідно зі щорічним звітом Національної технічної групи з

²⁸⁵ Satter Raphael. Chinese cybersecurity company accuses CIA of 11-year-long hacking campaign. *Reuters*. March 3. 2020. URL: <https://www.reuters.com/article/us-china-usa-cia-idUSKBN20Q2SI>

²⁸⁶ 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>

реагування на надзвичайні ситуації / координаційного центру Китаю (CNCERT/CC), у 2020 р. близько 5,31 млн хостів на материковій частині Китаю контролювали загалом близько 52 000 закордонних серверів керування шкідливими програмами, а трійко найбільших джерел закордонних серверів за кількістю скомпрометованих китайських хостів – усі з країн – членів НАТО²⁸⁷.

Відома антивірусна компанія *Antiy Labs* опублікувала документ, у якому стверджується, що з 2000 р. США вже проводили масштабні атаки на глобальному рівні, – *Equation*, підрозділ Агентства національної безпеки (АНБ), зламав 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 атак²⁸⁸. За даними китайської компанії, США проникають в інформаційні системи й атакують китайського телекомунікаційного гіганта *Huawei*, а також країни, якщо вони купують продукцію *Huawei*. Також стверджується, що США застосовують масову хакерську діяльність для того, щоб атакувати низку держав, включаючи 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, АРТ-С-39 належить ЦРУ, а злам, простежений із 2008 р., переважно спрямований на організації в Пекіні, провінціях Гуандун і Чжецзян²⁸⁹.

²⁸⁷ 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>

²⁸⁸ 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/>

²⁸⁹ 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

У Китаї пояснюють загострення конкуренції зі США у сфері кібербезпеки тим, що Америка намагається зберегти свою гегемонію у світі. Особливо це питання загострилось із приходом адміністрації Байдена, коли з боку Китаю розпочалася масштабна та системна інформаційна кампанія, у якій кібердіяльність і звинувачення Китаю як джерела кіберзагроз розглядаються як елемент 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 новий світовий порядок ще далекий від установаження, оскільки глобальна система переходить від одно- до багатополлярної»²⁹⁰.

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 та авторитарний Китай» як «єдиного конкурента, потенційно здатного поєднати свою економічну, дипломатичну, військову й технологічну силу, щоб кинути постійний виклик стабільній і відкритій міжнародній системі»²⁹¹. Як зазначають китайські спостерігачі, незважаючи на деякі можливості для співпраці, політика Байдена в Китаї схиляється до «стратегічної конкуренції й навіть конфронтації»²⁹².

²⁹⁰ Chen Qingqing, Xu Keyue and Xu Yelu. US Turning G7 Into Anti-China, Anti-Russia Chorus 'Wishful Thinking. *Global Times*. June 6. 2021. URL: <https://www.globaltimes.cn/page/202106/1225524.shtml>

²⁹¹ 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>

²⁹² Liu Guozhu. 拜登政府国家安全战略的基本方针与发展方向. (Bàidēng 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->

У Китаї вважають, що, на відміну від односторонньої позиції Трампа з відвертими нападами на Компартію Китаю, Байден обрав альтернативні інструменти багатосторонності й узаємодії із 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»²⁹³. Причому така позиція щодо більш жорсткої стратегії в бік Китаю підтримується обома американськими партіями, що засвідчено в Акті Сенату США про стратегічну конкуренцію (2021 р.)²⁹⁴. У базі 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 та більшої частини решти світу», і що така китайська політика «поставить під загрозу майбутній мир, процвітання й свободу міжнародного співтовариства в найближчі десятиліття»²⁹⁵.

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:

mexZ_mX1EJ:<https://dysw.cnki.net/kcms/detail/detail.aspx%3Ffilename%3DJSSDD202105008%26dbcode%3DCJFD%26dbname%3DCJFD2021%26v%3D+&cd=1&hl=uk&ct=clnk&gl=ua>

²⁹³ 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/>

²⁹⁴ 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>

²⁹⁵ Там само, с. 5.

«Байден знайомий із 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»²⁹⁶. Цінь Ань, керівник Пекінського Інституту кіберпросторової стратегії, зазначив, що США застосовують 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»²⁹⁷.

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, що 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»²⁹⁸.

Кібернетичні загрози зростають випереджаючими темпами в порівнянні з усіма іншими проблемами, пов'язаними з розвитком кіберпростору. Сьогодні світовими лідерами в кіберсфері й секторі інформаційної (кібер) безпеки є США та Китай. Сторони звинувачують одна одну в кібератаках з економічною метою, у кібершпигунстві, а протягом останніх років – і в політично мотивованих діях

²⁹⁶ Qingqing Chen, Siqu Cao. US turns cyberspace into another anti-China battlefield, 'futile to contain Beijing'. *Global Times*. Jul. 20. 2021. URL: <https://www.globaltimes.cn/page/202107/1229168.shtml>

²⁹⁷ US turns cyberspace into another anti-China battlefield, 'futile to contain Beijing'. *National Cyber Security News Today*. July 28. 2021. URL: <https://nationalcybersecuritynews.today/us-turns-cyberspace-into-another-anti-china-battlefield-futile-to-contain-beijing-cybersecurity-cyberattack/>

²⁹⁸ 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>

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 та економічних ресурсів у кіберсфері.

Взаємодія ЄС і США у сфері кібербезпеки

80. Яка концептуальна позиція Європейського Союзу щодо політики у сфері безпеки кіберпростору?

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 – центральний елемент кібербезпеки. Головною ознакою спільного для них західного підходу в питанні безпеки кіберпростору є дотримання принципу свободи обміну інформацією в мережі та демократичної концепції організації самого кіберпростору²⁹⁹.

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 сектору, коли держава забезпечує лише гарантії безпеки функціонування інформаційних систем та інформаційно-телекомунікаційної інфраструктури й боротьбу з кіберзлочинністю. Також держава забезпечує ефективну оборону та, 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 та свобод, а також, що не повинно

²⁹⁹ Taylor Emily, Hoffmann Stacie. *EU–US Relations on Internet Governance*. Chatham House. 2019. URL: <https://www.chathamhouse.org/publication/eu-us-relations-internet-governance>. [Google Scholar]

бути прямого й жорсткого урядового контролю в управлінні мережею, як це пропонують Росія та Китай, – управління інтернетом має регулюватися шляхом поєднання участі держави, промисловості й приватного сектору. Власне саме ці принципи, – забезпечення прав і свобод людини й невторчання в управління інтернетом, – розділяють демократичні ЄС та США, з одного боку, й авторитарні Росію та Китай – із 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 та 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 усе повніше реалізується в Росії, Китаї, Ірані.

81. Як узгоджуються зусилля ЄС і США у сфері міжнародної взаємодії щодо боротьби з кіберзлочинністю?

Одним із перших спільних інтересів ЄС та 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 кіберзлочинності³⁰⁰. Групу створено для розробки спільних підходів до широкого кола питань кібербезпеки й кіберзлочинності та, 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»³⁰¹.

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

Також нагадаємо, що Росія, продовжуючи тривалу боротьбу за свою модель міжнародної координації у сфері боротьби з кіберзлочинністю, запропонувала прийняття нового глобального правового акту стосовно кіберзлочинності на рівні ООН (одним з аргументів проти Будапештської конвенції її противники вважають недостатньо високий міжнародний рівень, апелюючи до необхідності прийняття відповідного акта на рівні ООН). Під час Генеральної Асамблеї у 2019 р. прийнято відповідну резолюцію про кіберзлочинність і про створення комітету експертів для розгляду нової угоди ООН про кіберзлочинність для підготовки протягом декількох

³⁰⁰ 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

³⁰¹ 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

років проєкту такого документа³⁰². Ця резолюція актуалізує давню мету Росії – замінити Будапештську конвенцію Ради Європи, яка є єдиним міжнародним документом, що вирішує питання міжнародної взаємодії у сфері кіберзлочинності. Росія, яка раніше запропонувала альтернативний проєкт конвенції ООН³⁰³, послідовно стверджує, що Будапештська конвенція є застарілою регіональною угодою й порушує принципи державного суверенітету та невтручання.

Опозицію російській ініціативі становили 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»³⁰⁴. Так, виступаючи від Європейського Союзу, представник Фінляндії також підкреслив, що наявна міжурядова експертна група ООН із кіберзлочинності вже вирішує питання про те, чи потрібен новий договір³⁰⁵. 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 (від 27 грудня 2019 р.), якою 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 перший проєкт Конвенції, головними цілями якої є³⁰⁶ вжиття кожною державою-учасницею

³⁰² 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>

³⁰³ 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 Ireland. URL: <https://www.rusemb.org.uk/fnapr/6394>

³⁰⁴ Цит. за: Lederer Edith M. UN gives green light to draft treaty to combat cybercrime. *AP*. December 28, 2019. URL: <https://apnews.com/article/79c7986478e5f455f2b281b5c9ed2d15>

³⁰⁵ Там само.

³⁰⁶ Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях. Проект. URL:

заходів для визнання злочину відповідно до національного законодавства про кіберзлочинність; визначення нових процедур правового співробітництва у сфері кіберзлочинності; утворення 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»³⁰⁷. (Основною причиною неприєднання Росії до Конвенції про боротьбу з кіберзлочинами 2001 р. було те, що Будапештська конвенція дозволяє транскордонні кібероперації). 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)³⁰⁸.

Цю ініціативу в ООН позитивно сприйняли коаліція країн, що розвиваються (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 у рамках ООН»³⁰⁹). Натомість позицію з цього приводу держав Заходу ще в листопаді 2019 р. чітко сформульовано зі сторони Сполучених Штатів: «Сполучені Штати розчаровані рішенням авторів цієї резолюції винести її

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf

³⁰⁷ Там само.

³⁰⁸ Там само.

³⁰⁹ 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

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»³¹⁰.

Європейський Союз чітко не заявив про підтримку чи протидію зазначеній 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 у 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»³¹¹). 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 усеосяжної 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 Асамблеї (вересень 2021 – вересень 2022)³¹².

³¹⁰ 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/>

³¹¹ 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>

³¹² 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>

Проте, на думку 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 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.

США також активно працюють щодо утвердження Будапештської конвенції, вважаючи розширення міжнародної співпраці в цьому напрямі безальтернативним. Із цього приводу держсекретар США Керрі так висловився в Корейському університеті (Сеул) 18 травня 2015 р.: «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 кожену країну розглянути можливість приєднання. Не існує кращої правової бази для транскордонної роботи, щоб визначити, що таке кіберзлочинність і як потрібно запобігти порушенням закону й притягнути до кримінальної відповідальності»³¹³.

Імовірним шляхом виходу із ситуації, що склалась у зв'язку з 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 в її преамбулу певного

³¹³ Cybercrime% Goals and Priorities. US Dept. of State. URL: <https://2009-2017.state.gov/documents/organization/255007.pdf>

захисного застереження, яке б гарантувало не заперечення, а доповнення цим документом уже наявних міжнародних інструментів співробітництва, уключаючи Будапештську конвенцію³¹⁴.

США підтримують Будапештську конвенцію, у 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, та підтримці збільшення участі країн, що розвиваються, у засіданнях конференції сторін³¹⁵. Також лише у 2018 р. в рамках проєкту *Cybercrime@Octopus* на цю мету виділено 500 тис. дол.³¹⁶

82. Які інституції функціонують у сфері співпраці ЄС і США щодо протидії кіберзагрозам?

У площині практичної співпраці в рамках Робочої групи ЄС і США з питань кібербезпеки й кіберзлочинності стали³¹⁷ розширення можливостей реагування на інциденти спільно й в усьому світі за допомогою програм співпраці, спільних навчань між ЄС і США для протидії кіберінцидентам; широке зобов'язання залучати приватний сектор, обмінюватися передовим досвідом співпраці з промисловістю та здійснювати конкретне залучення до таких ключових проблем, як боротьба з ботнетами, забезпечення систем промислового контролю (наприклад очищення води й виробництво електроенергії), а також підвищення

³¹⁴ Giovannelli D. 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*. 2021. URL: <https://ccdcoe.org/incyber-articles/proposal-of-united-nations-convention-on-counteracting-the-use-of-information-and-communications-technologies-for-criminal-purposes-comment-on-the-first-draft-text-of-the-convention/>

³¹⁵ 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/>

³¹⁶ 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>

³¹⁷ 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

стійкості та стабільність інтернету; реалізація програми негайних спільних заходів із підвищення обізнаності, обміну повідомленнями, а також дорожня карта синхронних щорічних зусиль щодо інформування й конференція з питань захисту дітей в інтернеті; продовження співпраці ЄС і США щодо видалення дитячої порнографії з інтернету, у тому числі через роботу з реєстраторами доменних імен і реєстрами.

У рамках останніх пунктів співпраці як реалізація одного з основоположних принципів західного підходу до кібербезпеки розглядається співпраця держав у розслідуванні та боротьбі з кіберзлочинністю. Сторони започаткували у 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 у 2016 р. із заснованим у 2013 р. американсько-британським альянсом *WePROTECT* цей спільний проєкт став одним із найбільших у сфері координації зусиль щодо кібербезпеки й сьогодні об'єднує 98 країн, десятки компаній, громадських і міжнародних організацій³¹⁸.

Здійснюється координація між ЄС та США і в практичних напрямках координації мережі, зокрема між спеціалізованими інституціями. Обидві сторони поділяють спільні принципи й візії щодо управління інтернетом, такі як відкритість, свобода та сумісність, а також гарантії прав і свобод людини у сфері кібербезпеки. США та 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 їхній 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

³¹⁸ The Alliance. URL: <https://www.weprotect.org/alliance/>

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 та США – це не вибір, а необхідність. Створення Робочої групи ЄС–США з кібербезпеки й кіберзлочинності у листопаді 2010 р. стало нашим першим кроком для визначення стратегічних цілей і конкретних дій»³¹⁹. У цій же промові єврокомісар відзначила високий рівень професіоналізму фахівців із кібербезпеки Федерального бюро розслідувань США, що «підкріпило думку, що ми повинні продовжувати поглиблювати трансатлантичну співпрацю проти кіберзагроз»³²⁰.

Відомо багато прикладів успішної співпраці з багатьма зацікавленими сторонами між ЄС і США, уключаючи перехідний орган Організації з адміністрування доменних імен верхнього рівня (IANA) та Європейського діалогу з питань управління інтернетом (EuroDIG)³²¹. У цьому напрямі Робоча група ЄС–США з кібербезпеки й кіберзлочинності також доклала зусиль для координації між ЄС та США, зокрема в питанні укладення рекомендацій для правоохоронних органів щодо неправомірного використання доменних імен та IP-адрес в інтернеті в незаконних цілях³²².

За словами згаданої вище Сесілії Мальмстрьом, близько 50 % даних, наданих претендентами на п'ять найкращих загальних доменів верхнього рівня

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 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

³²⁰ Там само.

³²¹ Taylor Emily and Hoffmann Stacie. 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>

³²² 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>

– .com (dot com), .org, .net, .info та .biz, – містять докази фальшивої, неправдивої чи неповної інформації, що засвідчує особу. І ця проблема розв’язана саме спільними зусиллями: «Після значного тиску з боку ЄС та США ми нарешті побачили зобов’язання інтернет-корпорації з присвоєння імен і номерів (ICANN) та приватного сектору впроваджувати конкретні рекомендації правоохоронних органів у своїй політиці»³²³.

Значним результатом розвитку євроатлантичної співпраці у сфері кібербезпеки став Кібердіалог між ЄС і США, який розпочав роботу в грудні 2014 р. У порівнянні з Робочою групою ЄС–США з кібербезпеки й кіберзлочинності його мета, окрім утилітарних аспектів протидії кіберзагрозам, більше орієнтована також на координацію зовнішньої політики сторін із кіберпитань 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 захист прав людини в інтернеті, нарощування потенціалу кібербезпеки в третіх країнах. Безпекові питання в полі інтересів кібердіалогу поширюються на встановлення норм поведінки й заходів щодо зміцнення довіри в кіберпросторі й застосування наявних норм міжнародного права в кіберпросторі³²⁴.

Зокрема, у напрямі розвитку кіберстійкості сторони розробили Директиву ЄС 2016/1148 про безпеку мережевих та інформаційних систем, ухвалену у 2016 р.³²⁵, яка впроваджується в усіх державах-членах, а також організували проведення

³²³ Там само.

³²⁴ 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>

³²⁵ 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

навчань *CyberEurope*. Вони також обговорили другу ітерацію Стандартів рамок кібербезпеки на добровільній основі, уключаючи постійне залучення зацікавлених сторін. За їх участі підготовлено Національний план реагування на кіберінциденти США³²⁶.

Важливою характеристичною ознакою американсько-європейського підходу до безпеки кіберпростору є активне залучення до управління ним приватного сектору, 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 розв'язання ключових проблем кіберполітики та збільшення потенціалу досліджень у сфері кіберпитань. На практиці Робоча група ЄС–США з кібербезпеки й кіберзлочинності та кібердіалог ЄС–США стали двома ключовими інституціями для обговорення політики й потенційної координації дій у сфері кібербезпеки.

83. Як відбуваються практична взаємодія ЄС і США й запозичення досвіду у сфері протидії кіберзагрозам?

Узаємодія ЄС і США в аспекті обговорення політики й потенційної координації дій у сфері кібербезпеки відбувається відповідно до принципу багатосторонньої координації, за допомогою добровільного прийняття та наслідування практики один одного. Наприклад, Агентство ЄС з інформаційної безпеки й безпеки мереж (ENISA) для відображення взаємозалежностей операторів основних послуг і постачальників цифрових послуг урахує найбільш актуальні й поширені стандарти у сфері управління ризиками, у тому числі міжнародний ISO/IEC 27002 та американську рамку *NIST Cybersecurity Framework*. Ця рамка оцінки ризиків й аудиту охоплює різні сфери ризиків і

³²⁶ 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>

надає конкретні вказівки для планування й реалізації детальної стратегії на основі ризиків в організаціях³²⁷.

Також у ЄС підтримано реалізовану значно раніше в США модель центрів аналізу й обміну інформацією (ISAC) – некомерційних організацій, які надають ресурси для збору інформації про кіберзагрози (у багатьох випадках для критичної інфраструктури), а також здійснюють двосторонній обмін інформацією між приватним і державним секторами про кіберінциденти й загрози, обмінюються досвідом, знаннями та результатами аналізу. Європейські законодавчі акти, такі як Директива NIS і Закон про кібербезпеку, підтримують розвиток публічно-приватного партнерства й утворення галузевих ISAC у межах ЄС. У США галузеві центри обміну та аналізу інформації співпрацюють між собою через Національну раду ISAC (NCI), створену ще у 2003 р., яка сьогодні об'єднує 25 організацій³²⁸.

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, котрі зазвичай відкрито публікують та просувають свої підходи й стандарти, а також за допомогою взаємодії європейських чиновників і представників американських компаній, що 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 в 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

³²⁷ 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>

³²⁸ National Council of ISACs. URL: <https://www.nationalisacs.org/>

скоординованій дії під керівництвом ФБР, яка забезпечила зрив ботнета *GameOver Zeus*, у реалізації якого влада США підозрює мешканця Росії³²⁹. 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 сектору демонтували сімейство шкідливих програм під назвою *Andromeda*. Статистичні дані, отримані під час розслідування в цій справі правоохоронними органами Німеччини, були передані через Європол до ФБР³³⁰. Улітку 2021 р. правоохоронні й судові органи з Європи, США й Канади, зокрема Національна поліція Нідерландів у координації з Європолем і Євроюстом, нейтралізували вебдомени 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 здійснена в рамках Європейської багатопрофільної платформи проти кримінальних загроз (EMPACT)³³¹. Загалом на вебсайті Європолу повідомляється про десятки подібних прикладів успішної, спільної з американською стороною боротьби з кіберзлочинністю, а в його структурі задіяно близько тридцяти фахівців, які репрезентують різні офіційні служби США³³².

³²⁹ 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>

³³⁰ 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>

³³¹ 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>

³³² Statistics & data. Europol staff numbers. URL: <https://www.europol.europa.eu/about-europol/statistics-data>

84. Які розбіжності існують у підходах ЄС і США до політики безпеки кіберпростору?

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 тероризму³³³.

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 недійсним правовий механізм для забезпечення взаємного транскордонного потоку даних між ЄС і США, чинний із початку 2000 рр., на підставі якого діяли близько 4000 компаній, зокрема й фейсбук, які використовували його для передачі даних через Атлантику³³⁴. 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 механізм під назвою *EU-US Privacy Shield* (Щит конфіденційності між ЄС і США), який передбачав належний захист під час передання персональних даних із країн ЄС до США. Підставою такого рішення стало встановлення конфлікту між

³³³ EU Data Protection Rules and U.S. Implications. *Congressional Research Service*. July 17, 2020. URL: <https://sgp.fas.org/crs/row/IF10896.pdf>

³³⁴ Vittorio Andrea. 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>

законодавствами США та ЄС: перше дозволяє спецслужбам здійснювати збір даних на території країни, а другі, згідно з GDPR, вимагають їх захищати³³⁵.

Загалом США і ЄС дотримуються подібних підходів щодо інформаційної (кібер) безпеки. І це зумовлено не лише подібністю їхніх 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 з управлінням інтернетом і правами людини в інтернеті. У контексті конкуренції за встановлення глобальних стандартів ЄС та США протистоять зусиллям Росії й Китаю в їх намаганні контролювати й цензурувати вміст інтернету та підірвати нинішню модель управління інтернетом (уключно з іншими зацікавленими сторонами, замінюючи її на міжурядові й державно-центричні структури). Очевидно, що спільні інтереси сприятимуть розвитку співпраці США і ЄС, зміцненню й поширенню західної концепції інформаційної (кібер) безпеки.

Взаємодія ЄС з іншими країнами

85. Які проблеми безпеки кіберпростору покликана розв'язати кіберстратегія ЄС за допомогою міжнародної взаємодії?

Важливо, що, переслідуючи власні цілі, ЄС бере активну участь у поширенні концепції розвитку кіберпростору, властивої демократичним системам. Але при цьому розробляються й просуваються власні позиції з актуальних для міжнародної взаємодії питань. Це стосується, наприклад, позиції ЄС щодо кіберстимування, яка ще виробляється та, відповідно до стратегії

³³⁵ Bodoni Stephanie. 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>

кібербезпеки 2020 р., «має сприяти відповідальній 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»³³⁶. Окрім того розглядаються можливості подальших варіантів обмежувальних заходів у рамках набору інструментів у сфері кібердипломатії й режим горизонтальних санкцій проти кібератак.

У стратегії ЄС надалі зміцнить свій набір інструментів із кібернетичної дипломатії (сукупність дипломатичних практик, що стосуються широко визначеного управління кіберпростором) для забезпечення її функціонування на регулярній основі, подальшого інтегрування інструментарію кібердипломатії в кризові механізми ЄС, забезпечення синергії в зусиллях щодо протидії гібридним загрозам, дезінформації й зовнішнього втручання в рамках Спільної рамки протидії гібридним загрозам³³⁷.

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 та 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 та затвердженні таких стандартів, а також тим, що міжнародна

³³⁶ 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

³³⁷ 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>

стандартизація все частіше використовується третіми країнами для просування своєї політичної й ідеологічної програми, зокрема спираючись на розробки в таких сферах, як штучний інтелект, хмарні та квантові обчислення й квантова комунікація, що часто не відповідає цінностям ЄС. Наприклад, перспективні технологічні розробки Китаю в зазначених сферах застосовуються для обмеження свободи слова, громадянських і політичних прав³³⁸.

Стратегія кібербезпеки ЄС передбачає створення Порядку денного розбудови зовнішнього кіберпотенціалу ЄС. Відповідно до прийнятих у 2018 р. керівних напрямів³³⁹ для розробки цього Порядку денного, «створення кіберпотенціалу стає однією з найважливіших тем у порядку денному міжнародної кіберполітики». А розбудова кіберпотенціалу третіх країн за участі ЄС передбачає: «систематичні зусилля з партнерами країн і відповідних організацій для покращення національних, інституційних та 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; удосконалення навичок та компетенцій кібербезпеки; сприяння підвищенню обізнаності й ефективній співпраці з цих питань на національному, регіональному й міжнародному рівнях»³⁴⁰. Також передбачено посилення цивільних аспектів Спільної політики безпеки й оборони за допомогою включення в неї заходів із кібербезпеки з акцентом на зміцнення стійкості та 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

³³⁸ Вейкфілд Джейн. 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>

³³⁹ 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>

³⁴⁰ Там само.

пріоритетних, щодо яких буде здійснено підтримку ЄС у справі розбудови кібернетичного потенціалу, держави-сусіди й загалом країни, що розвиваються.

Важливим у стратегії міжнародної співпраці ЄС із питань безпеки кіберпростору в аспекті міжнародної співпраці 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»³⁴¹.

86. Які головні регіональні напрями міжнародної співпраці ЄС у сфері розвитку потенціалу протидії кіберзагрозам?

Для практичної реалізації своїх цілей у сфері розвитку зовнішнього кіберпотенціалу ЄС утворює мережу *EU CyberNet*³⁴², яка повинна посилити глобальну реалізацію, координацію й узгодження проєктів Європейського Союзу щодо створення кіберпотенціалу та 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.³⁴³), коли в комюніке «Стійкість, стримування, оборона: створення міцної кібербезпеки для ЄС» Європейська комісія закликала

³⁴¹ 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

³⁴² EU CyberNet – the bridge to cybersecurity expertise in the European Union. URL: <https://www.eucybernet.eu/>

³⁴³ What can we learn from the «most devastating» cyberattack in history? *CBC News*. August 22. 2018. URL: <https://www.cbcnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/>

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»³⁴⁴. Запущена у 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, допомоги й перетворення на центр знань про зовнішні відносини ЄС у сфері кібербезпеки.

Пріоритетними для ЄС у цьому аспекті є держави Західних Балкан, країни сусідства, а також держави-партнери, що демонструють швидкий цифровий розвиток. Зокрема, у 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 та стандартами ЄС у сфері кібернетичної дипломатії. Наприклад, у 2021 р. в Домініканській Республіці проведено перші національні навчання з кібербезпеки «Кіберполум'я» й проведено роботу зі створення майбутнього центру кіберкомпетентності для країн Латинської Америки та Карибського басейну³⁴⁵.

Важливого значення ЄС надає співпраці з питань безпеки кіберпростору й 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

³⁴⁴ 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>

³⁴⁵ 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/>

європейського бачення кіберпростору, обміну інформацією й координації щодо подій у кіберпросторі.

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

87. Які головні напрями співпраці держав ЄС у сфері кібербезпеки й оборони?

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 декларацію³⁴⁶, щоб надати нового імпульсу й нової сутності стратегічному партнерству ЄС–НАТО, зокрема й у сферах протидії гібридним загрозам, кібербезпеки та оборони. На основі мандату Спільної декларації Європейський Союз і НАТО створили спільний набір пропозицій щодо її імплементації, який схвалено Радами ЄС та НАТО в грудні 2016 р.

У сфері кібербезпеки й оборони оголошено про розширення координації, уключаючи контекст місій та операцій, навчань й освіти, а також щодо сумісності у 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 загроз

³⁴⁶ 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>

за допомогою своєчасного обміну інформацією, співпраці у сфері стратегічної комунікації й реагування.

Окремо відзначимо роботу ЄС щодо розвитку напряму кібероборони в царині спільної політики безпеки та оборони (CSDP). У 2014 р. прийнято рамки політики ЄС щодо кібероборони (CDPF), оновлені у 2018 р³⁴⁷. Документ містить основи для протидії кіберзагрозам та визначає аспекти кіберзахисту в Стратегії ЄС із кібербезпеки, роз'яснює ролі різних європейських суб'єктів і визначає пріоритетні напрями кіберзахисту CSDP, зокрема сприяння цивільно-військовому узгодженню з кіберполітикою ЄС, установами ЄС та 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. відзначено необхідність перегляду Рамкової політики у сфері кібероборони (CDPF) для того, щоб «кібербезпека й кіберзахист ще більше інтегрувалися в ширшу програму безпеки та оборони»³⁴⁸. Важливим стратегічним напрямом є покращення співпраці між державами-членами щодо виявлення й реагування на кіберінциденти, 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, у рамках Глобальної стратегії ЄС із зовнішньої політики й політики безпеки. Серед перших сімнадцяти ключових напрямів співпраці,

³⁴⁷ 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>

³⁴⁸ 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

внесених до Декларації про проєкти в рамках PESCO, є створення бази обміну інформацією у відповідь на кібернетичні атаки та загрози й надання взаємодопомоги для забезпечення кібернетичної безпеки та створення кібергрупи швидкого реагування ³⁴⁹. 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).

³⁴⁹ 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 із них характерний для США, їхніх партнерів по НАТО й інших провідних держав Заходу, зокрема ЄС. Інший відстоюють Росія, Китай і низка інших країн із відносно менш розвинутою демократією. Послідовники цих підходів по-різному трактують поняття «інформаційна безпека». Якщо США виступають винятково за технічне регулювання кіберсередовища (захист комп'ютерних мереж і ресурсів) та 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 ґрунтується 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 лише 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 в порівнянні зі сприйняттям кібертероризму в демократичних країнах. Якщо на Заході кібертероризм трактують як загрозу інформаційним системам, що пов'язані передусім із критичною інфраструктурою, то в Росії кібертероризм розглядають серед комплексних загроз особі, суспільству й державі. Такого підходу дотримується також китайська влада.

Суттєво відрізняються підходи до розуміння інформаційних впливів стосовно воєнно-політичної стратегії. Російська концепція полягає в застосуванні інтегрального впливу всієї державної «машини», уключаючи силові структури й

підконтрольний медіасектор (концепція «інформаційних війн»). Натомість американський і загалом євроатлантичний підхід полягає в розділенні військових та цивільних інформаційних впливів (де цивільні як такі, по суті, і 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 зламі ХХ–ХХІ ст. використовувалося поняття «інформаційного протиборства» з виокремленням «інформаційних операцій наступального й оборонного характеру». Проте із середини 2000-х рр. його місце посіла 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 переважно з відчутним відставанням перших в інформаційно-технологічному плані. По-друге, у сфері міжнародного гуманітарного права (*jus in bello*) Росія, Китай, їхні союзники по ШОС і низка інших держав (що здебільшого не характеризуються високим рівнем демократії) виступають за формування в міжнародному праві окремого домену «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 чинних норм міжнародного права, спільного реагування на виникаючі кіберзагрози й добровільних і необов'язкових норм поведінки держав у кіберпросторі. Натомість у випадку військових конфліктів, нападів у всіх передбачених нормами

міжнародного гуманітарного права випадках цілком можуть застосовуватися чинні 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», із 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. У ґрунті російських пропозицій – лідируюча та керівна роль держави в усіх аспектах і процесах інформатизації й телекомунікацій, у тому числі управлінні інтернетом та «інформаційному суверенітеті». 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 («Уженські 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 та багатостороннього управління інтернетом, неонов'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 у 2010, 2013 і 2015 рр., а також 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 впровадження правил кіберуправління всередині країни й міжнародну співпрацю в цій сфері, але Китай зі своєю ідеєю «кіберсуверенітету» відстоює право кожної держави на участь в управлінні інтернетом й оголошує протидію американській «кібергегемонії». Ця концепція відкидається Сполученими Штатами, які розглядають китайський підхід як такий, що не відповідає демократичним принципам свободи слова та права на інформацію. Із погляду США, китайська модель інформаційної (кібер) безпеки орієнтована на встановлення цензури 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 брали активну участь у 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 у 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., став проявляти значну активність у цій сфері, прийнявши відповідну стратегію та ініціювавши принципово новий формат узаємодії зацікавлених сторін на рівні ООН – ініціативу щодо реалізації Програми дій із відповідальної поведінки держав у кіберпросторі.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

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 zìlǚ guǎnlǐ chéngnuò shū». 2014 Nián 11 yuè 06 rì 22:36 Xīnhuá wǎng) [29 вебсайтів підписали «Зобов'язання щодо самодисциплінованого менеджменту публікації коментарів». Сінхуа 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%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. A/RES/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. A/RES/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. A/RES/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. A/RES/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/RES/76/19. Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies. Resolution adopted by the General Assembly on 6 December 2021. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/377/48/PDF/N2137748.pdf?OpenElement>
 11. 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>
 12. 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>
 13. 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>
 14. 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>
15. Aruna Viswanatha, Del Quentin Wilber. U.S. Prosecutors Consider Charging Russian Officials in DNC Hacking Case. *The Wall Street Journal*. 2 November 2017. URL: <https://www.wsj.com/articles/prosecutors-consider-bringing-charges-in-dnc-hacking-case-1509618203>
 16. Balzacq T., Cavelti M. D. A theory of actor-network for cyber-security, *European Journal of International Security*. 2016. №. 2. P. 176–198.
 17. Basu Arindrajit, Hickok Elonnai and Chawla Aditya Singh. Unpacking Policy Moves For Sovereign Control Of Data In India. Cyberbricks. 26 March 2019. URL: <https://cyberbricks.info/unpacking-policy-moves-for-sovereign-control-of-data-in-india/>
 18. Biden Says Russia Has 'Some Responsibility' In Pipeline Ransomware Attack. Radio Free Europe. 10 May 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>
 19. Blake Andrew. Ardit Ferizi, hacker who aided Islamic State, sentenced for helping terror group with 'kill list'. *The Washington Times*. 24 September 2016. URL: <https://www.washingtontimes.com/news/2016/sep/24/ardit-ferizi-hacker-who-aided-islamic-state-senten/>
 20. Bodoni Stephanie. 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>
 21. Bowman Andrew S. (). Russian Armed Forces: Military Doctrine and Strategy (PDF). *Congressional Research Service*. 20 August 2020. No. IF11625. URL: <https://sgp.fas.org/crs/row/IF11625.pdf>

22. 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
23. 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>
24. Broad William J., Markoff John, Sanger David E. 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
25. Brown G., Yung C. D. Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace. The Diplomat. 2017. URL:
<https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/>
26. Brown G., Yung C. D. 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. 2017. URL:
<https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-3/>
27. 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/>
28. Cadell Cate. China launches hotline for netizens to report 'illegal' history comments. Reuters. 4 November 2021. URL:
<https://www.reuters.com/world/china/china-launches-hotline-netizens-report-illegal-history-comments-2021-04-11/>

29. Centre of Excellence Defence Against Terrorism, ed. 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, 2008. P. 119.
30. Charlie Savage. Assange, Avowed Foe of Clinton, Timed Email Release for Democratic Convention. *New York Times*. July 26, 2016. URL: https://www.nytimes.com/2016/07/27/us/politics/assange-timed-wikileaks-release-of-democratic-emails-to-harm-hillary-clinton.html?_r=0
31. Chen Abby. A Close Reading of China's Data Security Law, in Effect Sept. 1, 2021. *China Briefing*. 14 July 2021. URL: <https://www.china-briefing.com/news/a-close-reading-of-chinas-data-security-law-in-effect-sept-1-2021/>
32. 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>
33. China Delivers Midnight Internet Declaration – Offline (21 November 2014). *The Wall Street Journal*. Nov. URL: <https://www.wsj.com/articles/BL-CJB-24963>
34. China Security GB Standarts List. URL: http://www.gbstandards.org/index/Standards_Search.asp?word=security
35. 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>
36. 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>
37. China's government is keeping its security researchers from attending conferences. *Cyberscoop*. 8 March 2018. URL: <https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/>

38. 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/>
39. Chipman Koty Alexander. Personal Data Regulation in China: Personal Information Protection Law, Other Rules Amended. *China Briefing*. 13 May 2021. URL: <https://www.china-briefing.com/news/personal-data-regulation-in-china-personal-information-protection-law-other-rules-amended/>
40. 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>
41. 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>
42. 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>
43. 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
44. 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.
45. 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/CptICk6BZ29/content/id/191666
 46. 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>
 47. 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/>
 48. Cyber Policy and the 19th Party Congress. CSIS. October 26. 2017. URL:
<https://www.csis.org/analysis/cyber-policy-and-19th-party-congress>
 49. 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
 50. Cyber Threat Intelligence on Advanced Attack Groups and Technology Vulnerabilities. *Threat Intelligence Reports*. Fireeyes, 2013.
 51. Cyber Warfare and Cyber Terrorism / Edited by Lech J. Janczewski and Andrew M. Colarik. Hershey, PA. *Information Science Reference*. 2008.
 52. Cyberbricks. About us. URL: <https://cyberbrics.info/about-us/>
 53. Cybercrime: Goals and Priorities. US Dept. of State. URL: <https://2009-2017.state.gov/documents/organization/255007.pdf>
 54. 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>
55. Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure. URL: <https://fas.org/irp/eprint/cyber-review.pdf>
 56. Cyberwar. Britannica. URL: <https://www.britannica.com/topic/cyberwar>
 57. 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>.
 58. DEEP: Cybersecurity – A Generic Reference curriculum. NATO. URL: https://www.nato.int/cps/en/natohq/topics_157591.htm
 59. Dickinson Steve (30 September 2019). China’s New Cybersecurity Program: NO Place to Hide. Harris/Bricken. URL: <https://harrisbricken.com/chinalawblog/chinas-new-cybersecurity-program-no-place-to-hide/>
 60. 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>
 61. 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
 62. 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 Ireland. URL: <https://www.rusemb.org.uk/fnapr/6394>

63. 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/>
64. 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>
65. 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>
66. 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
67. EU CyberNet – the bridge to cybersecurity expertise in the European Union. URL: <https://www.eucybernet.eu/>
68. 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/>
69. EU Data Protection Rules and U.S. Implications. Congressional Research Service. July 17. 2020. URL: <https://sgp.fas.org/crs/row/IF10896.pdf>
70. 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>
71. 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>
72. 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>
73. 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
74. 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>
75. 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
76. 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>
77. 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>
78. 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/>
79. 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/>

80. Farrell H. *Promoting Norms for Cyberspace*. New York: Council on Foreign Relations, 2015.
81. 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>
82. Finkle Jim. Hundreds more cyber attacks linked to 2009 Google breach. *Reuters*. 12 September 2012. URL: <https://www.reuters.com/article/cybersecurity-espionage-idUSL2E8K7A9E20120907>
83. 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.
84. 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>
85. 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
86. 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/>
87. 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/incyber-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/
88. 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>
 89. Global Freedom Status. Freedom House. URL: <https://freedomhouse.org/explore-the-map?type=fiw&year=2021>.
 90. 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+Good+practices+on+interdependencies+between+OES+and+DSPs.pdf>
 91. Greenberg L. T., Goodman S. E., Soo Hoo K. J. *Information Warfare and International Law*. Washington: National Defense University Press, 1997.
 92. Greenberg, A. China tests the limits of its U.S. hacking truce. *Wired*. 13 October 2017. URL: <https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/#>
 93. Griffiths James. Chinese President Xi Jinping: Hands off our Internet. *CNN*. 12 December 2015. URL: <https://edition.cnn.com/2015/12/15/asia/wuzhen-china-internet-xi-jinping>
 94. 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>
 95. Haass Richard. Present at the Disruption. How Trump Unmade U.S. Foreign Policy. *Foreign Affairs*. 2020. September/October. URL: <https://www.foreignaffairs.com/articles/united-states/2020-08-11/present-disruption>

96. Hansen L., Nissenbaum H. Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*. 2009. 4. P. 1155–1175.
97. Hao Yeli. A Three-Perspective Theory of Cyber Sovereignty. Belfercenter, 2017. URL: <https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model>
98. Hofmann J. 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>
99. Holland Steve, Shalal Andrea. Biden presses Putin to act on ransomware attacks, hints at retaliation. *Reuters*. 10 July 2021. URL: <https://www.reuters.com/technology/biden-pressed-putin-call-act-ransomware-attacks-white-house-2021-07-09/>
100. How is the Term “Armed Conflict” Defined in International Humanitarian Law? *Opinion paper. ICRC*. March 2008. URL: <http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf>
101. HPCR Manual on International Law Applicable to Air and Missile Warfare. HPCR, 2009. URL: <https://reliefweb.int/sites/reliefweb.int/files/resources/8B2E79FC145BFB3D492576E00021ED34-HPCR-may2009.pdf>
102. Hu Henry L. The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration. *The China Quarterly*. 2011. 207 (207). P. 523–540.
103. 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>
104. 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
105. Internet Governance: A Grand Collaboration (ed. by D. MacLean) (2005). New York: UN ICT Task Force Series, 393 p.
 106. ISACA. Glossary of terms. 2008. ISACA. URL: <http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf>
 107. ITU estimates that at the end of 2019, a bit more than 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>
 108. Japan Cybersecurity Strategy. Information Security Policy Council. 2013. URL: <http://www.nisc.go.jp/active/kihon/pdf/cybersecuritystrategy-en.pdf>
 109. 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 14 final/2. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2021:14:REV1&rid=1>
 110. 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. 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164
 111. Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats. European Commission. Brussels, 6.4.2016 JOIN. 18 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN>
 112. 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. 450 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN>

113. 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>
114. Joint Publication 3–13, Information Operations. 13 February 2006. URL:
https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf
115. Joint Statement on Advancing Responsible State Behavior in Cyberspace. URL: <https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/>
116. Julian Nicholas. United States' and China's Cybersecurity Policies: Collaboration or Confrontation? *Journal of International Relations*. 24 January 2021. URL: <http://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation>
117. Kelley Michael B. 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>
118. Keohane R. Nye J. Power and interdependence in the information age. *Foreign affairs*. 1998. Vol. 77. No. 5. P. 81–94.
119. Koh Harold Hongju. International Law in Cyberspace. *Harvard International Law Journal*. 2012. 54 (December).
120. Кориіка М. 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>
121. Kosseff Jeff. *Cybersecurity Law*. 2017. Wiley.
122. Kurbalija Jovan. *An Introduction to Internet Governance*. 2014. DiploFoundation. 206 p.

123. Libicki M. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.
124. Liu Guozhu, «拜登政府国家安全战略的基本方针与发展方向, (Bàidēng zhèngfǔ guójiā ānquán zhànlüè de jīběn fāngzhēn yǔ fāzhǎn fāngxiàng) [Основна політика та напрям розвитку Стратегії національної безпеки адміністрації Байдена]. *Dangdai Shijie*. 5. 2021. Pp. 50–57. URL: https://webcache.googleusercontent.com/search?q=cache:7-mexZ_mX1EJ:https://dysw.cnki.net/kcms/detail/detail.aspx%3Ffilename%3DJSSD202105008%26dbcode%3DCJFD%26dbname%3DCJFD2021%26v%3D+&cd=1&hl=uk&ct=clnk&gl=ua
125. Lederer Edith M. UN gives green light to draft treaty to combat cybercrime. *AP*. 28 December 2019. URL: <https://apnews.com/article/79c7986478e5f455f2b281b5c9ed2d15>
126. Mandiant Consulting Services. *APT1: Exposing One of China's Cyber Espionage Units*. Fireeye. 2013. URL: <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>
127. 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>
128. 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>
129. Molander Roger C., Riddile Andrew, Wilson Peter A. *Strategic Information Warfare. A New Face of War*. RAND. 1996. MR-661-OSD. URL: https://www.rand.org/pubs/monograph_reports/MR661.html

130. Molander Roger C., Wilson Peter A., Mussington B. David, Mesic Richard. Strategic Information Warfare Rising. *RAND*. 1996. MR-964-OSD. URL: https://www.rand.org/pubs/monograph_reports/MR964.html
131. Morgan Steve. 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>
132. Nakashima Ellen, Timberg Craig. Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce. *The Washington Post*. 14 December 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
133. National Council of ISACs. URL: <https://www.nationalisacs.org/>
134. National Cyber Strategy of the United States of America. Trumpwhitehouse. URL: <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
135. 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
136. NATO, Information Warfare and International Security. NATO Parliamentary Assembly Science and Technology Committee, Brussels. 6th October. 1999.
137. Neumann Scott. Intelligence Chiefs Say China, Russia Are Biggest Threats To U.S. NPR. 14 April 2021. URL: <https://www.npr.org/2021/04/14/987132385/intelligence-chiefs-say-china-russia-are-biggest-threats-to-u-s>

138. 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
139. New PRC Internet Regulation. A January 1998 report from U.S. Embassy Beijing. URL: <https://fas.org/irp/world/china/netreg.htm>
140. Newman, Lily Hay. 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/>
141. NRC Working Group on Defence Reform and Cooperation Special Operations Forces Glossary Russian-English. 2006. NRC WGDRS SOF GLOSSARY (E-R) 08.12.06. URL: [https://www.nato.int/docu/other/ru/2006/pdf/SOFglossary\(R-E\).pdf](https://www.nato.int/docu/other/ru/2006/pdf/SOFglossary(R-E).pdf)
142. Obama and Xi Jinping of China Agree to Steps on Cybertheft. *The New York Times*. 25 September 2015. URL: <https://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html>
143. 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>
144. Oyedele Akin. BUFFETT: This is 'the number one problem with mankind'. *INSIDER*. 6 May 2017. URL: <https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5>
145. Perlroth Nicole. How China Transformed Into a Prime Cyber Threat to the U.S. *The New York Times*. 19 July 2021. URL: <https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html>
146. Pillars of The International Strategy for Cyberspace. U.S. Department of State. URL: <https://2009-2017.state.gov/s/cyberissues/strategy/index.htm>
147. 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
148. Qiang, Xiao. Congressional-Executive Commission on China (CECC) Hearing: Urging China's President Xi Jinping to Stop State-Sponsored Human Rights Abuses. *CECC*. 18 September 2015. URL: <https://www.cecc.gov/sites/chinacommission.house.gov/files/CECC%20Hearing%20-%20Human%20Rights%20Abuses%20-%2018Sept15%20-%20Xiao%20Qiang.pdf>
 149. Qingqing Chen, Siqi Cao. US turns cyberspace into another anti-China battlefield, 'futile to contain Beijing'. *Global Times*. 20 July 2021. URL: <https://www.globaltimes.cn/page/202107/1229168.shtml>
 150. 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>
 151. 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/>
 152. 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>
 153. 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>
154. 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>
155. Robertson Jordan, Riley Michael. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg Businessweek*. 4 October 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>
156. Ross Alec. Want job security? Try online security. *Wired*. 25 April 2016. URL: <https://www.wired.co.uk/article/job-security-cybersecurity-alec-ross>
157. Ruys Tom, Corten Olivier, Hofer Alexandra. *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>
158. Ryjov Alexander P., Mikhalevich Igor F. Hybrid Intelligence Framework for Improvement of Information Security of Critical Infrastructures. In *Handbook of Research on Cyber Crime and Information Privacy*. *IGI Global*. 2020. P. 310–337.
159. Satter Raphael. Chinese cybersecurity company accuses CIA of 11-year-long hacking campaign. *Reuters*. 3 March 2020. URL: <https://www.reuters.com/article/us-china-usa-cia-idUSKBN20Q2SI>
160. Schaffer Aaron (). The Cybersecurity 202: The United States is still number one in cyber capabilities. *The Washington Post*. 28 June 2021. URL: <https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/>
161. Schmitt Michael. The Sixth United Nations GGE and International Law in Cyberspace. *Just Security*. 10 June 2021. URL:

- <https://www.justsecurity.org/76864/the-sixth-United-nations-gge-and-international-law-in-cyberspace/>
162. Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013. URL: <http://www.cambridge.org/tallinnmanual2>
 163. *Security in Cyberspace: Targeting Nations, Infrastructures, Individuals* / Ed. by G. Giacomello. Bloomsbury Publishing USA, 2014.
 164. Shackelford Scott J. *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*. Cambridge University Press, 2014.
 165. *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
 166. Sink Justin, Parker Mario. 'America is back, Diplomacy is back' – Biden reverses Trump's foreign policy moves. *ThePrint*. 5 February 2021. URL: <https://theprint.in/world/america-is-back-diplomacy-is-back-biden-reverses-trumps-foreign-policy-moves/599152/>
 167. Soldatkin Vladimir, Holland Steve. Far apart at first summit, Biden and Putin agree to steps on cybersecurity, arms control. *Reuters*. 17 June 2021. URL: <https://www.reuters.com/world/wide-disagreements-low-expectations-biden-putin-meet-2021-06-15/>
 168. Soo Zen. How Huawei beat America's anti-China 5G propaganda war in Southeast Asia, years before it even began. *South China Morning Post*. 22 April 2019. URL: <https://www.scmp.com/tech/article/3006935/how-huawei-beat-americas-anti-china-5g-propaganda-war-southeast-asia-years-it>
 169. Soo Zen. China orders removal of 105 apps, including TripAdvisor. *Associated Press*. 9 December 2020. URL: <https://apnews.com/article/media-prostitution-china-hong-kong-pornography-84314d74600bd87d6dcea77524e43ed7>

170. 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>
171. 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>
172. 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
173. 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/>
174. Statistics & data. Europol staff numbers. URL:
<https://www.europol.europa.eu/about-europol/statistics-data>
175. Sternstein Aliya. Cyber early warning deal collapses after Russia balks. *Nextgov*. 7 December 2012. URL:
<https://www.nextgov.com/cybersecurity/2012/12/cyber-early-warning-deal-collapses-after-russia-balks/60035/>
176. Summary. DEPARTMENT OF DEFENSE CYBER STRATEGY (2018). URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
177. Szafranski R. A Theory of Information Warfare: Preparing for 2020. *Airpower Journal*. 1995. No. 1.

178. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / Ed. by M. Schmitt. New York: Cambridge University Press, 2017. 638 p.
179. Tallinn Manual on the International Law Applicable to Cyber Warfare / Ed. by M. Schmitt. New York: Cambridge University Press, 2013. 282 p.
180. 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>
181. Terrorism 2002–2005. U.S. Department of Justice. Federal Bureau of Investigation. URL: <https://www.fbi.gov/stats-services/publications/terrorism-2002-2005>
182. The Alliance. URL: <https://www.weprotect.org/alliance/>
183. 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/>
184. 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
185. The Comprehensive National Cybersecurity Initiative. URL:
<https://fas.org/irp/eprint/cnci.pdf>
186. 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

187. 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>
188. The First amendment. Legal Information Institute. URL: http://www.law.cornell.edu/anncon/html/amdt1afrag1_user.html#amdt1a_hd4
189. 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>
190. The National Strategy to Secure Cyberspace. February 2003. URL: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf
191. The Recovery and Resilience Facility. European Commission. URL: https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en
192. 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/>
193. Tiede Peter. 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>
194. Tikk-Ringas E. Evolution of the Cyber Domain: The Implications for National and Global Security. London: Routledge, for the International Institute for Strategic Studies, 2015. 212 p.
195. Triolo Paul, Sacks Samm, Graham Webster, Creemers Rogier. China's Cybersecurity Law One Year On, An Evolving and Interlocking Framework. *New America*. 30 November 2017. URL: <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/>

196. Turton Williams, Jacobs Jennifer. Russia ‘Cozy Bear’ Breached GOP as Ransomware Attack. *Bloomberg*. 7 July 2021. Hit. URL: <https://www.bloomberg.com/news/articles/2021-07-06/russian-state-hackers-breached-republican-national-committee>
197. U.S. Army Heritage and Education Center. Who first originated the term VUCA (Volatility, Uncertainty, Complexity and Ambiguity)?. *USAHEC Ask Us a Question*. 16 February 2018. The United States Army War College. URL: <https://usawc.libanswers.com/faq/84869>
198. U.S. charges four Chinese nationals charged in global hacking campaign. *Reuters*. 19 July 2021. URL: <https://www.reuters.com/technology/four-chinese-nationals-charged-global-hacking-campaign-us-justice-department-2021-07-19/>
199. UNIDIR. Report of the International Security Cyber Issues Workshop Series. 2016. URL: <https://www.unidir.org/publication/report-international-security-cyber-issues-workshop-series>
200. 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/>
201. US justice department charges Chinese with hacking. *BBC*. 14 May 2014. URL: <https://www.bbc.com/news/world-us-canada-27475324>
202. US support to the Budapest Convention. 25 September 2018. Council of Europe. URL: <https://www.coe.int/en/web/cybercrime/-/us-support-to-the-budapest-convention>
203. US turns cyberspace into another anti-China battlefield, ‘futile to contain Beijing’. National Cyber Security News Today. 28 July 2021. URL:

- <https://nationalcybersecuritynews.today/us-turns-cyberspace-into-another-anti-china-battlefield-futile-to-contain-beijing-cybersecurity-cyberattack/>
204. Ventre Daniel. *Information Warfare*. 2016. Wiley.
205. Vittorio Andrea. *Surveillance in Spotlight Amid Ongoing EU-U.S. Data Privacy Rift*. *Bloomberg Law*. 16 July 2021. URL: <https://news.bloomberglaw.com/privacy-and-data-security/surveillance-in-spotlight-amid-ongoing-eu-u-s-data-privacy-rift>
206. Wendt A. *Constructing International Politics*. *International Security*. 1995. No. 1(20). P. 71–8.
207. Wenger A. *The Internet and the Changing Face of International Relations and Security*. *Information and Security*. 2001. No. 7. P. 5–11.
208. *What can we learn from the «most devastating» cyberattack in history?* *CBC News*. 22 August 2018. URL: <https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation/>
209. Wolfe Derek. *How China Became a Digital Adversary and Threat to the U.S.* *GSIXchange*. 21 July 2021. URL: <https://gsiexchange.com/how-china-became-a-digital-adversary-and-threat-to-the-u-s/>
210. Xi Jinping calls for 'cyber sovereignty' at internet conference. *BBC*. 16 December 2015. <https://www.bbc.com/news/world-asia-china-35109453>
211. Xinmin Ma. 马新民 · *The Law of Use of Force: Development and Challenges*. *China International Law Yearbook*. 2013. 1, 中国国际法年刊 (2013). 93.
212. Yan Luo, Zhijing Yu, Nicholas Shepherd. *Cybersecurity risk classification under China's multi-level protection scheme*. *Practical Law*. Thomson Reuters. 2021. URL: [https://uk.practicallaw.thomsonreuters.com/w-022-3160?originationContext=document&transitionType=DocumentItem&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/w-022-3160?originationContext=document&transitionType=DocumentItem&contextData=(sc.Default)&firstPage=true)

213. Zetter Kim. New York Times Hacked Again, This Time Allegedly by Chinese. Wired. 31 January 2013. URL: <https://www.wired.com/2013/01/new-york-times-hacked/>
214. Zhong Raymond, Mozur Paul, Krolik Aaron, Kao Jeff. Leaked Documents Show How China's Army of Paid Internet Trolls Helped Censor the Coronavirus. ProPublica. 19 December 2020.
215. Zhu Shenshen. Wuzhen initiative on Internet future. Shanghai Daily. 29 December 2015. URL: <https://archive.shine.cn/business/it/Wuzhen-initiative-on-Internet-future/shdaily.shtml>
216. Zunyou Zhou (). China's Draft Cybersecurity Law. China Briefing. 21 December 2015. 15. No. 24. URL: <https://jamestown.org/program/chinas-draft-cybersecurity-law/>.
217. Быков А. И. Управление Интернетом как одна из проблем современных международных отношений. Политэкс. 2008.
218. В Москве прошел митинг против изоляции Рунета. РБК. 10.03.2019.
219. Вейкфілд Джейн. Китай використовує уйгурів як піддослідних щурів. Що відомо про камери розпізнавання емоцій. *BBC News Україна*. 27.05.2021. URL: <https://www.bbc.com/ukrainian/news-57265671>
220. Глобальная безопасность: инновационные методы анализа конфликтов / под ред. А. И. Смирнова. Москва: Общество «Знание» России, 2011. 272 с.
221. 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>)
222. Дані ЮНКТАД (UNCTADSTAT. International trade in ICT services, value, shares and growth, annual. URL: <https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=158359>)
223. 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
224. Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895) Совет безопасности РФ.
225. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.
226. 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
227. 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>
228. 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>
229. 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>
230. Зиновьева Е. Международное сотрудничество по обеспечению информационной безопасности. *Право и управление. XXI век*. 2014. № 4.
231. Иванов Станислав, Томилов Олег. Кибертерроризм: угроза национальной и международной безопасности. ИА «Оружие России». 14.03.2013.

232. Канев Сергей. Чебурашка, или Хорошими делами прославиться нельзя. *Новая Газета*. 05.2014.
233. Кісілевич-Чорнойван О. М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика*. 2009. № 8. С. 11–18. URL: http://nbuv.gov.ua/UJRN/utp_2009_8_2
234. Конвенція про кіберзлочинність. Офіційний переклад. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
235. Коротков А. В. Безопасность критических информационных инфраструктур в международном гуманитарном праве. *Вестник МГИМО-Университета*. 2011. № 4. С. 154–162.
236. Крутских А. В. К политико-правовым основаниям глобальной информационной безопасности. *Международные процессы*. 2007. № 1(5). С. 28–37.
237. Кучерявый М. М. Глобальное информационное общество и проблемы безопасности. *Власть. Общественно-политический журнал*. 2013. № 9 (сентябрь). С. 89–92.
238. Манойло А. В. Государственная информационная политика в особых условиях: монография. Москва: МИФИ, 2003. 388 с.
239. Манойло А. В. Информационные войны и психологические операции. Руководство к действию. Москва: Горячая Линия-Телеком, 2022.
240. Макаренко Є. А., Рижков М. М., Ожеван М. А., Кучмій О. П., Фролова О. М. Міжнародна інформаційна безпека: теорія і практика: підручник. Київ. Центр вільної преси, 2016. 418 с.
241. Настюк В. Я., Белєвцева В. В. Правові засади міжнародного співробітництва щодо протидії інформаційним правопорушенням. *Правова інформатика*. 2014. № 2(42). URL: <http://ippi.org.ua/sites/default/files/14nvypip.pdf>

242. Основы государственной политики Российской Федерации в области международной информационной безопасности (Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213).
243. Правила поведения в области обеспечения международной информационной безопасности / Документ ООН A/69/723/. 13 января 2015.
244. Принят закон о «суверенном интернете». Государственная Дума Федерального собрания Российской Федерации. 16.04.2009.
245. 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
246. Расторгуев С. П. Введение в формальную теорию информационной войны. Москва: Вузовская кн. 2016.
247. 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
248. Романчук Ю. В. 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, 2009. 20 с.
249. Россия и США перетягивают всемирную паутину. В ООН представлены конкурирующие резолюции по кибербезопасности. *Коммерсантъ*. 12.11.2018. № 207. С. 6.
250. 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>
251. Солодка О. М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. 2020. № 1(32). URL: <http://il.ippi.org.ua/article/view/200311>
252. «Таллинское руководство» о войне в интернете встревожило Россию – этот документ сам по себе опасен. NEWSru.com. 27.05.2013.
253. Указ Президента Российской Федерации от 05.12.2016 г. № 646. Об утверждении Доктрины информационной безопасности Российской Федерации.
254. 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>
255. 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>
256. 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>
257. Федоров А. В., Зиновьева Е. С. Международная информационная безопасность: политическая теория и дипломатическая практика. Москва: МГИМО, 2017. 360 с.
258. Фролова О. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. *Вісник Львівського університету. Серія: Міжнародні відносини*. 2019. Вип. 46. С. 123–136. URL: http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_13

259. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. *Електронне видання Інституту міжнародних відносин «Міжнародні відносини. Серія: Політичні науки»*. 2018. №18. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468
260. Швец Д. Ю. Информационная безопасность Российской Федерации в современных международных отношениях: дис. ... канд. социол. наук. Москва: МГИМО (У) МИД России, 2005. 153 с.
261. Якушев М. В. Информационное общество и правовое регулирование: новые проблемы теории и практики. *Информационное общество*. 1999. № 1.
262. 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
263. 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
264. 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>
265. 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 tèshè 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
266. 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
267. 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
268. 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 xìn xī huà fāzhǎn hé qièshí bǎozhàng xìn xī 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.
269. 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 xìn xī 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 проєкт збору коментарів, 10 липня 2021)» Публічне

- звернення за коментарями]. URL: http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm
270. 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>
271. 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>.
272. 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>.

ГЛОСАРІЙ

Інформаційна війна – комплексне забезпечення політичних і геополітичних інтересів авторитарних держав за допомогою військових та цивільних інформаційних- і кіберзасобів.

Інформаційна загроза – потенційно або реально негативні явища, тенденції й чинники інформаційного впливу, що застосовуються в інформаційній сфері, унеможливають або ускладнюють реалізацію національних інтересів держави й можуть прямо чи опосередковано завдати шкоди її інтересам, національній безпеці та обороні.

Інформаційне протиборство – наступальне й оборонне застосування інформації й інформаційних систем для використання, пошкодження або знищення інформації й інформаційних систем супротивника під час захисту своїх власних.

Інформаційний суверенітет – деклароване авторитарними державами верховенство в розпорядженні певними інформаційними ресурсами, оголошеними невід’ємним складником національного суверенітету, що проявляється в запобіганні проникненню небажаної інформації всередину країни й витоку чутливої інформації за кордон.

Інформаційні операції – дії, ужиті для впливу на інформацію й інформаційні системи супротивника під час захисту власної інформації та інформаційних систем, які застосовуються в усьому діапазоні військових операцій та на всіх рівнях війни.

Кіберактивність – будь-яка діяльність або дія, котра відбувається в кіберпросторі, що включає використання комп’ютерних систем, мереж і цифрових технологій. Вона охоплює широкий спектр дій, як законних, так і зловмисних, що виконуються окремими особами, організаціями або навіть національними державами

Кібервійна – сукупність операцій, що здійснюються засобами й методами ведення військових дій, спрямованих проти комп'ютерів або через комп'ютери чи комп'ютерні мережі шляхом інформаційного потоку, коли такі операції в кіберпросторі застосовуються в контексті збройного конфлікту за змістом міжнародного гуманітарного права.

Кібердипломатія – використання дипломатичних зусиль та переговорів для вирішення кібербезпекових питань між країнами.

Кібердіалог – процес обговорення кіберполітики, безпеки та правил в інтернеті між різними країнами й стейкхолдерами.

Кіберзагроза – наявні й потенційно можливі явища та чинники, що створюють небезпеку життєво важливим національним інтересам держави в кіберпросторі, негативно впливають на стан кібербезпеки держави, кібербезпеку й кіберзахист її об'єктів.

Кіберзброя – комплексна система технічних засобів, програмного забезпечення й тактичних методів, що використовуються для виконання атак, захисту та маніпуляцій у кіберпросторі задля заподіяння шкоди, руйнування або контролю над інформаційними системами, мережами й інфраструктурою противника (використовується в контексті кібервійни й інших кіберопераційних дій).

Кіберзлочинність – сукупність кіберзлочинів, тобто суспільно небезпечних винних діянь у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законодавством й/або яке визнано злочином міжнародними договорами.

Кіберінфраструктура – сукупність комп'ютерних систем, мереж, програмного забезпечення та даних, які утворюють основу цифрового середовища (інформаційні системи, хмарні платформи, мережева інфраструктура, сервери, сховища даних, телекомунікаційні системи й інші компоненти, що забезпечують передачу, зберігання, обробку та управління інформацією), є важливою

складовою частиною для функціонування електронних послуг, економіки й суспільства загалом, а також є об'єктом кіберзагроз та потенційних кібератак.

Кіберінцидент (інцидент кібербезпеки) – неочікувана подія, що може завдати шкоди комп'ютерним системам, мережам, даним або інформації, уключаючи вторгнення, втрату даних, витоки даних тощо.

Кібернорми – прийняті (формально не обов'язкові, або такі, що розглядаються як потенційно обов'язкові) правила й стандарти поведінки держав у кіберпросторі, спрямовані на забезпечення безпеки та стабільності.

Кібероборона – заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету й обороноздатності держави, запобігання виникненню збройного конфлікту та відсічі збройній агресії.

Кіберпростір – віртуальний світ цифрової й електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою.

Кіберсуверенітет – популярна в автократіях і не прийнята в демократичних державах концепція державного контролю над кіберпростором, застереження виняткового права держави на контроль будь-якої інформації, технологій і телекомунікації в мережі (із погляду міжнародного права суверенітет, яким володіє держава над територією, дає їй право контролю кіберінфраструктури та кібердіяльності на її території).

Кібертероризм – політично мотивовані атаки, що здійснюються субнаціональними групами, або таємними агентами, або окремими індивідами проти інформаційних і комп'ютерних систем, комп'ютерних програм або даних, результатом яких є насильство проти некомбатантів.

Критична інфраструктура – системи, мережі й процеси, що мають важливе значення для функціонування суспільства й економіки, пошкодження або недоступність яких можуть мати серйозні наслідки.

Мережева й інформаційна безпека – 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 та пов'язаних із ними служб, доступ до яких відбувається за допомогою таких мереж або систем.

Мережевий нейтралітет – принцип інформаційної політики держави, за якого забезпечується рівний доступ до мережі й комунікації, швидкість передавання даних для кожного користувача, виключаючи таким чином будь-яку можливість маніпулювання вмістом.

Міжнародна інформаційна безпека – концепція у сфері міжнародної політики, що підтримується з боку Росії та декларує на меті досягнення «стану міжнародних відносин, що виключає порушення світової стабільності та створення загрози безпеці держав і світової спільноти в інформаційному просторі».

Міжнародна стратегія кібербезпеки – документ, який визначає політичні й стратегічні цілі, принципи та заходи, спрямовані на співробітництво між країнами для забезпечення кібербезпеки на міжнародному рівні.

Мультистейкхолдерський підхід – підхід, який уключає різні групи зацікавлених сторін, такі як уряди, громадські організації, приватний сектор та академічна спільнота, у процес прийняття рішень і розробки стратегій кібербезпеки й управління інтернетом.

Нарощування кіберпотенціалу – відповідно до «Міжнародній стратегії для кіберпростору» США, допомога країнам, що розвиваються через надання необхідних ресурсів, знань і фахівців, у тому числі для підготовки національних стратегій кібербезпеки

Національна стратегія кібербезпеки – документ, який визначає політичні та стратегічні цілі, принципи й заходи, спрямовані на забезпечення кібербезпеки національного рівня.

Психологічні операції – здійснення впливу на установки й поведінку іноземних цільових груп через різні засоби інформаційного протиборства.

Стратегічне інформаційне протиборство – використання державами глобального інформаційного простору й інфраструктури для проведення стратегічних військових операцій і зменшення дії на власний інформаційний ресурс.

Стратегічні комунікації – скоординоване й належне використання публічної дипломатії, цивільних і військових зв'язків із громадськістю та інформаційних і психологічних операцій на підтримку політики суб'єкта міжнародних відносин та для досягнення його стратегічних цілей.

Наукове електронне видання на CD-ROM

Федонюк Сергій Валентинович

**МІЖНАРОДНА ПОЛІТИКА ІНФОРМАЦІЙНОЇ (КІБЕР) БЕЗПЕКИ.
87 ПИТАНЬ І ВІДПОВІДЕЙ**

Навчальний посібник

Літературний редактор і коректор Г. О. Дробот
Верстання С. В. Федонюк

Один електронний оптичний диск (CD-ROM). Об'єм даних 3,55 МБ.
Тираж 300 прим. Зам. 154. Видавець і виготовлювач – Вежа-Друк,
м. Луцьк, вул. Шопена, 12, тел. 066 936 25 49.
E-mail: vezhaprint@gmail.com
Свідоцтво Держ. комітету телебачення та радіомовлення України
ДК № 4607 від 30.08.2013 р.



ISBN 978-966-940-515-9



9 789669 405159 >