Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

СЯБРО АНАСТАСІЯ ВІКТОРІВНА

УДК 32.327

ДИСЕРТАЦІЯ

ТРАНСФОРМАЦІЯ ПРІОРИТЕТІВ РЕГІОНАЛЬНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (НА ПРИКЛАДІ КРАЇН АТР)

291 – Міжнародні відносини, суспільні комунікації та регіональні студії

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ *Сябро Анастасія Вікторівна*

Науковий керівник *Рижков Микола Миколайович*, доктор політичних наук, професор

Київ – 2022

АНОТАЦІЯ

Сябро А.В. – Трансформація пріоритетів регіональної політики у сфері інформаційної безпеки (на прикладі країн АТР). – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 291 – Міжнародні відносини, суспільні комунікації, регіональні студії. – Київський національний університет імені Тараса Шевченка, Міністерство освіти і науки України, Київ, 2022.

Дисертаційну роботу присвячено дослідженню теоретичних і методологічних аспектів регіональної політики у сфері інформаційної безпеки в умовах трансформації парадигми міжнародної безпеки та прискорення інформаційного та науково-технологічного розвитку, та визначенню особливостей стратегії інформаційної безпеки провідних країн АТР на прикладі Японії та Індії.

У роботі досліджено інформаційні та науково-технологічні чинники трансформації сучасної парадигми міжнародної безпеки; проаналізовано та узагальнено теоретико-методологічні підходи зарубіжних і вітчизняних дослідників до феномену міжнародної та національної інформаційної безпеки; представлено типологію понятєвих категорій інформаційної безпеки; з’ясовано роль інформаційних та науково-технологічних зрушень у формуванні сучасної архітектури регіональної безпеки АТР, охарактеризовано політико-системні особливості стратегії інформаційної безпеки регіональних інститутів, зокрема, Асоціації держав Південно-Східної Азії, Шанхайської організації співробітництва та Чотиристороннього діалогу з питань безпеки (QUAD); досліджено особливості стратегії інформаційної безпеки Японії та Індії.

Дослідження особливостей впливу інформаційного та науково-технологічного розвитку на сучасну архітектуру безпеки АТР показало, що інноваційні зрушення стали не тільки каталізатором вже існуючих проблем у традиційних вимірах геополітичного протиборства, але й призвели до появи нових викликів і загроз – інформаційних війн і конфліктів, політично мотивованих інформаційних атак,

кіберзлочинності, кібершахрайства та кібертероризму, що обумовило включення питань інформаційної безпеки до пріоритетів регіональної безпекової політики. На основі політичного аналізу діяльність провідних регіональних інститутів (АСЕАН, ШОС та QUAD) узагальнено особливості регіональної політики інформаційної безпеки та з'ясовано, що модернізація інформаційних викликів та загроз призводить до потреби регулярно переглядати стратегії інформаційної безпеки та включати до її пріоритетів нові напрями діяльності.

Розгляд особливостей стратегії інформаційної безпеки Японії уможливив висновки про те, що її базовим пріоритетом на сучасному етапі є формування безпечного інформаційного середовища для розбудови сталої, інклюзивної соціально-економічної системи «Суспільства 5.0» , що базується на цифрових технологіях, таких як аналітика великих даних, штучний інтелект, Інтернет речей і робототехніка. З'ясування пріоритетів політики інформаційної безпеки Індії показало, що держава, яка відрізняється високими темпами інформаційного та науково-технологічного розвитку, демонструє загалом недостатню ефективність реалізації стратегій сфері кібербезпеки, про що свідчить постійне зростання кількості економічно та політично мотивованих атак на інформаційний простір та інфраструктуру держави. Характерними особливостями підходу Індії у сфері реалізації політики інформаційної безпеки є прагнення уряду Індії поєднати зорієнтовані на ринок механізми з регулюванням за активної участі держави та переважно реактивний характер діяльності у сфері кібербезпеки, що не дозволяє створити ефективні механізми захисту інформаційного простору держави.

Наукова новизна одержаних результатів визначається тим, що дисертаційна робота є оригінальним системним дослідженням регіональної політики інформаційної безпеки у сучасних міжнародних відносинах, що містить аналіз новітніх тенденцій у теорії і практиці забезпечення національної безпеки провідних держав АТР в умовах потужних інформаційних та науково-технологічних зрушень. У проведеному дослідженні:

Вперше:

- на оригінальних джерелах здійснено аналіз інформаційного виміру регіональної архітектури безпеки АТР та встановлено, що в умовах швидкоплинного інформаційного і науково-технологічного розвитку базові характеристики системи безпеки регіону набувають нового характеру, зокрема, зростають масштаби використання у територіальних конфліктах інформаційних методів протиборства, посилюється геополітичні позиції провідних держав регіону за рахунок нарощування кібермогутності, набуває розвитку стратегія «кіберстримування» Китаю, відбувається модернізація військової потужності основних гравців регіону завдяки використання досягнень у сфері науки і технологій;

- розглянуто діяльність Чотиристороннього діалогу з питань безпеки (QUAD) у сфері кібербезпеки, яка спрямована на формування високого потенціалу стійкості інформаційної інфраструктури з метою усунення вразливостей для кібербезпеки та вироблення ефективних механізмів протидії кіберзагрозам, визначено, що основними принципами політики кібербезпеки є посилення співпраці у сфері безпеки критичної інформаційної інфраструктури, управління ризиками, ефективна співпраця між усіма зацікавленими сторонами; впровадження стратегії формування «кіберстійкості» замість стратегії «наступальних кіберможливостей» для створення ефективної системи захисту від кіберзагроз з боку Китаю;

- проаналізовано політику інформаційної безпеки провідних держав АТР – Японії та Індії і встановлено, що незважаючи на високі темпи інформаційного та науково-технологічного розвитку та збільшення масштабів інформаційних викликів і загроз для обох країн, пріоритети політики інформаційної безпеки та підходи до їх реалізації мають суттєві відмінності, які полягають у механізмах забезпечення балансу інтересів всіх зацікавлених сторін, особливостях реагування на кіберкризи, наявності чіткої структури системи інформаційної безпеки, у різному рівні розвитку інформаційної грамотності суспільства, наявності ефективних механізмів аудиту інформаційної безпеки, що суттєво впливає на ефективність реалізації політики інформаційної безпеки в обох країнах.

Удосконалено:

- твердження про сучасну трансформацію парадигми міжнародної безпеки, що відбувається внаслідок інформаційних і науково-технологічних зрушень та появи нових викликів і загроз, які потребують вироблення сучасних механізмів запобігання ним з метою забезпечення міжнародного миру і безпеки;
- аргументацію про те, що в сучасній регіональній структурі інформаційної безпеки АТР відбувається перегляд базових підходів до формування пріоритетів інформаційної безпеки, наслідком чого є вироблення спільного бачення проблеми всіма державами-учасницями, розробка ефективних механізмів протидії сучасним інформаційним загрозам на рівні регіону як чинник створення регіонального кіберпотенціалу та формування кіберстійкості регіону.

Набуло подальшого розвитку:

- визначення типології понятєво-категоріальних характеристик інформаційної безпеки і доведено, що подальший інформаційний та науково-технологічний розвиток впливає на міжнародну систему інформаційної безпеки, обумовлює потребу постійно переглядати теоретичні і концептуальні підходи, відповідно до нових реалій, пов'язаних з появою нетрадиційних викликів і загроз та нових форм протиборства у сучасних міжнародних відносинах;
- дослідження політики інформаційної безпеки на рівні міжнародних регіональних організацій, зокрема, АСЕАН та ШОС, що уможливило висновки про трансформацію пріоритетів їх діяльності, спрямовану на протидію новим викликам і загрозам, які виникають внаслідок подальшого інформаційного і науково-технологічного розвитку світу.

Практичне значення отриманих результатів полягає у тому, що теоретичні висновки та узагальнення, представлені у дисертаційній роботі, можуть бути використані у подальших наукових дослідженнях сучасної регіональної та національної політики інформаційної безпеки, враховані у практиці діяльності дипломатичних установ і департаментів МЗС України, реалізації політики України щодо країн Індо-Тихоокеанського регіону, а також у діяльності урядових, політичних, науково-дослідницьких і громадських інституцій, які займаються

питаннями національної інформаційної безпеки та оборони, реформуванням базових стратегічних документів України у сфері інформаційної безпеки – Доктрини інформаційної безпеки та Стратегії кібербезпеки України.

Ключові слова: інформаційна безпека, кібербезпека, регіональна архітектура безпеки, міжнародні організації, АСЕАН, ШОС та QUAD, Індія, Японія, США, КНР, Пакистан.

ANNOTATION

Anastasiia Siabro – Transformation of regional policy priorities in the field of information security (on the example of APR countries). – Manuscript.

The thesis for the Doctor of Philosophy degree on specialty 291 – International Relations, Social Communications and Regional Studies. – Taras Shevchenko National University of Kyiv, Ministry of Education and Science of Ukraine, Kyiv, 2022.

The dissertation is devoted to the study of theoretical and methodological aspects of regional policy in the field of information security in the context of the transformation of the international security paradigm and the acceleration of information and scientific-technological development, and to the determination of the features of the information security strategy of the leading APR countries using the example of Japan and India.

The paper analyses the information and scientific-technological factors of the transformation of the modern paradigm of international security; the theoretical and methodological approaches of foreign and domestic researchers to the phenomenon of international and national information security are analyzed and summarized; a typology of conceptual categories of information security is presented; the role of information and scientific-technological changes in the formation of the modern architecture of the regional security of the APR is clarified, the political and systemic features of the information security strategy of regional institutions are characterized, in particular, the Association of SouthEast Asian Nations, the Shanghai Cooperation Organization and the Quadrilateral Security Dialogue (QUAD); the peculiarities of the information security strategy of Japan and India are investigated.

The research of the specifics of the influence of information and scientific-technological development on the modern security architecture of the Asia-Pacific region showed that innovative achievements became not only a catalyst for existing problems in the traditional dimensions of geopolitical confrontation, but also led to the emergence of new challenges and threats - information wars and conflicts, politically motivated information attacks, cybercrime, cyberfraud and cyberterrorism, which led to the inclusion of information security issues in the priorities of the regional security policy. On the basis of a political analysis of the activities of leading regional institutions (ASEAN, SCO and QUAD), the features of the regional information security policy were summarized and it was found that the modernization of information challenges and threats leads to the need of regularly revising of information security strategies and including new areas of activity in its priorities.

Consideration of the features of Japan's information security strategy made it possible to conclude that its basic priority at the current stage is the formation of a secure information environment for the development of a sustainable, inclusive socio-economic system of «Society 5.0» , based on digital technologies, such as big data analytics, artificial intelligence, Internet of things and robotics. Clarification of the priorities of India's information security policy showed that the state, which is characterized by high rates of information and scientific-technological development, demonstrates a generally insufficient effectiveness of the implementation of strategies in the field of cyber security, which is evidenced by the constant increase in the number of economically and politically motivated attacks on the information sphere and infrastructure of the state. Characteristic features of India's approach in the field of information security policy implementation are the desire of the Indian government to combine market-oriented mechanisms of regulation with the active participation of the state and the predominantly reactive nature of activities in the field of cyber security, which does not allow to create effective mechanisms for the protection of the state's information space.

The scientific novelty of the obtained results is determined by the fact that the dissertation is an original systematic study of the regional policy of information security in modern international relations, containing an analysis of the latest trends in the theory and

practice of ensuring the national security of the leading APR states in the conditions of powerful information and scientific-technological achievements. In the conducted research:

For the first time:

- based on original sources, an analysis of the information dimension of the regional security architecture of the APR was carried out and it was established that in the conditions of rapid information and scientific-technological development, the basic characteristics of the security system of the region are acquiring a new character, in particular, the scope of the use of information methods of confrontation in territorial conflicts is increasing, the geopolitical positions of the leading states of the region are strengthening due to the increase of cyber power, the strategy of «cyber containment» of China is developing, the military power of the main players in the region is being modernized due to the use of achievements in the field of science and technology;
- considered the activities of the Quadrilateral Security Dialogue (QUAD) in the field of cyber security, which is aimed at forming a high potential for the stability of information infrastructure in order to eliminate vulnerabilities for cyber security and develop effective mechanisms for countering cyber threats, it was determined that the main principles of cyber security policy are to strengthen cooperation in the field of security critical information infrastructure, risk management, effective cooperation between all stakeholders, implementation of the strategy of forming «cyber resilience» instead of the strategy of «offensive cyber capabilities» to create an effective system of protection against cyber threats from China;
- the information security policy of the leading APR states - Japan and India was analyzed and it was established that despite the high pace of information and scientific-technological development and the increase in the scale of information challenges and threats for both countries, the priorities of the information security policy and approaches to their implementation have significant differences, which consist in the mechanisms for ensuring the balance of interests of all stakeholders, the specifics of responding to cyber crises, the presence of a clear structure of the information security system, the different level of development of information literacy in society, the presence of effective

information security audit mechanisms, which significantly affects the effectiveness of information security policy implementation in both countries.

The following questions were advanced:

- a statement about the modern transformation of the paradigm of international security, which occurs as a result of information and scientific and technological shifts and the emergence of new challenges and threats, which require the development of modern mechanisms to prevent them in order to ensure international peace and security;

- the argument that in the modern regional structure of information security of the APR there is a review of basic approaches to the formation of information security priorities, the result of which is the development of a common vision of the problem by all participating states, the development of effective mechanisms for countering modern information threats at the regional level as a factor in the creation of regional cyber potential and the formation of the region's cyber resilience.

The following questions were further developed:

- the definition of the typology of conceptual and categorical characteristics of information security and it is proven that further information and scientific and technological development affects the international system of information security, determines the need to constantly review theoretical and conceptual approaches, in accordance with new realities associated with the emergence of non-traditional challenges and threats and new forms of confrontation in modern international relations;

- the research of information security policy at the level of international regional organizations, in particular, ASEAN and the SCO, which made it possible to draw conclusions about the transformation of the priorities of their activities aimed at countering new challenges and threats that arise as a result of further information and scientific and technological development of the world.

The practical significance of the obtained results is that the theoretical conclusions and generalizations presented in the dissertation work can be used in further scientific studies of modern regional and national information security policy, taken into account in the practice of activities of diplomatic institutions and departments of the Ministry of Foreign Affairs of Ukraine, the implementation of Ukraine's policy towards countries of

the Indo-Pacific region, as well as in the activities of government, political, research and public institutions dealing with issues of national information security and defense, reforming the basic strategic documents of Ukraine in the field of information security - the Doctrine of Information Security and the Cyber Security Strategy of Ukraine.

Keywords: information security, cyber security, regional security architecture, international organizations, ASEAN, SCO and QUAD, India, Japan, USA, China, Pakistan.

Список публікацій здобувача за темою дисертації

Статті у наукових фахових виданнях України:

1. **Сябро А.В.** Сучасний стан розвитку інформаційно-комунікаційних технологій в Україні. *Гілея: науковий вісник.* 2018. Вип. 135 (№8). С. 364-367.

2. **Сябро А.В.** Пріоритети співробітництва Японії зі США у сфері кібербезпеки. *Гілея: науковий вісник*. 2019. Вип. 150 (№ 11). Ч. 3. С.72-77.

3. Рижков М.М., **Сябро А.В.** Позиції держав Азійсько-Тихоокеанського регіону щодо ухвалення резолюцій з питань міжнародної інформаційної безпеки в рамках ООН. *Актуальні проблеми міжнародних відносин.* 2019. Вип. 139. С.13-26.

4. **Сябро А.В.** Особливості національної стратегії кібербезпеки Індії. *Міжнародні відносини. Серія «Політичні науки».* 2019. № 20. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/4136

Статті в іноземних виданнях:

5. **Siabro Anastasiia.** The influence of scientific and technological development on the transformation of the global security paradigm. « *Evropský politický a právní diskurz» («European political and law discourse»).* 2021. Vol. 8 Iss. 5. C. 6-13.

Праці, які додатково відображають наукові результати дисертації:

6. **Сябро А.В.** Мілітаризація кіберпростору як чинник актуалізації проблеми інформаційної безпеки у сучасних міжнародних відносинах. *Міжнародна інформація / Міжнародні комунікації: історія, сучасність і перспективи:* матеріали Міжнародної науково-практичної конференції, 6 грудня 2019 року. *Міжнародні відносини. Серія «Політичні науки».* 2019. № 21. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/3873/3533

7. **Сябро А.В.** Проблема запровадження обмежень у сфері інформації і комунікації як чинник забезпечення національної інформаційної безпеки. *Стратегічне позиціонування України в сучасному міжнародному просторі*: матеріали Міжнародної науково-теоретичної конференції, 15 жовтня 2020 року. Київ, 2020. С. 72-73.

8. **Сябро А.В.** Сутнісні характеристики стратегії інформаційної безпеки Південної Кореї. *Актуальні питання суспільних та гуманітарних наук (Глухівські читання-2020)*: збірник матеріалів X Міжнародної науково-практичної інтернет-конференції, 9-11 грудня 2020 року. Глухів: Глухівський НПУ ім. О. Довженка, 2020. С. 113-115.

9. **Сябро А.В.** Трансформація концепту «м'якої» сили в сучасному інформаційному протиборстві. *Травневі студії 2021: історія, міжнародні відносини, філософія:* збірник матеріалів III Міжнародної наукової конференції студентів та молодих вчених, 23 квітня 2021 року. Вінниця: ДонНУ імені Василя Стуса, 2021. Вип. 6. С. 92-94.

10. **Сябро А.В.** Інформаційна безпека у стратегіях діяльності міжнародних регіональних організацій (на прикладі АТР). *Шевченківська весна 2021:* матеріали Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених, 29 березня, 2021. Київ, 2021. С. 51-55.

ЗМІСТ

ВСТУП …… **14**

РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ …… **23**

1.1. Трансформація парадигми міжнародної безпеки в умовах розбудови інформаційної цивілізації …….. 23

1.2. Теоретичні і концептуальні підходи до проблеми інформаційної безпеки у зарубіжній та вітчизняній політологічній думці ……. 36

1.3. Понятєво-категоріальні характеристики інформаційної безпеки …….. 61

Висновки до першого розділу……. 74

РОЗДІЛ 2. Регіональна політика інформаційної безпеки …… **76**

2.1. Інформаційна складова сучасної архітектури безпеки Азії ……. 76

2.2. Сутнісні характеристики міжнародного співробітництва у сфері інформаційної безпеки в рамка Асоціації держав Південно-Східної Азії …… 95

2.3. Особливості політики інформаційної безпека Шанхайської організації співробітництва …… 107

Висновки до другого розділу …… 126

РОЗДІЛ 3. Трансформація пріоритетів політики інформаційної безпеки Японії та Індії …….. **129**

3.1. Сучасні пріоритети стратегії інформаційної безпеки Японії ……..... 129

3.2. Еволюція національної політики кібербезпеки Індії …… 155

Висновки до третього розділу……. 180

ВИСНОВКИ …… **183**

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……... **191**

ДОДАТКИ …… **217**

ВСТУП

Обґрунтування вибору теми дослідження визначається процесами трансформації парадигми міжнародної безпеки, обумовленими прискореним інформаційним та науково-технологічним розвитком. Зростання кількості конфліктів з використанням високотехнологічних озброєнь, трансформація стратегії і тактики ведення війни, поширення практики використання методів кібервійни та гібридної війни, мілітаризація кіберпростору та зростання масштабів негативних наслідків появи кіберфізичних систем призвели до потреби переглянути принципи і підходи до формування глобальної і регіональної архітектури безпеки. Тому питання розробки і реалізації стратегії інформаційної безпеки набули значної актуальності та увійшли до пріоритетів діяльності регіональних інституцій (АСЕАН, ШОС), були включенні до пріоритетних напрямів двостороннього співробітництва між США та їх союзниками у регіоні (Японією, Індією та Австралією) та кібердипломатії провідних країн АТР.

Вибір теми дослідження щодо політики інформаційної безпеки провідних країн АТР визначається динамікою їх інформаційного і науково-технологічного розвитку та перетворенням цих держав на об’єкти постійних економічно чи політично мотивованих інформаційних впливів і атак. В умовах розширення практики використання досягнень науки і техніки у геополітичному протистоянні провідних держав регіону зростає актуальність розробки і реалізації національних стратегій інформаційної безпеки з метою захисту національних інтересів та суверенітету. Важливим чинником дестабілізації регіональної системи інформаційної безпеки виступає також інформаційне протистояння США і КНР, що суттєво підвищує роль і значення інструменту двосторонніх альянсів з державами-союзниками у регіоні та використання їх потенціалу для реалізації стратегії стримування Китаю у кіберпросторі. До того ж, дедалі частіше країни АТР почали використовувати у територіальних конфліктах методи інформаційного протиборства, що призводить до подальшої мілітаризації кіберпростору та гонки сучасних високотехнологічних озброєнь. Отже, для провідних держав АТР – Японії

та Індії – питання інформаційної безпеки набувають критичного значення, що обумовлює активізацію їх діяльності у сфері розробки та реалізації стратегії інформаційної безпеки, важливою складовою яких є нарощування кіберпотенціалу та формування ефективної системи кібероборони.

Таким чином, основний напрям дослідження полягає у вивченні досвіду провідних країн АТР у розробці та реалізації стратегій інформаційної безпеки в умовах подальшого прискорення інформаційних та науково-технологічних зрушень, зростання масштабів використання інноваційних досягнень для економічно та політично мотивованих атак на інформаційний простір цих держав, їх критичну інформаційну інфраструктуру та населення. Вивчення стратегій інформаційної безпеки Японії та Індії дозволило з'ясувати особливості механізмів забезпечення інформаційної безпеки держав, що є корисним для удосконалення стратегії інформаційної безпеки України.

Актуальність дослідження глобальної і регіональної політики у сфері інформаційної безпеки викликає значний інтерес багатьох зарубіжних та вітчизняних дослідників. Зокрема, у роботах Д. Альбертса, Д. Арквілли, Р. Армітіджа, Р. Бенкера, Б. Берковіца, Л.К. Вентса, Д. Гарстки, К. Демчака, Д. Деннінга, П. Домбровського, Р. Ендреса, А. Ечеваррії, О. Клімберга, М. ван Кревельда, Ф.Д. Креймера, М. Лібікі, У. Лінда, Л. Мура, Дж. Ная, У. Оуенса, Г. Реттрея, Д. Ронфельдта, А. Себровскі, Е. Сміта, С. Старра, Д. Стейна, Е. Тоффлера, Г. Тоффлер, Т. Хеммса, Д. Уордена, Ф. Хоффмана, Р. Шафранскі, В. Швартау, Д. Шелдона, Ф. Штейна та ін. представлено аналіз трансформації сучасної парадигми безпеки в умовах прискореного інформаційного і науково-технологічного розвитку, виникнення нових високотехнологічних викликів і загроз для системи підтримання миру і безпеки, формування кібервестфальської системи, мілітаризації кіберпростору, нових підходів до використання сили у сучасних міжнародних відносинах, кібермогутності сучасних держав, війни четвертого покоління, інформаційної війни, кібервійни, мережевої та мережноцентрованої війни, «тринітарної» війни, гібридної війни, інформаційного озброєння та

«перегорнутої мілітаризованої дипломатії» . Основні ідеї і висновки фахівців були використані в дисертаційній роботі.

Наукові розвідки з проблем інформаційної безпеки українських дослідників (О. Андрєєвої, А. Баровської, Н. Бєлоусової, В. Бойко, О. Добржанської, Д. Дубова, В. Горбуліна С. Гнатюка, О. Гребініченка, О. Запорожець, Т. Ісакової, М. Копійки, Б. Кормича, О. Кучмій, В. Ліпкана, О. Литвиненка, А. Луценко, Є. Макаренко, М. Ожевана, Г. Перепелиці, В. Петрова, А. Покровської, С. Постоловського, Г. Почепцова, М. Рижкова, Ю. Романчука, О. Сосніна, О. Фролової, Г. Яворської та ін.) присвячені дослідженню кіберпростору як нового виміру геополітичного протиборства, глобального політико-інформаційного простору, кібермогутності, формування нової парадигми світової безпеки в умовах становлення інформаційної цивілізації, моделей міжнародної інформаційної безпеки, права міжнародної інформаційної безпеки, діяльності міжнародно-політичних інститутів у сфері інформаційної безпеки, проблем інформаційної, когнітивної, віртуальної та гібридної війни, проведення спеціальних інформаційних операцій, державно-приватного партнерства у сфері кібербезпеки, еволюції підходів до використання сили у сучасних міжнародних відносинах тощо. Отже, в умовах подальшого інформаційного та науково-технологічного розвитку, проблема інформаційної безпеки стає дедалі більш актуальною і потребує наукового аналізу як на теоретичному, так і прикладному рівнях, враховуючи досвід провідних акторів у реалізації стратегій протидії сучасним викликам і загрозам. Для України, в умовах масштабної воєнної та інформаційної агресії, вивчення досвіду таких країн, як Японія та Індія, які змушені протистояти потужним геополітичним супротивникам в кіберпрострі та застосовувати різноманітні засоби протидії інформаційним атакам, є вкрай потрібним для формування сучасного бачення проблеми та вироблення ефективним механізмів протистояння інформаційним викликам і загрозам.

Зв’язок роботи з науковими програмами, планами, темами, грантами. Дослідження виконано у рамках комплексної програми науково-дослідних робіт Київського національного університету імені Тараса Шевченка і наукової теми Інституту міжнародних відносин Київського національного університету імені

Тараса Шевченка «Асоціація як новий формат відносин України з Європейським Союзом: політичний, правовий, економічний та інформаційний аспекти» (номер державної реєстрації 16БФ048-01).

Мета і завдання дослідження. Мета дослідження полягає у тому, щоб на основі теоретичного і практичного матеріалу цілісно представити характеристики сучасної регіональної архітектури безпеки в умовах інформаційних і науково-технологічних зрушень та виявити національні особливості стратегій інформаційної безпеки країн АТР на прикладі Японії та Індії. Досягнення поставленої мети зумовило розв'язання таких дослідницьких **завдань:**

- визначити та проаналізувати інформаційні та науково-технологічні чинники трансформації сучасної парадигми міжнародної безпеки;
- критично проаналізувати та узагальнити теоретико-методологічні підходи зарубіжних і вітчизняних дослідників до феномену міжнародної та національної інформаційної безпеки;
- дослідити понятєво-категоріальні характеристики проблеми інформаційної безпеки та проаналізувати сучасні підходи до визначення понятєвих категорій, трансформація яких обумовлена зміною парадигми міжнародної безпеки;
- з'ясувати роль інформаційних та науково-технологічних зрушень у формуванні сучасної архітектури регіональної безпеки АТР
- охарактеризувати політико-системні особливості стратегії інформаційної безпеки регіональних інститутів, зокрема, Асоціації держав Південно-Східної Азії, Шанхайської організації співробітництва;
- проаналізувати еволюцію стратегії інформаційної безпеки Японії, визначити сучасні пріоритети та механізмів їх реалізації в умовах постійного зростання масштабів економічно і політично мотивованих атак на інформаційний простір держави;
- дослідити трансформацію підходів до політики кібербезпеки Індії, визначити чинники, що впливають на ефективність її реалізації та формування національної системи інформаційної безпеки та оборони.

З урахуванням зазначеної мети і завдань, *об'єктом* дослідження виступає сфера міжнародних відносин в умовах трансформації парадигми міжнародної безпеки, а *предметом* дослідження є політика регіональної інформаційної безпеки у сучасних міжнародних відносинах.

Методи дослідження. Для вивчення особливості трансформації регіональної політики у сфері інформаційної безпеки у роботі було використано загальнонаукові, загальнологічні та спеціальні методи дослідження, які уможливили цілісне бачення феномену інформаційної політики у сучасних міжнародних відносинах і дозволили виявити регіональні і національні особливості політики інформаційної безпеки АТР. Так, було використано політологічний метод – для аналізу теоретичних і концептуальних засад дослідження проблеми інформаційної безпеки, системний і структурно-функціональний методи – для вивчення понятєво-категоріальних характеристик політики інформаційної безпеки, компаративний метод – для аналізу діяльності регіональних інститутів у сфері інформаційної безпеки, політико-системний метод – для виявлення особливостей реалізації стратегій інформаційної безпеки провідними регіональними державами; політологічний нормативно-ціннісний метод – для вивчення особливостей нормативно-правового забезпечення політики інформаційної безпеки на рівні дво- та багатостороннього співробітництва у сучасних міжнародних відносинах.

Обраний методологічний підхід уможливив комплексне дослідження сучасної регіональної політики інформаційної безпеки із врахуванням процесів, пов'язаних з трансформацією міжнародної парадигми безпеки в умовах пришвидшеного процесу інформаційного і науково-технологічного розвитку, зростання залежності діяльності держав регіону від стратегій і практики діяльності регіональних інститутів та зростання геополітичних протиріч між провідними регіональними державами АТР. Використання зазначених методів дозволило конкретизувати та якісно наповнити змісту дисертаційної роботи, перевірити сформульовані аналітичні узагальнення та аргументувати потребу постійного оновлення стратегій інформаційної безпеки і механізмів їх реалізації для ефективного протистояння сучасним викликам і загрозам, що впливають на подальший поступальний розвиток сучасної держави.

Джерельну базу дослідження складають документи з питань регіональної політики інформаційної безпеки міжнародних регіональних організацій (АСЕАН, ШОС), стратегічні та нормативно-правові документи з інформаційної безпеки урядів провідних країн АТР, зокрема, Японії та Індії, спеціальні аналітичні дослідження провідних науково-дослідницьких центрів та міжнародних організації з різних аспектів глобальної і регіональної політики інформаційної безпеки, а також чисельні статистичні матеріали та бази даних.

Хронологічні межі дослідження визначено 1990-ті рр. – початок 2022 р. Нижня межа дослідження обумовлена ухваленням перших стратегічних документів у сфері інформаційної безпеки регіональних інститутів та провідних держав АТР. Верхня хронологічна межа окреслена початком 2022 р., коли розпочинається перегляд пріоритетів діяльності у сфері інформаційної безпеки провідних акторів міжнародних відносин внаслідок військової агресії РФ проти України.

Наукова новизна одержаних результатів визначається тим, що дисертаційна робота є оригінальним системним дослідженням регіональної політики інформаційної безпеки у сучасних міжнародних відносинах, що містить аналіз новітніх тенденцій у теорії і практиці забезпечення національної безпеки провідних держав АТР в умовах потужних інформаційних та науково-технологічних зрушень. У проведеному дослідженні:

Вперше:

- на оригінальних джерелах здійснено аналіз інформаційного виміру регіональної архітектури безпеки АТР та встановлено, що в умовах швидкоплинного інформаційного і науково-технологічного розвитку базові характеристики системи безпеки регіону набувають нового характеру, зокрема, зростають масштаби використання у територіальних конфліктах інформаційних методів протиборства, посилюється геополітичні позиції провідних держав регіону за рахунок нарощування кібермогутності, набуває розвитку стратегія «кіберстримування» Китаю, відбувається модернізація військової потужності основних гравців регіону завдяки використання досягнень у сфері науки і технологій;

- розглянуто діяльність Чотиристороннього діалогу з питань безпеки (QUAD) у сфері кібербезпеки, яка спрямована на формування високого потенціалу стійкості інформаційної інфраструктури з метою усунення вразливостей для кібербезпеки та вироблення ефективних механізмів протидії кіберзагрозам, визначено, що основними принципами політики кібербезпеки є посилення співпраці у сфері безпеки критичної інформаційної інфраструктури, управління ризиками, ефективна співпраця між усіма зацікавленими сторонами; впровадження стратегії формування «кіберстійкості» замість стратегії «наступальних кіберможливостей» для створення ефективної системи захисту від кіберзагроз з боку Китаю;

- проаналізовано політику інформаційної безпеки провідних держав АТР – Японії та Індії і встановлено, що незважаючи на високі темпи інформаційного та науково-технологічного розвитку та збільшення масштабів інформаційних викликів і загроз для обох країн, пріоритети політики інформаційної безпеки та підходи до їх реалізації мають суттєві відмінності, які полягають у механізмах забезпечення балансу інтересів всіх зацікавлених сторін, особливостях реагування на кіберкризи, наявності чіткої структури системи інформаційної безпеки, у різному рівні розвитку інформаційної грамотності суспільства, наявності ефективних механізмів аудиту інформаційної безпеки, що суттєво впливає на ефективність реалізації політики інформаційної безпеки в обох країнах.

Удосконалено:

- твердження про сучасну трансформацію парадигми міжнародної безпеки, що відбувається внаслідок інформаційних і науково-технологічних зрушень та появи нових викликів і загроз, які потребують вироблення сучасних механізмів запобігання ним з метою забезпечення міжнародного миру і безпеки;

- аргументацію про те, що в сучасній регіональній структурі інформаційної безпеки АТР відбувається перегляд базових підходів до формування пріоритетів інформаційної безпеки, наслідком чого є вироблення спільного бачення проблеми всіма державами-учасницями, розробка ефективних механізмів протидії сучасним інформаційним загрозам на рівні регіону як чинник створення регіонального кіберпотенціалу та формування кіберстійкості регіону.

Набуло подальшого розвитку:

- визначення типології понятєво-категоріальних характеристик інформаційної безпеки і доведено, що подальший інформаційний та науково-технологічний розвиток впливає на міжнародну систему інформаційної безпеки, обумовлює потребу постійно переглядати теоретичні і концептуальні підходи, відповідно до нових реалій, пов'язаних з появою нетрадиційних викликів і загроз та нових форм протиборства у сучасних міжнародних відносинах;
- дослідження політики інформаційної безпеки на рівні міжнародних регіональних організацій, зокрема, АСЕАН та ШОС, що уможливило висновки про трансформацію пріоритетів їх діяльності, спрямовану на протидію новим викликам і загрозам, які виникають внаслідок подальшого інформаційного і науково-технологічного розвитку світу.

Практичне значення отриманих результатів полягає у тому, що теоретичні висновки та узагальнення, представлені у дисертаційній роботі, можуть бути використані у подальших наукових дослідженнях сучасної регіональної та національної політики інформаційної безпеки, враховані у практиці діяльності дипломатичних установ і департаментів МЗС України, реалізації політики України щодо країн Індо-Тихоокеанського регіону, а також у діяльності урядових, політичних, науково-дослідницьких і громадських інституцій, які займаються питаннями національної інформаційної безпеки та оборони, реформуванням базових стратегічних документів України у сфері інформаційної безпеки – Доктрини інформаційної безпеки та Стратегії кібербезпеки України. Теоретичні узагальнення, матеріали та висновки дисертаційної роботи можуть доповнити зміст навчальних курсів політологічного характеру, зокрема, з теорії міжнародних відносин та зовнішньої політики, конфліктології та медіації, міжнародної інформації та комунікації, міжнародної інформаційної безпеки, інформаційного протиборства, національної безпеки, стратегічних комунікацій, технологій медіавпливу, інформаційних операцій в мережевих медіа, практики протидії дезінформації та інших спеціальних дисциплін для студентів вищих навчальних закладів України.

Апробація матеріалів дисертації. Ключові положення наукового дослідження було апробовано на міжнародних науково-практичних, науково-теоретичних конференціях і круглих столах, зокрема: міжнародній науково-практичній конференції «Міжнародна інформація: історія, сучасність і перспективи» (6 грудня 2019 р., м. Київ); міжнародній науково-теоретичної конференції «Стратегічне позиціонування України в сучасному міжнародному просторі» (15 жовтня 2020 р., м. Київ); міжнародній науково-практичній конференції «Глухівські наукові читання – 2020. Актуальні питання суспільних та гуманітарних наук» (9-11 грудня 2020 р., м. Глухів); міжнародній науково-практичній конференції студентів, аспірантів і молодих вчених «Шевченківська весна» (29 березня 2021 року, м. Київ); міжнародній науковій конференції «Травневі студії 2021» (23 квітня 2021, м. Вінниця). Наукові узагальнення та висновки дисертації обговорювалися на наукових семінарах, круглих столах і міжкафедральних засіданнях Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка.

Публікації. За результатами дослідження опубліковано 10 наукових робіт: 4 статті, які вийшли у наукових фахових виданнях України; 1 стаття в іноземному виданні; 5 праць, які додатково відображають наукові результати дисертації.

Структурно дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації – 220 сторінок, в тому числі основний текст – 177 сторінки, список використаних джерел складається з 226 найменувань і займає 26 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

1.1. Трансформація парадигми міжнародної безпеки в умовах розбудови інформаційної цивілізації

Інформаційний та науково-технологічний розвиток країн і регіонів світу призвів до глибинних зрушень у сфері безпеки. Як свідчать чисельні теоретичні і прикладні дослідження феномену розбудови інформаційної цивілізації, найбільш важливою проблемою подальшого поступального розвитку людства нині виступає проблема трансформації парадигми міжнародної безпеки із врахуванням нових викликів і загроз, що виникли внаслідок бурхливого інформаційного та наукового-технологічного розвитку.

Слід підкреслити, що в умовах потужних технологічних зрушень відбувається перегляд класичних теорій міжнародної безпеки, що стало необхідним внаслідок цілої низки факторів, які вплинули на формування сучасного середовища безпеки. Серед найбільш важливих експерти виділяють: зміну характеру, масштабів та спектру конфліктів, зростання кількості асиметричних війн і конфліктів, полегшення доступу до більш потужного озброєння, зростання загрози тероризму та екстремізму, суперечливість мотивів та відносно хаотичну організацію залучених до конфліктів сторін. Диверсифікація загроз та діючих акторів призводить до появи нових викликів для світового співтовариства, в цілому, та структур, що займаються питання безпеки та оборони, зокрема. Вразливість світу збільшується не тільки завдяки пришвидшенню процесів глобалізації, збільшенню масштабів міграції, геополітичним зрушенням та зміни балансу сил, але й тому, що було значно розширено доступ до сучасних інформаційних та науково-технологічних ресурсів. Власне це й призводить до трансформації сучасної парадигми міжнародної безпеки (European Commission, 2020.).

Найбільш значимим фактором, що впливає на зміну парадигми безпеки, є поява нових технологій в рамках Четвертої промислової революції. Зрушення, про

які почали активно говорити у Німеччині у 2011 р. як про новий етап промислової революції (MacDougall, 2014), у 2016 р. та 2018 р. були остаточно представлені як нова концепція індустріального розвитку світу у доповідях засновника Світового економічного форуму у Давосі К. Шваба «Четверта індустріальна революція» (2016) та «Формуючи четверту індустріальну революцію» (2018) (Шваб, 2019). Як зазначається у документах, завдяки бурхливому науково-технологічному прогресу та активному впровадженню інновацій, відбувається не тільки формування нової технологічної бази індустріального розвитку, але й значні зміни у всіх сферах життєдіяльності людини. Серед основних науково-технологічних досягнень, що вже з'явилися чи мають з'явитися найближчим часом, автор визначає мініатюризацію комп'ютерів та суцільну цифровізацію, імплантовувані технології, технології цифрової присутності, гаджети з інтерактивним інтерфейсом, «цифровий зір» , натільний портативний інтернет, інтернет речей і для речей, під'єднані будинки, «розумні» міста, безпілотні автомобілі, штучний інтелект, робототехніка, адитивне виробництво, біткойни та блокчейн, генна інженерія, нейротехнології тощо. Перелічені технології мають суттєвий потенціал соціального, економічного і політичного розвитку, відкривають можливості для впровадження нових економічних моделей, більш високих стандартів у сфері соціального забезпечення, надання послуг, у тому числі, медичних та освітніх, нових підходів до розробки і реалізації політичних стратегій, ухвалення рішень тощо (Шваб, 2019).

Проте дедалі більше у експертів викликає занепокоєння використання окреслених технологічних новацій з протиправною, злочинною чи терористичною метою, адже майже всі вони є подвійного призначення і можуть бути застосовані, наприклад, для підвищення боєздатності армії та удосконалення озброєнь держав-аутсайдерів чи держав-«невдах» , що підтримують або фінансують, наприклад, терористичні угруповання, для скоєння масштабних терористичних атак терористичними організаціями або «окремо діючими особами» , що може призвести до руйнування міжнародної системи миру і безпеки. Більш того, новітні науково-технологічні досягнення активно використовуються у процесі модернізації засобів протиборства, стаючи основою для реалізації програм « Революції у військовій

сфері». Це суттєво впливає на характер війн і конфліктів, а також на стратегії протиборства у сучасних міжнародних відносинах.

Так, імплантовувані технології та технології «цифрового зору» можуть стати причиною зростання недовіри до системи електронної ідентифікації внаслідок потенційної небезпеки порушення конфіденційності приватного життя, витоку персональної інформації, логічних помилок в ідентифікації особистості чи втручання у приватне життя громадян (Шваб, 2019, Arthur, 2013). У той же час, імерсивні технології дозволяють легко створювати гнучкі можливості штучного відтворення ситуації військового протистояння чи випробовування бойової техніки для підготовки військових до різних ситуацій у майбутніх реальних військових кампаніях. Гаджети, оснащені технологіями віртуальної або доповненої реальності надають солдатам інформацію про карти, маркери руху та інші дані, що значно покращує прийняття ситуаційних рішень у режимі реального часу для наземних сил (Top 10 Military Technology Trends & Innovations for 2022, 2022).

Розвиток технологій адитивного виробництва також має неоднозначні наслідки і містить чимало викликів для системи безпеки. Наприклад, поява можливості створювати за допомогою 3D-принтерів зброї поставила на порядок денний проблему ефективності її ідентифікації та використання. Викликає також занепокоєння факт застосування даних технологій у сфері виробництва хімічної, біологічної та ядерної зброї. Так, за допомогою 3D-друку нині створюються деталі паливних систем ядерних реакторів, а також ракет та боєголовок. У поєднанні з розвитком штучного інтелекту або нанотехнологій адитивні технології можуть стати більш потужними і небезпечними (Fernandez, 2013). Як зазначається у доповіді «Можливості зброї масового ураження, підсиленої адитивним виробництвом», увесь потенціал адитивного виробництва, особливо пов’язаний з можливістю поєднання різних матеріалів (традиційних та новітніх), генеративним дизайном та багатошаровою електронікою, ще неможливо осягнути повністю. Але вже сьогодні стає зрозумілим той факт, що потенціал використання таких інновацій може перетворитися на своєрідного «чорного лебедя» , якщо стане складовою військової стратегії держави, спрямованої на набуття нових нетрадиційних / асиметричних

військових переваг. При цьому, застосування таких засобів протиборства не може бути вчасно ідентифіковано, що робить систему безпеки вкрай вразливою до такого типу загроз, а протидія їх використанню ще не набула правового оформлення (Daase, Christopher, Dalnoki-Veress, Pomper, Shaw, 2019).

Використання Big Data та аналітики дозволяє збройним силам отримувати необхідні дані, точно й швидко аналізувати їх, а потім оперативно поширювати інформацію, що надає значної стратегічної переваги у сучасному протиборстві. Для цього аналітика великих даних збирає статистичні дані з різних джерел, а квантові обчислення знаходять застосування в криптоаналізі та запуску симуляцій для прийняття обґрунтованих рішень. Аналітика також забезпечує ефективну інтерпретацію даних, зібраних з інфраструктури Інтернету військових речей. Крім того, прогнозна аналітика запобігає загрозам і підвищує ефективність досягнення небезпечних завдань. Наприклад, австралійський стартап Q-CTRL, який пропонує хмарне програмне забезпечення для максимальної продуктивності квантових комп'ютерів, використовує квантові обчислення для різних оборонних програм. Рішення стартапу дозволяє проводити криптографічний аналіз і сенсорне виявлення підземних міцних структур і прихованих систем зброї. Крім того, це полегшує квантово розширену навігацію на полях битв, де GPS заборонено, за допомогою атомних акселерометрів (Top 10 Military Technology Trends & Innovations for 2022, 2022). Технологія блокчейн забезпечує безпеку даних під час обміну ними з усіма зацікавленими сторонами. Саме тому в оборонній сфері реалізуються рішення на основі блокчейну для захисту конфіденційних військових даних і протидії кіберзагрозам. Інші застосування технології блокчейн в галузі включають відстеження пристроїв, оптимізацію процесу закупівель і безпеку ланцюжка поставок. Розумні контракти значно знижують ризик шахрайства або корупції під час роботи з оборонними підрядниками (Top 10 Military Technology Trends & Innovations for 2022, 2022).

Безпілотні літальні апарати використовуються нині не тільки для розвідувальних цілей, встановлення зв'язку або передачі медикаментів, але й для ідентифікації цілей ураження, доставки боєприпасів або нанесення ударів (Drones:

What are they and how do they work, 2012). Використання технології штучного інтелекту дає можливість модернізувати засоби протиборства, у тому числі, й безпілотні літальні апарати, які не тільки отримують більш досконалу систему управління, але й можливість діяти як система завдання удару за допомогою тактики бойового «рою» , що суттєво підвищує їх бойову ефективність та покращує показники витривалості. Зазначимо, що штучний інтелект використовується й для створення « розумних матеріалів» , здатних змінювати свої властивості, що дозволяє досягати ще більших успіхів у зменшенні помітності зразків військової і спеціальної техніки та підвищує ефективність здійснення розвідки, наприклад, з використанням технологій Stealth (Top 10 Military Technology Trends & Innovations for 2022, 2022). Нині актуальними є також дослідження у сфері квантової криптографії, що не тільки підвищує рівень інформаційної безпеки, але й створює нові проблеми, пов’язані із збором розвідувальних даних (Chen, 2017).

Досягнення у сфері робототехніки дозволяють суттєво підсилити ударну міць військових підрозділів, наприклад, за рахунок підвищення обізнаності про ситуацію, зменшення фізичного та когнітивного навантаження на солдатів, а також полегшення пересування у складних місцевостях. Робототехніка та автономні системи стають дедалі більш важливими для забезпечення свободи маневру та виконання місії з найменшим ризиком для військових. Використання дронів також покращує обізнаність про ситуацію на полі бою, а мультифункціональні роботи сприяють розмінуванню, пошуково-рятувальним операціям, знешкодженню вибухонебезпечних предметів і матеріально-технічній підтримці (Top 10 Military Technology Trends & Innovations for 2022, 2022). Використання робототехніки та автономних систем призвело до бурхливої дискусії серед науковців щодо віднесення роботів до категорії гуманної зброї. Але провідні армії світу вже мають на озброєнні різноманітні системи, що передбачають використання роботів з можливістю управління в автономному режимі (наприклад роботи-турелі на рухомій платформі) для ведення пошуку або навіть знищення цілей. Як зазначається у Директиві міністерства оборони США «Autonomy in Weapon Systems», автономні системи озброєння – це система зброї, яка після активації може обирати і вражати цілі без

подальшого втручання оператора-людини» (Department of Defense, 2012). Небезпека полягає й у тому, що на відміну від інших засобів масового ураження, використання автономних військових систем не набуло остаточного правового оформлення. Це, у свою чергу, може призвести до неконтрольованого їх використання як державами, так й терористичними угрупованнями, та, відповідно, до порушення балансу світової геополітики. Зазначимо, що вироблення таких систем стає більш простим і дешевим за рахунок поширення технологій 3D-друку, а визначити джерело загрози – майже неможливо. Наприклад, в рамках сучасного конфлікту у Сирії відбулася атака дронів на російсько-сирійську базу, джерело якої так й не було офіційно встановлено (Dreifus and Walsh, 2019).

Обговорення проблеми вироблення правових норм, що могли б врегулювати використання досягнень робототехніки, удосконаленої штучним інтелектом, нині є надзвичайно актуальним, оскільки відтермінування вирішення цієї проблеми може суттєво порушити баланс сил. В рамках ООН ініціативу не підтримують такі країни, як США, Велика Британія, Російська Федерація, Ізраїль і Південна Корея, а Китай висловлює готовність підтримати заборону використання у військових цілях, але проти заборони ведення наукових розробок у цій сфері. Основними аргументами противників ухвалення обмежувальних норм є переконання у етичності та гуманності робототехніки, оснащеної штучним інтелектом, яку можна запрограмувати на дотримання норм міжнародного гуманітарного права (Dreifus and Walsh, 2019). Тим більше, що є й очевидні переваги використання робототехніки, зокрема, для ведення розмінування або підтримки дій збройних сил під час хімічної атаки.

Суцільна цифровізація робить вкрай вразливою інформаційну інфраструктуру, особливо в умовах підключення до неї об’єктів енергетики, управління транспортом чи медичного обслуговування, що може призвести не тільки до технічних чи програмних збоїв, але й реальних людських жертв. Проблема буде поглиблюватися із зростанням кількості осіб, які використовують різноманітні пристрої Інтернету речей у повсякденному житті, що актуалізує питання кібербезпеки та стійкості мереж до різноманітних атак.

Так, нині у світі набуває актуальності проблема безпеки даних та послуг в умовах поширення технологій 5G, що стануть основою для взаємодії мільярдів пристроїв Інтернету речей (European Commission, 2020). Застосування ж Інтернету речей у сфері безпеки та оборони передбачає об'єднання кораблів, літаків, танків, безпілотних літальних апаратів, солдатів і операційних баз у єдину мережу, що значно покращує сприйняття, розуміння ситуації, ситуаційну обізнаність і суттєво зменшує час реакції на події. Периферійні обчислення, штучний інтелект і 5G підтримують постійний потік даних у всіх військових підрозділах, що зміцнює структуру командування й контролю. У Інтернет військових речей датчики та обчислювальні пристрої, які носять солдати або які вбудовані в їхнє обладнання, збирають різноманітні статичні та динамічні біометричні дані (Top 10 Military Technology Trends & Innovations for 2022, 2022).

Занепокоєння викликає й той факт, що в умовах відсутності ефективної системи управління науково-технологічним розвитком, постійне зростання темпів проникнення технологій у всі сфери життєдіяльності суспільства може призвести до кінетичних наслідків кібератак, оскільки проникнення технологій у фізичний світ утворює так звані кіберфізичні системи (World Economic Forum, 2020). Проблема ускладнюється й тим, що досягнення у сфері ІКТ можуть легко потрапити до рук терористів, злочинців або так званих «окремо діючих осіб» . Доступність сучасних досягнень і розробок у сфері науки і технологій, поява нових форм фінансування такого типу протиправної діяльності (наприклад, використання благодійних організацій або фейкових компаній, краудсорсингу, онлайн-платежів та криптовалют), активне використання можливості даркнету для отримання доступу до надсучасних озброєнь призводить до збільшення вразливості системи безпеки, що, у свою чергу, обумовлює виникнення потреби переглядати існуючі механізми протидії новим викликам і загрозам як на національному, так й на глобальному рівнях (RAND Corporation, 2017; European Commission, 2020).

Пришвидшення процесів цифровізації світу та поширення високих технологій суттєво вплинули на трансформація сучасної парадигми безпеки. Найбільш показовим в цьому плані є переміщення геополітичного протистояння акторів

міжнародних відносин у кіберпростір. В цих умовах посилення геополітичної напруженості, ускладнене проблемами соціально-економічного, ресурсно-екологічного та суто військового характеру, неефективності механізмів міжнародно-правового регулювання розробки і використання сучасних наукових і технологічних досягнень, може призвести до подальшого поглиблення конфронтації між різними акторами міжнародних відносин, але вже у новому форматі. Подвійний характер використання досягнень науково-технологічного прогресу неоднозначно впливає на геополітичне суперництво, перетворюючи ІКТ і наукові досягнення на надпотужну зброю, яка може загрожувати існуванню людства. Отже, мережі 5G-зв'язку, квантові технології та штучний інтелект виступають як масштабний виклик для системи безпеки, оскільки можуть бути використані для нарощування власне військового потенціалу або удосконалення методів ведення війни (World Economic Forum, 2020).

Слід зазначити, що використання кіберпростору у військових цілях розпочалося ще у 1999 р., коли під час операції у Югославії постало питання ефективності «електронної ізоляції» С. Мілошевича, що потенційно могло б зменшити кількість людських жертв і матеріальні втрати від застосування традиційних видів озброєнь. З одного боку, на думку верховного головнокомандувача сила НАТО у Європі У. Кларка, хакерські операції були здатні зупинити фінансування режиму Мілошевича, його оточення і всіх прибічників, що значно прискорило б перемогу союзницьких сил. З другого, виникла проблема, пов'язана із міжнародно-правовим тлумаченням поняття « інформаційна операція» як форми протиборства і можливістю застосування норм традиційного права війни у таких випадках (Borger, 1999). Про це йшлося у спеціально підготовленому дослідженні НАТО «Оцінка міжнародно-правових питань щодо інформаційних операцій». Таким чином, поширення комп'ютерних вірусів, логічних бомб, націлених на цивільні об'єкти, наприклад, банки або університети, дезінформація щодо дій керівництва держави, діяльності збройних підрозділів або миротворчого процесу, можуть бути розцінені як військовий злочин (Department of Defense, 1999). Найбільш небезпечними вважаються випадки, коли удар завдається по елементам критичної інформаційної інфраструктури країни, що може призвести до реальних

фізичних втрат, зокрема, серед мирного населення (наприклад, внаслідок атаки на систему енергопостачання, системи атомної енергетики або управління водопостачанням, дамбами і шлюзами тощо). (Department of Defense, 1999). Але тільки у 2009-2010 рр. світ уперше усвідомив реальність виникнення не потенційної, а справжньої небезпеки загроз у кіберпросторі, що спонукало значну кількість країн (як інформаційно розвинених, так й інформаційно бідних) розпочати стратегії нарощування кіберпотенціалу для оборонних та наступальних цілей.

У 2009 р. стало відомо про появу та стрімке поширення нового вірусу Stuxnet, який вразив комп'ютерні системи заводу із збагачення урану в Натанзі, а також призвів до подальшого гальмування програми запуску ядерної АЕС в Бушері у 2010 р. Вірус вразив систему диспетчерського управління і збору даних (SCADA) компанії Siemens, яка широко використовується на різноманітних промислових об'єктах, а також для управління транспортними системами, системами енергопостачання, водо-, газо-, нафтопроводами тощо в різних країнах світу (Hein, 2010). Саме після цього інциденту світова спільнота усвідомила, наскільки можуть бути небезпечними цілеспрямовані кібератаки. На думку експертів, відтепер міжнародні терористичні угруповання та диктаторські режими будуть прагнути якомога швидше отримати подібні електронні засоби, використання яких не потребує спеціальних знань та власних ноу-хау. Такі розробки стануть доступними для купівлі-продажів, що призведе до появи ринку, на якому кібератаку можна буде просто оплатити. Об'єктами ж таких атак стануть критично важливі елементи інфраструктури суспільства (Hein, 2011).

Таким чином, загрози виникають не тільки для військової, а й для цивільної сфери, що суттєво ускладнює процес забезпечення національної інформаційної безпеки. Наслідком появи таких типів загроз стали дії багатьох держав, спрямовані на розробку і реалізацію національних військових доктрин у сфері кібербезпеки, національних кіберстратегій та створення відповідних військових підрозділ, що відповідають за ведення військових дій у кіберпросторі. Таким чином, кіберпростір розглядається як простір, в якому розгортаються як наступальні, так й оборонні військові дії, що сприяє подальшій його мілітаризації, і, як наслідок, – новій гонці

озброєнь (Gomez, 2016). За даними UNIDIR, вже у 2013 р. серед досліджуваних 114 держав, що мають доктрину і стратегію кібербезпеки, 47 розробляли і реалізовували саме військові програми, але решта 67 – виключно цивільні (UNIDIR, 2013). Це свідчить про усвідомлення державами небезпеки мілітаризації кіберпростору та їх прагнення максимально убезпечити свій інформаційний простір від кібервикликів та кіберзагроз, особливо в умовах пришвидшення процесів цифровізації суспільств та постійного зростання кількості інтернет-користувачів.

Прикладом подальшої мілітаризації кіберпростору можуть слугувати події вересня 2019 р., коли дронами були атаковані два критично-важливих об'єкта в Саудівській Аравії, у тому числі найбільший у світі нафтопереробний завод. Внаслідок атаки добича нафти скоротилася приблизно на 5,7 млн. барелей на добу, що становить близько 50 % від загального обсягу добичі нафти у країні. І хоча відповідальність за інцидент взяли на себе йєменські повстанці-хусити, держсекретар США Майк Помпео заявив про пряму причетність Ірану до нападів (Talmazan, 2019). В свою чергу, Іран спростував звинувачення на свою адресу. Невизначеність ситуації, на думку експертів, обумовлена тим, що період, коли бойовими дронами володіли лише декілька найбільш технологічно розвинених держав, минув. Відтепер безпілотники стають більш доступними як для держав (США, КНР, Ізраїлю, Ірану), так й для різноманітних організації по типу «Хамас» або «Хезболи» (Marcus, 2019). Відповіддю на ситуацію, що склалася, стали дії адміністрації Д. Трампа, що мали на меті «покарати» Іран, але при цьому не допустити перехід конфлікту у «гарячу» фазу. В цій ситуації саме кібератаки проти іранських цілей розглядалися як найбільш ефективний засіб, оскільки вважався потенційно безкровною демонстрацією могутності США. Водночас експерти у сфері кібербезпеки висловили занепокоєння з приводу негативних наслідків такої політики для системи національної безпеки і оборони США, оскільки ставка на цифрову зброю може призвести до пришвидшення процесу мілітаризації кіберпростору та збільшення кількості і масштабів кібератак у відповідь, а відтак призвести до зниження «порогу» використання кіберзброї (Groll and Seligman, 2019).

Але більш показовою у цьому контексті є відповідь Ізраїлю бомбардуванням на кібератаки терористичної організації ХАМАС у травні 2019 р. Зазначимо, що це був перший випадок, коли держава відреагувала на дії хакерів застосуванням фізичної сили під час конфлікту в режимі реального часу. Після ідентифікації хакерської атаки проти Ізраїлю відбувся авіаудар по будівлі у секторі Гази, в якій за офіційними даними розміщувалися сили кібероперацій ХАМАСу. Як заявили ізраїльські військові, внаслідок удару ХАМАС був позбавлений кіберможливості здійснювати операції (Borghard and Schneider, 2019).

Зазначимо, що у 2015 р. США атакували бойовика ІДІЛ, який виклав у мережу персональні дані американських військових, але це відбулося не в режимі реального часу, як в Ізраїлі. Водночас самий факт можливості фізичної відповіді на кібератаку став причиною продовження дискусій, що розпочалися ще у 2009-2010 рр., коли провідні держави світу заявили про потребу врегулювання питань кібербезпеки шляхом визнання кібератак «актом війни» . Таку позицію зайняли представники США, які відзначали масштабність наслідків для національної системи безпеки і оборони кібератак з боку країн-супротивників. Так, під час Світового економічного форуму у Давосі у 2010 р. С. Колінз, сенатор від Республіканської партії США, заявила, що Америка схильна розглядати випадки кібератак як оголошення війни. Цю позицію згодом підтвердив Дж. Мілер, представник міністерства оборони США, який заявив, що США готові нанести військовий удар у відповідь на кібератаки на свій кіберпростір. У цьому ж році в рамках НАТО групою експертів на чолі з М. Олбрайт було запропоновано розглядати масштабні кібератаки на рівні із загрозами, що підпадають під дію статті 5 Північноатлантичного договору (НІСД, 2010). Водночас, одностайної підтримки на міжнародній арені така позиція не отримала, оскільки мала суттєвий потенціал для ескалації військового протистояння у світі.

Отже, ситуація з авіаударом у відповідь на кібератаки на Ізраїль у 2019 р. свідчить про суттєві зміни підходів до боротьби з кібератаками під час міжнародних конфліктів. Згідно із загальними принципами ведення війни та нормами міжнародного гуманітарного права, удар у відповідь має бути пропорційним.

Оскільки ізраїльські військові визнали факт завершення кібератаки до початку авіаудару, таку реакцію деякі експерти розцінили як надмірну і таку, що може призвести до подальшої ескалації конфлікту, а отже, до збільшення жертв та насильства. Саме тому за часів адміністрації Б. Обами США переважно утримувалися від використання засобів кібервійни і намагалися розробити та впровадити стратегії, спрямовані на стримування кібератак, звертаючи особливу увагу на розробку правових норм у сфері кібербезпеки. Аргументом слугували чисельні дослідження, що свідчили про низьку вірогідність переростання кібервійни у фізичну агресію, оскільки провідні світові держави усвідомлюють небезпеку, що може призвести не тільки до поглиблення кризи, але й до пришвидшення процесів мілітаризації кіберпростору. Тому відповідь на кібератаки переважно відбувається за принципом « око за око» і передбачає або симетричні дій у відповідь, або використання засобів міжнародно-правового, дипломатичного чи економічного тиску. Наприклад, у відповідь на кібератаку Stuxnet Іран розпочав кібератаки на фінансову систему США, а після кібератаки на компанію Sony Pictures США вдалися до розширення санкцій проти Північної Кореї. За часів адміністрації Д. Трампа США зайняли більш активну позицію з цього питання, вважаючи, що протистояти супротивникам краще превентивно і в їх власному кіберсередовищі, для недопущення виникнення загроз для системи національної безпеки Америки (Borghard and Schneider, 2019). Отже, можна вважати, що події в Ізраїлі призвели до створення прецеденту термінової військової відповіді на кібератаки, що має стати певним застереженням для країн (наприклад, Ірану), що нарощують свій наступальний кіберпотенціал і можуть його використати в умовах вже існуючого військово-політичного протистояння (Doffman, 2019).

Варто зазначити, що незважаючи на наявність розбіжностей в оцінці феномену мілітаризації кіберпростору, більшість експертів вважає, що рівень та темпи мілітаризації кіберпростору держави залежать від кількості кібернападів або наступальних операцій у кіберпросторі проти неї. Важливим фактором також є ефективність реалізації національних стратегій інформатизації, оскільки масштаби використання кіберпростору формують залежність від гарантій його безпеки. Отже,

чим вищим є рівень інформатизації держави, тим більше вона схильна до мілітаризації кіберпростору задля забезпечення національної інформаційної безпеки. В останні роки темпи мілітаризації кіберпростору суттєво зросли. Значна кількість країн в усьому світі вживають заходи для вдосконалення стратегічного планування кібербезпеки, розширення систем військових кіберорганізацій і зміцнення можливостей наступальних кібероперацій.

Таким чином, подвійний характер використання сучасних наукових і технологічних досягнень обумовив появу нового типу викликів і загроз як для глобальної системи підтримання миру і стабільності, так й для системи національної безпеки усіх держав світу (Сябро, 2018). Окрім загальновизнаного позитивного ефекту для реалізації проєктів модернізації суспільства на основі появи нових моделей економічної діяльності, розв'язання проблем соціально-економічного характеру, трансформації політичної діяльності та гуманітарного розвитку, окреслені інновації містять колосальний руйнівний потенціал, здатний зруйнувати систему глобальної безпеки і поставити світ перед небезпекою нового типу війн і конфліктів, запобігти яким неможливо діючими міжнародними політичними та правовими механізмами. Така ситуація суттєвим чином вплинула на трансформацію сучасної парадигми безпеки, яка відтепер має враховувати фактори інформаційного і науково-технологічного розвитку як такі, що можуть докорінним чином вплинути на саму систему безпеки або окремих її акторів. Саме тому, починаючи з 1990-х рр. питання впливу досягнень у сфері науки і технологій на міжнародну безпеку активно обговорюються представниками різних країн світу в рамках ООН, що відображено у чисельних резолюціях Генеральної Асамблеї, ухвалених на підставі оприлюднених позиції держав та аналітичних доповідях Комітету ГА ООН з питань роззброєння і міжнародної безпеки.

1.2 Теоретичні і концептуальні підходи до проблеми інформаційної безпеки у зарубіжній та вітчизняній політологічній думці

Зміна парадигми безпеки в умовах побудови глобального інформаційного суспільства призвела до появи нових теоретико-методологічних засад дослідження проблеми інформаційної безпеки, які в сучасних концептуальних та прикладних розробках представлені цілою низкою нових підходів до проблеми сучасного міжнародного політичного середовища та інформаційної геополітики, визначення потужності держав та її лідерських позицій на світовій арені, трансформації понять «національний суверенітет», «національні кордони», «права на застосування сили», «балансу сил» тощо. Визначення базових теоретичних підходів до проблеми інформаційної безпеки уможливлює всебічний аналіз сучасної практики розбудови ефективної системи інформаційної безпеки на глобальному, регіональному та національному рівнях.

Дослідженню процесу трансформації міжнародної політичної системи в умовах пришвидшення інформаційного і науково-технологічного розвитку присвячені роботи К. Демчака та П. Домбровські. Як зазначають дослідники у роботі «Розквіт кібервестфальської доби» , внаслідок бурхливої інформатизації та впровадження досягнень науково-технологічного прогресу відбувається віртуалізація міжнародного політичного простору, що представлено у концепціях « кібервестфалю» , «Вестфаль 2.0» або «постстакснет епохи» . Автори розглядають ці процеси крізь призму інформаційного протиборства як нового виміру геополітичного протистояння. Отже, на думку дослідників, актори міжнародних відносин відтепер змушені переглядати стратегії діяльності, оскільки зазнають суттєвих змін традиційні поняття «територія», «державні кордони», «державний суверенітет» , «національні інтереси» , «потужність держави» , «сила» і «баланс сил» тощо. Як наслідок – держави стикаються з цілою низкою викликів, зокрема, встановлення кордонів у кіберсередовищі, захист інформаційного суверенітету та нарощування кібермогутності. Тобто у цьому новому середовище відбувається

процес встановлення нової системи за принципом Вестфальської (Demchak, Dombrowski, 2011).

В іншій праці – «Кібервестфалія утверджує переваги держави у кіберпросторі», автори роблять висновок, що нині відбувається перехід до формування кібернетичної міждержавної системи. Таким чином держави намагаються відтворити у кіберпросторі вестфальський процес, що передбачатиме визначення нового типу національних кордонів та вироблення механізмів захисту державного суверенітету в інформаційному просторі (Demchak, Dombrowski, 2014). Але адаптація вестфальської моделі до реалій кіберпростору буде складною і суперечливою, оскільки нова, кібервестфальська система не зможе повністю відтворити попередню. Наприклад, держави, готові до нових реалій існування, зможуть забезпечити реалізацію гарантій територіальної цілісності у кіберпросторі, встановити віртуальні державні кордони, виробити нові принципи взаємодії на основі взаємного визнання та невтручання у внутрішні справи. Неспроможні ж держави у глибоко кіберізольованому світі опиняться у ситуації, коли не зможуть захищати національні кордони, контролювати власний громадський порядок на своїй території, підтримувати життєздатність державних інститутів або послуги, що ними надаються, і стануть вразливими перед неконституційними внутрішніми проблемами – від падіння загального рівня економічного розвитку та соціального добробуту до ескалації конфліктів.

К. Демчак у роботі «Три сценарії майбутнього для постзахідного кібернетичного світу» (Demchak, 2018), на основі аналізу вразливості до інформаційних загроз західних демократичних держав та зростання кіберпотужності незахідних авторитарних держав, пропонує сценарії розвитку міжнародної системи безпеки в умовах подальшого розгортання кіберконфліктів між цими двома групами країн: сценарій «Кібер-статус-кво», що передбачає продовження хаотичного зіткнення сучасних держав з одночасним послабленням політико-ідеологічного впливу та фінансових можливостей демократичних держав; «Кібервестфальська система» – система, в якій кожна держава змушена захищатися самостійно і є вразливою перед загрозою опинитися під кіберконтролем з боку кібергегемону; та

«Альянс кібероперативної стійкості» – колективна інтегрована відповідь всіх націй в рамках союзних демократичних громадянських суспільств. Два перших сценарії К. Демчак вважає негативними для розвитку міжнародної системи, оскільки передбачають подальше ослаблення кібермогутності демократичних держав та їх неспроможність чинити опір цифровому підпорядкуванню потужній авторитарній державі-кіберекономічному гегемону, наприклад, КНР. Третій сценарій передбачає створення та функціонування системи спільної кібернетичної безпеки та оборони. Він є позитивним і потребує термінових зусиль, поки нова міжнародна система миру і безпеки ще формується (Demchak, 2018).

Важливим напрямом наукових дискусій є трансформація підходів до використання сили міжнародними акторами. Поняття сили завжди було у центрі уваги теорії міжнародної безпеки, але саме із інформаційним та науково-технологічним розвитком вона набуває нового значення. В сучасних умовах жорсткі механізми здобуття та утримання влади почали поступатися новим, більш гнучким інструментам, які відповідають новим реаліям розвитку міжнародних відносин. Про це йдеться у чисельних працях Дж.Ная (Nye, 1990; Nye, 2002; Nye, 2004; Nye, 2008; Nye, 2011), в яких автор розвиває теорію «м'якої сили», визначає її базові характеристики та відмінності від «жорсткої сили». Так, на думку автора, «м'яку силу» слід тлумачити як здатність формувати привабливий образ того, хто володіє інструментами сили (Soft Power). Основними елементами «м'якої сили» є зовнішня політика і дипломатія, політична ідеологія, культура і цінності, а «жорсткої» – економічні та військові можливості. Таким чином за допомогою несилових методів можна впливати на процес ухвалення рішення у сфері міжнародних відносин, досягаючи поставленої мети (Nye, 2004). Як зазначає автор, держава може досягнути бажаних результатів у світовій політиці, оскільки інші країни хочуть наслідувати її у всьому, прагнучі досягнути такого ж рівня процвітання та відкритості. Саме цей аспект влади, що змушує інші держави бажати того ж, що бажає держава-ініціатор застосування таких засобів, і називається «м'яка сила» (Nye, 2002).

У спільній праці Дж. Ная та У. Оуенса «America's Information Edge» (Nye and Owens, 1996) «м'яка сила» розглядається в контексті інформаційної переваги США у використанні найважливіших засобів зв'язку та інформаційних технологій, зокрема, технологій супутникового спостереження, прямого мовлення, високошвидкісних комп'ютерів, а також у можливостях інтегрування складних інформаційних систем. Така інформаційна перевага допомагає стримувати або нейтралізувати традиційні військові загрози при порівняно незначних витратах. Як зазначають автори, у світі, де змінився сенс понять «стримування», «ядерна парасоля» та «неядерного залякування», наявність інформаційної переваги здатна не тільки зміцнити інтелектуальний зв'язок між зовнішньої політикою США та їх воєнною могутністю, але й призвести до виникнення нових способів збереження лідерства в альянсах та тимчасових коаліціях. Дж. Най та У. Оуенс також аналізують появу феномену «інформаційної парасолі» (Nye and Owens, 1996), який передбачає зростання залежності держав від оперативності отримання достовірної інформація задля ухвалення збалансованого рішення щодо її дії на міжнародній арені або в умовах конфронтації з іншими акторами міжнародних відносин. Отже, лідерство держав у найближчому майбутньому буде дедалі більше узалежнюватися не від воєнних можливостей знищити сили супротивника, а від оперативного пояснення неоднозначних ситуацій, пов'язаних з насильством, гнучкого реагування і за потреби застосування силу – точно і акуратно (Nye and Owens, 1996). На роль держави-лідера, на думку авторів, можуть претендувати лише США, які мають високий рівень інформаційного і технологічного розвитку, що дає можливість збирати усю необхідну інформацію про міжнародні події і ефективно її використовувати для досягнення переваги у геополітичному протистояння. Держави-союзники отримують можливість доступу до стратегічно важливої інформації, завдяки чому вони стають здатними досягнути такої ж воєнної переваги, що й Америка. Таким чином, відбувається формування «інформаційної парасолі», що, подібно до розширеного ядерного стримування, може стати фундаментом для взаємовигідних відносин (Nye and Owens, 1996).

У розвиток теорії «м'якої сили» Дж. Най та Р. Армітідж у 2007 р. запропонували концепт «розумної сили» , що передбачає ситуативне поєднання «м'якої» і «жорсткої» сили для підвищення ефективності реалізації стратегій у міжнародних відносинах. Так, в аналітичному дослідженні «Більш розумна, більш безпечна Америка», зокрема, зазначається, що США повинні стати більш «розумною державою», інвестуючи у глобальне благо та допомагаючи досягнути цілей, які інші держави не можуть досягнути самостійно. Саме додаючи до військової та економічної могутності збільшення інвестиції у «м'яку силу», Америка може створити міцний фундамент для вирішення складних глобальних проблем. Зокрема, слід зосередитися на п'ятьох важливих сферах: союзи, партнерство та міжнародні інститути; узгодження національних інтересів з тенденціями глобального розвитку; розширення можливостей використання публічної дипломатії, економічна інтеграція, що передбачає більш тісну взаємодію з глобальною економікою, розвиток та інвестиції у технології та інновації (Armitage and Nye, 2007). «Розумна сила», на думку авторів, передбачає розробку інтегрованої стратегії, ресурсної бази та набору інструментів для досягнення цілей держави, спираючись як на «жорстку», так і на м'яку» силу. Такий підхід не виключає наявності потужних збройних сил і передбачає, що держава, зокрема, Америка, може одночасно використовувати союзи, партнерство та міжнародні інституції на всіх рівнях для розширення американського впливу та встановлення легітимності американських дій (Armitage and Nye, 2007). В іншій роботі – «Майбутнє сили», Дж. Най зазначає, що наявність ресурсів сили не гарантує досягнення бажаного результату у взаємовідносинах з іншими акторами. Тому часто невеликі держави, за умови правильного розрахунку, можуть використовувати обмежений ресурс сили для досягнення значних переваги у міжнародних відносинах (Nye, 2011).

У розвиток теорії «м'якої» і «розумної» сили було також запропоновано теорію «гострої» сили, яка пов'язана із зовнішньополітичною діяльність авторитарних режимів і передбачає використання прийомів маніпулювання громадською думкою в демократичних країнах з метою підриву їх політичної системи (Сябро, 2021а). Так, Дж. Най у роботі «Майбутнє сили» зазначає, що

«гостра сила», на відміну від «м'якої», допомагає авторитарним режимам контролювати поведінку всередині держави і маніпулювати громадською думкою за її межами. Отже, завдяки «гострій силі» відбувається зменшення привабливості демократії (Nye, 2011).

Іншим напрямом наукових дискусій щодо інформаційної безпеки як на глобальному, так й на національному рівнях виступає проблема інформаційного потенціалу та кібермогутності. Як зазначають автори (Дж. Най, С. Старр, Г. Реттрей, А. Клімбург, Д. Шелдон та ін.), в умовах формування нової системи міжнародних відносин відбувається переосмислення поняття могутності та потенціалу, що дає можливість забезпечувати стратегічні переваги держави у геополітичному протиборстві. Так, С. Старр (Starr, 2017), спираючись на підходи, представлені у «Національній військовій стратегії операцій у кіберпросторі», визначає «кібермогутність» як здатність використовувати кіберпростір для створення переваг і впливу на події в інших операційних середовищах за допомогою інструментів влади. В цьому контексті інструменти влади включають елементи парадигми традиційних важелів влади – політичних/дипломатичних, інформаційних, військових та економічних, але основний наголос робиться на військовому та інформаційному важелях (Starr, 2017). Автор також приділяючи особливу увагу питанням трансформації принципів ведення війни, теорії сили та ризику, а також підходам до організації та проведення воєнних операцій на прикладі мережноцентрованих війн (Starr, 2017).

Г. Реттрей, досліджуючи феномен кібермогутності, визначає особливості різних вимірів протистояння – наземного, військово-морського, повітряного, космічного та кіберпростору. Так, на думку автора, усі визначені простори мають низку спільних рис – використання технологічних досягнень, швидкість і масштаб операцій, контроль ключових ознак і загальнонаціональна мобілізація. Але у кіберпросторі ці характеристики набувають нового значення. При цьому, використання технологічних досягнень та збільшення залежності від кіберпростору призводять до появи нових стратегічних вразливостей, що може мати масштабні негативні наслідки, наприклад, призвести до так званого «цифрового Перл-

Харбора». Внаслідок здешевлення технологій та їх доступності для недержавних акторів (окремо діючих осіб, терористичних угруповань та транскордонної злочинності) кіберпростір стає ще більш вразливим і непередбачуваним. До того ж, розвиток кіберпростору підвищив швидкість різноманітних глобальних операцій та посприяв покращенню здатності автоматизувати управління і контроль, що суттєво скоротило класичний цикл спостереження-орієнтація-прийняття рішень-дії» . Як зазначає автор, важливим фактором переваги є контроль над ключовими чинниками, що уможливлює панування актора у конкретному вимірі протистояння. Наприклад, у морському вимірі протистояння перевагою є контроль над критично-важливими елементами транспортної інфраструктури, зокрема, морськими протоками; у космічному – системи управління об'єктами на геостаціонарній орбіті. Але у кіберпросторі такі переваги є штучними і мінливими (наприклад, так звані «серверні ферми» – групи серверів, що поєднані між собою в єдину мережу передачі даних і працюють як єдина система). Щодо питання національної мобілізації, для демонстрації кібермогутності держави у разі потреби формується штат професійних кадрів у сфері кібербезпеки за рахунок спеціалістів як у цивільній, так й військовій сферах. Таким чином утворюється резерв інтелектуального капіталу, який можна використовувати у разі виникнення проблеми у кіберпросторі (Rattray, 2017).

О. Клімбург, характеризуючи феномен кібермогутності у контексті національної кібербезпеки, підкреслює, що кіберпростір безпосередньо впливає на всі аспекти людського існування – економічний, соціальний, культурний, політичний, що призводить до зростання кількості кіберзагроз для різних сфер життєдіяльності сучасного суспільства. Таким чином, дедалі більшої актуальності набуває питання національної кібербезпеки, оскільки саме від здатності держави ефективно відповідати на виклики у кіберпросторі, залежить успіх у реалізації стратегій соціально-економічного та політичного розвитку. Автор також зазначає, що поняття кібермогутності включає як традиційні чинники, що формують сукупну міць держави на світовій арені, так й ті, що не входять до кола власне безпекових – економічні або культурні, що, у свою чергу, може призвести до секьюризації низки сфер, які не вважалися частиною національної безпеки (Klimburg, 2013).

Слід підкреслити, що на думку О. Клімберга поняття « кібермогутність» поступово витісняє поняття «кібервійна», оскільки в сучасних умовах не всі держави здатні реалізовувати доктринальні концепції міждержавного конфлікту, які діють як у мирний, так й у військовий час. Наприклад, КНР нині реалізує концепцію інформаційної війни під назвою «Три війни» («Правова війна», «Медіа-війна» та «Інформаційна війна» у широкому розумінні). Для ліберальних демократій постійне перебування у стані війни є неприйнятним на даному етапі, але використання інформаційного простору уможливлює дії у відповідь на інформаційну атаку, не порушуючи демократичних норм і принципів. Важливою також є проблема поєднання усієї сукупності питань національної кібербезпеки в єдину парадигму, яка охопила б і військові, і цивільні питання, могла б функціонувати як під час миру, так й під час війни, а також бути присутньою у різних компонентах « національної могутності» (Klimburg and Tirmaa-Klaar, 2011).

Важливим напрямом дискусії щодо інформаційної безпеки є еволюція феномену війни, обумовлена бурхливим інформаційним та науково-технічним розвитком. Зазначимо, що в умовах ескалації глобальної геополітичної конфронтації, тема війни, її нових форм, методів і засобів ведення, активно обговорюється в експертному середовищі. За останній час з'явилося значна кількість теорій і концепцій, які підкріплюються практичними діями акторів міжнародних відносин, зокрема, Р. Банкера, Д. Деннінг, М. ван Кревельда, М. Лібікі, В. Лінда, Л. Мура, Д. Стейна, Е. Тоффлера та Г. Тоффлер, Г. Уілсона, Т. Хеммса, Р. Шафранскі, В. Швартау Д. Шміта та ін. В рамках досліджуваної теми слід зупинитися на найбільш значущих, які мають практичне застосування в сучасних війнах і конфліктах.

Так, у роботі «Війна та антивійна: виживання на початку XXI століття» відомі американські соціологи Е. Тоффлер та Г. Тоффлер визначають новий тип війни – «війну третьої хвилі» , яка суттєві відрізняється від методів, засобів і стратегій війн попередніх хвиль розвитку. Війни «третьої хвилі», перш за все, пов'язані із технологічної трансформацією та зростанням ролі знань. Таким чином, перехід до нового етапу цивілізаційного розвитку передбачає й новий виток революції у

військовій сфері, що порушує існуючий баланс сил і призводить до удосконалення засобів ведення війни. Цікавими є висновки авторів про те, що у політиці технології і знання перетворюються на джерело влади, а у військовій сфері – на ресурс для руйнування (Toffler, A. And Toffler, H., 1995). Новий тип війн має масштабний характер і здатен охопити усю цивілізацію. Водночас, автори виокремлюють ще один феномен – «малих війн», які характеризуються значно меншим масштабом і появою диференційованих фрагментів, тобто своєрідних ніш локальних загроз (наприклад, сепаратистських війн, етнічних чи релігійних конфліктів, суперечки щодо кордонів і прикордонних територій, терористичних актів, актів громадянської непокори тощо (Toffler, A. And Toffler, H., 1995). Саме тому, для ведення таких війн необхідні невеликі підрозділи «інтелектуальних бійців», оснащених сучасними засобами протиборства (робототехнікою, безпілотними літальними апаратами, супутниковими технологіями спостереження, технологіями розумного маскування, штучним інтелектом і технологіями віртуальної реальності тощо), які здійснюють різноманітні військові операції за принципом мережноцентрованих війн і здатні виводити з ладу ворожі засоби ведення війни без масштабних людських втрат. Автори також вводять термін «антивійна», яку вони визначають як війну нового типу, що передбачає активну діяльність, спрямовану на недопущення виникнення масової війни (якщо це можливо) чи ефективне протистояння військовим діям сучасними засобами, що мають колосальний потенціал швидкого завершення операцій супротивника (якщо зіткнення неможливо уникнути) (Toffler, A. And Toffler, H., 1995).

Показовим для аналізу теорій інформаційної війни стали роботи Р. Банкера, який критично оцінює концепцію Е. і Х. Тоффлерів. У роботі «Покоління, хвилі та епохи: типи війни та революція у політичній та військовій справах» стверджується, що у періодизації зміни поколінь війни слід спиратися на зміну енергетичної парадигми розвитку цивілізації. Саме трансформація у сфері базових енергетичних процесів здатна суттєво вплинути на форму державного управління та саму національну державу, призводячи до виникнення нової постмодерністської форми політичної спільноти. Так, якщо війни першої епохи базувалися на людській енергії,

другої – на тваринній, третьої – на механічній, то четвертої – на постмеханічній. Війни четвертого покоління можуть базуватися як на ідеях, так й технологіях і поділятися на два типи – війна незахідних країн (базуються на поєднанні тероризму та конфліктів низької інтенсивності як виклик домінуванню Заходу) та війна передових технологій (передбачає активне використання сучасних воєнних технологій, зокрема, високоточної зброї, роботизованих бойових одиниць, зброї спрямованої енергії тощо). Впровадження нових технологій призведе до втрати монополії національних держав на війну та збільшення кількості нетрадиційних учасників воєнних дій, зокрема, терористів, партизанських угруповань, приватних армій, наркокартелів та транснаціональних корпорацій. В кінцевому результаті це може призвести до втрати політичної легітимності, а згодом – поставити під сумнів можливість виживання самої національної держави. Тому війна перетвориться з «боротьби між національними державами або їх коаліціями за збереження і розширення державного суверенітету» на «боротьбу між конкуруючими формами державного суверенітету» (Bunker, 1996). Про це зазначає й В. Лінд у теорії «війни четвертого покоління». На думку автора, нове покоління війн є найбільш небезпечним, оскільки призводить до кризи легітимності держави і уможливлює вторгнення на територію іншої держави без офіційного оголошення війни (наприклад, імміграція, що руйнує систему національної безпеки держави). В таких умовах традиційні засоби ведення війни не можуть бути ефективними (Lind, 2004).

В іншому дослідженні Р. Бенкера у співавторстві з Л. Мур «Нелетальні технології і війни четвертої епохи: нова парадигма політико-військової сили» йдеться про засоби ведення війни в сучасних реаліях інформаційного і технологічного розвитку, що суттєво впливає на стратегію безпеки сучасної держави. Так, на думку авторів, впровадження передових технологій у військову сферу суттєво модернізує практику застосування політичного насильства Заходом, який буде прагнути роззброїти супротивника, а не знищити його. Отже, потреба у розробці і застосуванні нелетальних засобів протиборства буде лише зростати, допоки не досягне ефективності летальних технологій. При цьому, нелетальні технології матимуть попит як у зовнішньої та безпекової політики, так й у сфері

національної безпеки, особливо у ситуаціях, коли необхідно відновити громадський порядок і не допустити дестабілізації ситуації всередині країни. Перевага нелетальних технологій полягає й у тому, що їх застосування дозволяє поєднати різні інновації у в єдину бойову силу. Тобто раніше дискретні і не пов'язані одна з одною форми війні – інформаційна і радіоелектронна війна, психологічна війна і пропаганда, біологічна і хімічна війна можуть поєднуватися з досягненнями у сфері енергетики, акустики, комп'ютерних програм, генної інженерії тощо. Тобто йдеться про новий тип війни, аналогів якої ще не було (Bunker and Moore, 1996)

У розвиток теорії війн четвертого покоління М.ван Кревельд у роботі «Трансформація війни» вводить поняття «нетринітарної» війни, яка поєднує в собі новітні методи протиборства, зокрема, інформаційну війну, економічну війну, кібервійну, і характеризується як асиметричний конфлікт «низької інтенсивності». Найбільш важливою рисою цього типу війни є те, що в ній також беруть участь різноманітні квазідержавні та недержавні актори, зокрема, приватні військові компанії, терористичні угруповання, партизанські об'єднання тощо. Саме тому в нетринітарних війнах втрачається вага технологічної переваги, тобто технологічно розвинені держави можуть програвати партизанським угрупованням. Водночас, це не означає, що фактор технологій втрачається абсолютно. Навпаки, спостерігається розмивання межі застосування військових технологій, які швидко проникають у сучасне суспільство і можуть стати доступними для використання як комбатантам, так й некомбатантам в цій новій війні (Creveld, 2005).

Інший дослідник – Т. Хеммс – у статті «Війна переходить у четверте покоління» зазначає, що такий тип війн нині становить один з найбільших викликів для сучасної системи міжнародної безпеки, оскільки уможливлює використання усіх доступних засобів – політичних, економічних, соціальних, військових – для того, щоб переконати ворога, який ухвалює рішення, у тому, що їх стратегічні цілі або недосяжні, або не матимуть позитивного ефекту. Ініціатори такого типу війни не прагнуть перемогти завдяки військовим силам. Навпаки, вони використовують партизанську тактику або акти громадянської непокори у поєднанні з «м'якою» дією мереж соціальних, культурних, економічних зв'язків, кампанії з дезінформації

задля прямого впливу на політичну волю супротивника. Тому війна четвертого покоління є політичним, соціальним (а не технологічним), мережевим і довготривалим конфліктом (Hammes, 2007).

Натомість А. Ечеваррія у роботі «Війна четвертого покоління та інші міфи» зазначає, що ця теорія має чимало недоліків фундаментального характеру, що може негативно вплинути на операційне і стратегічне мислення американського керівництва, на стратегію зовнішньої і безпекової політики, а також на воєнну доктрину США. На думку автора, важливим є не самий тероризм, а те, якими засобами користуються терористи для завдання удару, не теорія бліцкригу або принципи Вестфальської системи, а те, що в умовах глобалізації відбувається демократизація доступу до сучасних технологій, інформаційних ресурсів та фінансів, що робить діяльність терористичних і злочинних угруповань більш мобільною і глобально доступною. Отже, нині глобалізація більше допомагає недержавним суб'єктам, а ніж державам, але держави все ж продовжують відігравати провідну роль у формуванні глобальної системи безпеки (Echevarria, 2005).

Д. Стейн у своїй праці «Інформаційна війна», зокрема, зазначає, що новий тип війни слід розглядати як конфлікт на рівні суспільства або між націями, який розгортається на стратегічному рівні. Інформаційна війна не тільки змінює спосіб та простір (театр) ведення бойових дій на тактичному (операціональному) і стратегічному рівнях, але може стати й театром воєнних дій, де проводяться «операції, відмінні від війни», що дозволяє досягати важливих цілей національної безпеки без застосування військової сили. На думку автора, така війна тісно пов'язана з ідеями та епістемологією, тобто пов'язана з тим, як люди мислять і ухвалюють рішення, тому саме свідомість буде найважливішою сферою протиборства (Stein, 1995).

На думку іншого дослідника, Р. Шафранскі, інформаційну війну, яку він тлумачить як військову діяльність, спрямовану проти будь-якої системи знань чи передбачень ворога (Szafranski, 1995), доцільно розглядати крізь призму феномену «інформаційних озброєнь». Інформаційна зброя, на відміну від традиційної (автор

тлумачить її як набір смертельних і несмертельних засобів ведення збройного конфлікту), може бути використана як проти внутрішніх, так й проти зовнішніх ворогів. Вона є універсальною і багатоваріативною, має атакуючий характер, тривалий час залишається непомітною, спричиняє значний вплив на об'єкти дій, дозволяє ретельно обрати час і місце застосування, а також є значно менш витратною. Таким чином, на думку автора, використання нового типу озброєнь в рамках інформаційні війни призводить до руйнування чітких меж між станом війни і миру, між військовими і цивільними об'єктами впливу, що суттєво ускладнює систему забезпечення безпеки (Szafranski, 1995). Р.Шафранскі також зазначає, що чим більше є інформаційно і технологічно розвиненою держава, тим більш вразливою вона стає в умовах інформаційного протистояння. Демократичні держави, хоча і менш вразливі, ніж тоталітарні, залишаються привабливим об'єктом для застосування інформаційних озброєнь. У той же час, із розвитком інформаційних систем і мереж, збройні конфлікти, ініціаторами яких виступають терористи чи релігійні екстремісти, будуть становити реальну загрозу, оскільки інформаційна зброя в їх руках, спрямована на різні вузли критичної інфраструктури, може негативно впливати на діяльність лідерів держав (Szafranski, 1995).

Американський дослідник Р. Ендрес у своїй роботі «Перегорнута мілітаризована дипломатія: як держави домовляються за допомогою кіберзброї», аналізуючи проблему мілітаризації кіберпростору, доходить висновку про існування тісного взаємозв'язку між військовим суперництвом та стратегічними цілями держав-учасників протистояння. Це проявляється у впровадженні так званої «перегорнутої мілітаризованої дипломатії», що передбачає використання мілітаризованих активів (тобто кіберзброї) задля доступу до необхідних ресурсів, покладаючись при цьому на діяльність дипломатів, які повинні обмежити потенційну ескалацію протистояння. Таким чином, якщо об'єкт такої діяльності є вкрай важливим для захисту національних інтересів або для досягненні переваги у міждержавному протистоянні, то використання кіберзброї має передбачати усвідомлення небезпеки викриття як держави-ініціатора використання інформаційних засобів протиборства, неможливості подальшого використання

аналогічних засобів у відповідь та потенційну можливість подальшої ескалації конфлікту у разі ідентифікації кібератаки (Andres, 2014).

Вагомими для розробки теорії інформаційного протиборства стали праці відомого теоретика інформаційної війни М. Лібікі. У своїй роботі «Що таке інформаційна війна?» автор зазначає, що інформаційні війни є настільки багатогранним явищем, що говорити про його концептуальні рамки майже неможливо. Тобто, такого поняття як «інформаційна війна», на думку автора, не існує. У той же час автор намагається всебічно проаналізувати феномен нового типу війни і дати певні теоретичні узагальнення. По перше, М. Лібікі зазначає, що інформація і інформаційні технології набувають дедалі більшого значення для системи національної безпеки і значно змінюють характер і способи війн і конфліктів в сучасному світі, які перетворюються на боротьбу за контроль над інформаційними системами. Використання методів ведення інформаційної війни дає беззаперечні переваги для тих, хто оволодів цими методами над прибічниками традиційних форм ведення війни, навіть в умовах значної переваги у військовій сфері. По-друге, можна виокремити сім форм інформаційної війни, кожна з яких може претендувати на окрему, більш широку концепцію, зокрема, командно-адміністративну війну; розвідувальну війну; радіоелектронну війну; психологічну війну; хакерську війну; економічну інформаційну війну та кібервійну (Libicki, 1995). Розглядаючи проблему кіберпростору як нового виміру протиборства держав, М. Лібікі зазначає, що попередні теорії війни базувалися на класичному розподілі просторів протистояння на повітряний, наземний, водний і космічний. Але тільки кіберпростір є штучно створеним і поєднує всі попередні виміри. Таким чином, якщо за наявності переваг в одному з перелічених просторів ініціатор війни буде обмежений у доступі до кіберпростору, він приречений на поразку (Libicki, 2012). Автор також зауважує, що неправильним є пряме перенесення реалій фізичного протиборства у кіберпростір, оскільки надзвичайно складно встановити джерело атаки, визначити межу для дій у відповідь, передбачити ескалацію конфлікту та ідентифікувати всіх задіяних в конфлікті осіб (Libicki, 2009.).

Значний внесок у розробку теорії інформаційної війни зробили дослідники Д. Арквілла і Д. Ронфельдт. У своїй праці «Кібервійна наближається» автори зазначають, що інформаційна революція та інноваційні технології змінюють природу конфлікту, типи військових структур, організацію збройних сил, військові доктрини і стратегії. Кібервійна дає можливість суттєво збільшити ударну міць і зменшити масштаби руйнування. Автори також зазначають, що слід відрізняти поняття кібервійни та мережної війни. Так, на їх думку, кібервійна – це конфлікт, пов'язаний зі сферою знання на військовому рівні, а мережна війна – конфлікт низької інтенсивності за участю недержавних акторів (наприклад, терористичні угруповання або наркокартелі), пов'язаний із соціальною боротьбою. Обидва види конфліктів є боротьбою великих « мереж» , а не « ієрархій» , тому у сучасному протистоянні перемагає той, хто найкраще опанує мережну форму протиборства (Arquilla and Ronfeldt, 1993). В іншій праці – «Мережі і мережні війни: Майбутнє терору, злочинності та бойових дій» автори приділили увагу детальному аналізу саме мережної війни, яку тлумачать як « різновид конфлікту (і злочинності) на соціальному рівні, відмінний від традиційних воєнних дій, в якому голові його учасники використовують мережні форми організації та пов'язані з ними доктрини, стратегії, технології, що відповідають вимогам і можливостям інформаційної епохи» (Арквілла та Ронфельдт, 2005). Під час мережних війн учасники намагаються взаємодіяти і координувати діяльність за принципом мережної взаємодії розсіяних організацій, невеликих груп, окремих осіб. Така мережа може навіть не мати єдиного центру чи керівництва і постійно переформуватися відповідно до обставин. Отже, для системи безпеки мережні війни перетворюються на виклик, оскільки ефективно протистояти злочинним угрупованням, що діють за таким принципом, стає дедалі складніше (Арквілла та Ронфельдт, 2005).

Важливою для розуміння особливостей сучасних методів ведення війни, що впливають стратегії інформаційної безпеки на глобальному, регіональному і національному рівнях, є концепція мережноцентрованих війн. Так, А. Себровскі і Д. Гарстка у дослідженні «Мережноцентровані війни: витоки та майбутнє» (Cebrowski and Garstka, 1998) зазначають, що під впливом інформаційного і

науково-технологічного розвитку відбуваються значні трансформації не тільки у суспільстві, бізнесі, політиці, а й у військовій сфері. Розпочинається новий етап так званої Революції у військовій сфері, яка призвела до зміни стратегій і методів ведення військових операцій, а також поняття стратегічних переваг. Отже, для того, щоб отримати переваги, тактично важливою стає швидкість, яка вимагає нової операційної архітектури з трьома критичними елементами: сенсорні решітки, решітки взаємодії та високоякісна інформаційна платформа, що об'єднує всі складові. Особливостями мережноцентрованої війни є швидкість ухвалення рішень командуванням та принцип самосинхронізації. Наприклад, швидкість командування передбачає нарощування інформаційної переваги, шляхом збільшення обсягу корисної інформації про супротивника, що дозволяє досягати в короткий термін позитивного масованого ефекту завдяки блокуванню діяльності супротивника і введення його у шоковий стан, тобто нейтралізації будь-яких контр-стратегій і можливостей використовувати наявний потенціал для протидії. Самосинхронізація дозволяє добре поінформованим силам організовувати і синхронізувати складні бойові дії знизу уверх. Реалізувати цей принцип можливо за умови отримання повного доступу до оперативної інформації. Таким чином, зменшуються втрати бойової потужності, характерні для командно-керованої синхронізації в рамках традиційних доктрин, а сама військова операція перетворюється із ступеневої функції на високошвидкісний континуум. Концепція мережноцентрованих війн була розвинена у колективній праці «Мережноцентрована війна: розвиток та використання інформаційної переваги» Д. Альбертса, Д. Гарстки і Ф. Штейна. Так, автори, використовуючи базову теорію мережноцентрованих війн, зазначають, що новий тип війни передбачає формування мережноцентрованого способу мислення та його використання у військових операціях. Впровадження мережевого принципу дозволяє швидко досягати необхідної бойової потужності завдяки взаємодії географічно розподілених сил, формуванню спільного усвідомлення бойового простору та реалізації спільних мережноцентрованих операцій (Alberts, Garstka and Stein, 2000)

Е. Сміт, аналізуючи проблему трансформації війн і конфліктів в інформаційну добу, пропонує у розвиток теорії мережноцентрований війн концепцію « операції із досягнення ефективності». Так, у роботі «Операції із досягнення ефективності: застосування мережноцентрованих війн в умовах миру, кризи та війни» (Smith, 2002), зокрема, зазначається, що адаптація до інформаційної доби передбачає не тільки активне використання досягнень науки і техніки, але й суттєвої зміни підходів до здійснення військових операцій. Так, на думку автора, «операції із досягнення ефективності» дозволяють застосовувати потенціал мережноцентрованих війн навіть у традиційних конфліктах задля посилення ефекту та виходу за межі лише кінетичних засобів протиборства, залучення інформаційної і когнітивної сфер для створення більшого ефекту операції, які можуть проводитися як у мирний час, так і під час відкритого військового протистояння, в умовах криз та конфліктів. Отже, такі операції дозволяють переключити увагу з цілей та збитків на стимули, які змінюють поведінку, що стає основою для оновлення концепції стратегічного стримування і суттєво впливає на формування сучасного середовища безпеки (Smith, 2002).

Б. Берковіц у роботі «Нове обличчя війни: як буде вестися війна у XXI столітті» зазначає, що нині інформаційне протиборство набуває самостійного характеру і вже не є другорядними діями на тлі великої війни. Нині важливим є високоточні удари по конкретним цілям, перевага в інформації та швидкість ухвалення рішень. Нова війна має чотири ключові фактори: асиметричність загроз, які роблять вразливими навіть найбільш потужні армії, конкуренція в інформаційних технологіях, що дає переваги у воєнному використанні комп'ютерів та засобів зв'язку, гонка у циклах ухвалення рішень, в якій перемагає та сторона, яка першою отримує, обробляє інформацію і оперативно реагує на неї, мережева організація, яка дозволяє швидко утворювати різноманітні структури для боротьби з будь-яким супротивником (Berkowitz, 2007).

В контексті дослідження сучасних теорій у сфері безпеки дедалі більшої актуальності набуває концепція гібридної війни. Так, Ф. Хоффман у роботі «Гібридні війні та виклики» зазначає, що нині відбувається «розмивання» форм

війни. Таким чином, супротивник може використовувати синергетичний ефект від одночасного використання різних режимів війни. Для держави-об'єкта такої діяльності виникає одразу комплекс проблем, які необхідно швидко вирішувати. Отже супротивник може поєднувати найбільш руйнівні ефекти з традиційними або нерегулярними формами війни, досягаючи катастрофічних наслідків. Як зазначає автор, гібридна війна – це такий тип конфлікту, в якому супротивник використовує унікальні комбіновані загрози, спрямовані на найбільш вразливі елементи системи національної безпеки держав. Багатоваріативність такого типу війн пов'язана й з можливістю використовувати у протиборстві представників злочинних груп або терористів, повстанців та нерегулярні війська, які ще більше дестабілізують ситуацію і допомагають тим самим досягати бажаного ефекту. Гібридну війну можуть вести як держави, так й недержавні суб'єкти. Тобто у такому протистоянні перевагу отримує той, хто обирає не один спосіб ведення війни, а кілька тактик і технологій, змішаних із сучасними, інноваційними способами, які відповідають їх власній стратегічній культурі, територіальному розташуванню та цілям. Як підкреслює Ф. Хоффман, гібридні загрози включають у себе цілий спектр способів ведення війни, зокрема, конвенційні методи, нерегулярні тактики, терористичні атаки, злочинні дій, що дозволяє досягати бажаного стратегічного ефекту у фізичному і психологічному вимірах конфлікту. З одного боку, це дає підстави стверджувати, що гібридна війна є неновим явищем, але з другого, стає очевидним факт інноваційного поєднання усіх відомих способів протиборства в єдину систему заходів. До того ж, слід зауважити, що до переліку способів ведення війни у гібридній формі нині долучаються й технологічні та інформаційні інновації, що значно розширює спектр дії та руйнівний ефект гібридних загроз (Hoffman, 2009)

Зазначимо, що в України нині вивчення різноманітних питань інформаційної безпеки набули особливої актуальності. Чисельні роботи українських політологів присвячені як загальним питанням трансформації системи міжнародної безпеки в умовах формування глобального інформаційного суспільства, впливу досягнень науки і техніки на сучасну архітектуру безпеки, так і спеціальним питанням, зокрема, ведення інформаційних, гібридних та когнітивних війн, трансформації

методів протиборства та особливості використання спеціальних інформаційних операцій, зміни поняття сили в сучасних міжнародних відносинах, ефективності впровадження різних механізмів безпеки на рівні держав та міжнародних інституцій тощо.

Так, у працях відомого українського дослідника Г. Почепцова, зокрема, зазначає, що інформаційні війни стали одним з найважливіших інструментів впливу як у мирному житті, так й в умовах воєнного протистояння. У дослідженні «Інформаційні війни» автор зазначає, що інформаційний характер сучасного світу обумовлює зростання ваги інформації для будь-якого актора міжнародного чи національного політичного простору. При цьому в умовах ведення інформаційної війни більш потужні держави можуть значно посилювати свої позиції на світовій арені, при цьому країни менш розвинені отримують шанс зрівнятися з ними, оскільки інформаційні озброєння мають асиметричний характер дії і залишаються найбільш дешевим варіантом відповіді на чужі агресивні дії (Почепцов, 1999). У роботі «Сучасні інформаційні війни» автор розглядає феномен інформаційної війни у контексті аналізу загальних тенденцій інформаційного розвитку цивілізації, таким чином, підкреслюючи особливий характер нового типу війни, який перетворився на складову повсякденного життя. Автор також зазначає, що новий, інформаційний інструментарій протиборства дає не лише більш дешеві засоби впливу, а й дозволяє уникнути відповідальності, оскільки інформаційна сфера не настільки ефективно захищена на законодавчому рівні. До того ж, стає дедалі складніше відрізнити умисний і випадковий розвиток подій. Отже, на думку автора, сучасні інформаційні війни – це квазіагресивний інструментарій мирного життя, а не лише збройного конфлікту між державами (Почепцов, 2015).

В праці «Когнітивні війни у соцмедіа, масовій культурі та масових комунікаціях», зокрема, зазначається, що інформаційні війни впливають на процеси передачі інформації, а когнітивні – на процеси мислення та ухвалення рішень. Саме завдяки когнітивному впливу інтерпретація подій може стати абсолютно протилежною, хоча стосується однієї події. Таким чином, в когнітивній війні головним стає не брехня, фейк чи дезінформація, а підтримка полеміки, перевіреної

об’єктивними фактами. Таким чином, поширюється новий тип війни – когнітивний (Почепцов, 2019c). У роботі «Віртуальні війни. Фейки» Г.Почепцов, досліджуючи питання інформаційної інтервенції та їх смислових інтерпретацій, проводить чітку межу між когнітивними війнами і кібератаками. Так, внаслідок інформаційної інтервенції відбувається поєднання інформаційної і віртуальної складової, а внаслідок кібератаки – інформаційної і фізичної. Тому у першому випадку метою впливу виступає когнітивний простір масової або індивідуальної свідомості, у другому – фізична трансформація інформаційних ресурсів (Почепцов, 2019a). У роботі «Війни нових технологій» зазначається, що нині світ пішов від звичайних воєн із застосуванням зброї до воєн нетрадиційних способів протиборства – гібридних, смислових і інших, але при цьому вони не стають менш небезпечними, оскільки зберігають свою основну мету – захоплення чужої території або чужого розуму. Часто ці війни неможливо побачити відразу, але вони змінюють сприйняття світу, а тому, все те, що досягається в результаті перемоги, стає важко або неможливо змінити, оскільки нетрадиційні війни розроблено так, щоб не допустити прийняття правильного рішення. Подальший розвиток інформаційно-технологічної сфери призводитиме до модернізації кібератак, які ставатимуть більш креативними та інтенсивними. Тому подальший науково-технологічний та інформаційний розвиток перетворить інформаційне протиборство на більш небезпечне явище, оскільки це пов’язано з найбільш вразливим елементом – людським фактором. (Почепцов, 2019b).

Робота «Від покемонів до гібридних війн. Нові комунікативні технології XXI століття» Г. Почепцова присвячена аналізу інформаційної складової гібридних війн. Так, автор зазначає, що у гібридній війні, яка може стати домінуючою у майбутньому, важливою складовою є саме інструментарій інформаційного протиборства, оскільки сама війна такого типу можлива лише у випадку потужної інформаційної агресії. Адже країна, яка атакує, не афішує своєї участі у війні, присутності війська та передачі зброя. Усе це можна компенсувати лише потужною інформаційною підтримкою (Почепцов, 2017).

Так, у колективній монографії «Світова гібридна війна: український фронт» (В.П. Горбуліна, Д. Дубова, М. Ожевана, О. Литвиненка, С. Гнатюка, Г. Яворської та ін.) детально досліджено феномен гібридної війни у контексті як світових процесів системної кризи глобальної безпеки, так й російської агресії проти України. Зокрема, аналізуючи передумови початку гібридної агресії Росії проти України, автори наголошують на проблемах в інформаційній сфері (деструктивна діяльність медіа, недостатньо розвинений вітчизняний телерадіопростір, відсутність концептуалізованої державної інформаційної політики, недостатньо високий рівень фахової компетентності представників журналістської спільноти, надмірна залежність ЗМІ від власників, брак дієвих інституцій та механізмів оперативного реагування на інформаційні та інформаційно-психологічні загрози), яка перетворилася на важливий вимір протистояння. Отже, станом на кінець 2013 р. в Україні практично не було дієвої системи захисту національного інформаційного простору. Як підкреслюють автори, саме інформаційна складова гібридної війни стала наскрізною для всієї агресії Росії проти України. Наприклад, спираючись на значну перевагу в інформаційній сфері, агресор зміг на початковому етапі досягнути поставлених цілей психологічної дезорієнтації населення на окупованих територіях (Горбулін та ін., 2017). Підкреслимо, що дана наукова праця є результатом діяльності фахівців Національного інституту стратегічних досліджень, які формують нині потужну наукову школу з вивчення питань інформаційної безпеки.

У науковій праці Д. Дубова «Кіберпростір як новий вимір геополітичного суперництва» досліджуються проблеми кіберпростору у вимірі геополітичного і геостратегічного суперництва держав – США та КНР, а також можливості України у забезпеченні національних інтересів в умовах зростання геополітичного значення кіберпростору та інтенсифікації протистояння у ньому. Д. Дубов звертає увагу на проблему мілітаризації кіберпростору, аналізує сучасні військово-політичні та політологічні концепції нового світоустрою, зокрема, формування кібервестфальської системи. У науковій праці також розглядаються питання інформаційного протиборства та інформаційних конфліктів, механізмів сучасного протистояння (хактивізм, кібершпигунство, ківбердиверсії), а також політика у

сфері кібербезпеки США та КНР. Особливу увагу автор приділяє питанням забезпечення національних інтересів України в глобальному та національному кіберпросторах (Дубов, 2014)

Питання інформаційної війни та інформаційної безпеки розглядаються у парцях іншого відомого українського дослідника М Ожевана. Так, у монографії М. Ожевана та Д. Дубова «Homo ex Machina. Філософські, культурологічні та політичні передумови формування конвергентного суспільства» досліджується питання впливу технологічного розвитку на сучасну систему глобальної і національної безпеки. Аналізуючи феномен інформаційного суспільства, автори приділяють особливу увагу трансформації підходів до стратегій конкуренції держав, еволюції поняття «національний інтерес» в умовах формування глобального політико-інформаційного простору та концепції «цифрового стримування». Так, на думку авторів, в умовах розбудови інформаційного суспільства важливого значення для системи безпеки набуває поняття цифрового суверенітету. Тривале ігнорування цієї проблеми західними країнами обумовлено, на думку Д. Дубова та М. Ожевана, двома принциповими факторами: досить обережне ставлення до будь-яких концепцій та досліджень щодо проблеми суверенітету та переконаність країн Заходу як найбільш технологічно розвинених у світі у тому, що сама постановка проблеми, коли держава може бути недостатньо суверенною в сенсі контролю за своїм цифровим простором, є неприпустимою. Автори також наголошують, що з поняттями інформаційного та цифрового суверенітету тісно пов’язана також поняття кібермогутності, яку вони тлумачать як «здатність до використання кіберпростору для створення переваг та впливу в усіх інших операційних просторах через інструменти могутності». Фактично цифровий суверенітет (точніше, його елементи) є як наслідком, так і джерелом цієї кібермогутності (Ожеван, Дубов, 2017).

Вагомий внесок у розвиток теорії інформаційної безпеки та інформаційного протиборства було зроблено О. Литвиненком, який у своїх працях детально аналізує теоретико-методологічні засади здійснення інформаційних операцій та впливів у сучасному світі. Так, у монографії «Інформаційні впливи та операції. Теоретико-

аналітичні нариси» автор представив аналіз феномену інформаційних операцій з позиції ідейно-політичної гегемонії, практики здійснення інформаційних операцій у провідних країнах світу, їх структури та сценаріїв, а також підходи до захисту від спеціальних інформаційних операцій. Аналізуючи сучасну практику захисту від спеціальних інформаційних операцій, О. Литвиненко зазначає, що актуальною стає проблема зміни парадигми безпеки, яка в сучасних умовах повинна передбачати адаптацію системи, що захищається, до змін у зовнішньому і внутрішньому середовищі. Отже, на думку автора, найбільш ефективною стратегією захисту нині є «стратегія гнучкого реагування на асиметричній основі» (Литвиненко, 2003).

Питання інформаційної безпеки також ґрунтовно представлені у колективній монографії «Міжнародна інформаційна безпека: сучасні виклики і загрози». Так, у науковій праці розглянуто концептуальні питання формування міжнародної інформаційної безпеки у глобальній системі підтримання миру і стабільності, представлено аналіз сучасних методів протиборства, визначено особливості інструментарію інформаційних війн і конфліктів, а також проаналізовано міжнародні нормативно-правові документи у сфері інформаційної безпеки та інституціональні засади формування глобальної і регіональної інформаційної безпеки (Гондюл, В.П. та ін, 2006). Данна наукова праця є підсумком діяльності наукової школи з досліджень сучасних методів протиборства та інформаційної безпеки Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка. У чисельних працях її представників (Є. Макаренко, М. Рижкова, С. Даниленка, О. Андрєєвої, Н. Бєлоусової, О. Запорожець, О. Кучмій, О. Фролової та ін.) міститься аналіз трансформації доктрини зовнішньої і безпекової політики США, важливою складовою якої нині виступає інформаційна безпека, досліджується феномен сили у сучасних міжнародних відносинах, аналізується практика використання «м'якої» і «розумної» сили, досліджуються проблеми формування нової системи міжнародної безпеки в умовах глобалізації комунікації, діяльність міжнародних інституцій у сфері інформаційної безпеки, а також сучасні методи і прийоми інформаційного протиборства, формування підходів до державно-приватного партнерства у сфері забезпечення інформаційної безпеки; формування

стратегії проблеми інформаційної безпеки провідних акторів міжнародних відносин, а також проблеми дії норм і принципів гуманітарного співробітництва в умовах зростання масштабів інформаційного протиборства та ін. (Рижков, 2007; Макаренко, 2011; 2016; Бєлоусова, 2018; Кучмій, 2016; Фролова, 2019 та ін.)

Наприклад, у чисельних наукових працях Є. Макаренко висвітлюються різноманітні аспекти міжнародної інформаційної безпеки – проблеми формування нової парадигми світової безпеки в умовах становлення інформаційної цивілізації, моделі міжнародної інформаційної безпеки, права міжнародної інформаційної безпеки, а також діяльності міжнародно-політичних інституцій у сфері інформаційної безпеки. Авторка, зокрема, зазначає, що формування нової геостратегічної структури міжнародних відносин під впливом глобалізації та швидкоплинного розвитку високих технологій зумовило нові підходи та окреслення нових параметрів сучасної системи міжнародної безпеки. В цьому контексті особливої ваги набуває проблема міжнародної інформаційної безпеки. Аналізуючи особливості трансформації підходів міжнародних інституцій до проблеми інформаційної безпеки, зокрема, в рамках ООН, Є. Макаренко особливу увагу приділяє питанням вироблення норм міжнародного права у сфері інформаційної безпеки та зростання суперечностей між державами щодо принципів міжнародної інформаційної безпеки. Як зазначає авторка, багатогранність ІКТ у політичному, економічному, безпековому, соціальному та культурному плані, визнання руйнівного чинника нових високотехнологічних озброєнь змусило ООН та інші впливові міжнародні організації включити проблему міжнародної інформаційної безпеки у сферу своїх інтересів (Макаренко, 2016). Окремо слід відзначити наукові праці, присвячені діяльності регіональних інституцій АТР – АТЕС, АСЕАН та ШОС. Так, у публікації «Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст» авторка аналізує стратегії регіональних інституцій у сфері кібербезпеки, розглядаючи спільні і відмінні чинники їх діяльності та визначаючи перспективи забезпечення інформаційної та кібербезпеки регіональних спільнот з різним рівнем інформаційного розвитку. Наприклад, авторка зазначає, що безпекові імперативи регіонального об’єднання АТЕС переважно пов’язані з

питання інформаційної безпеки у сфері цифрової економіки, АСЕАН реалізує їх через стратегії інформаційної безпеки і боротьби з кібертероризмом, а ШОС намагається реалізувати їх в рамках ініціативи щодо ухвалення концепції і міжнародної конвенції з інформаційної безпеки на регіональному та глобальному рівнях міжнародного співробітництва (Макаренко, 2011).

Питання застосування асиметричних засобів ведення війни у сучасних міжнародних відносинах висвітлюються у колективній науковій праці « Асиметричні стратегії у сфері безпеки та оборони» . Так, Г. Перепелиця, вивчаючи асиметричні методи і прийоми ведення сучасних війн і конфліктів, виокремлює феномен «інформаційної зброї», яка тлумачиться як «засоби знищення, спотворення або викрадення інформаційних масивів; добування з них необхідної інформації після подолання систем захисту; обмеження чи заборона доступу до них законних користувачів; дезорганізація роботи технічних засобів; виведення з ладу телекомунікаційних мереж, комп'ютерних систем, усього високотехнологічного забезпечення життя суспільства та функціонування держави». Таким чином у розвитку систем озброєнь простежується стала тенденція збільшення питомої ваги в цих системах саме інформаційної зброї. Під термін «інформаційна зброя» підпадають технічні або програмні засоби для забезпечення несанкціонованого доступу до інформаційних баз даних, порушення штатного режиму функціонування технічних засобів і програмного забезпечення, а також виведення з ладу ключових елементів інформаційної інфраструктури окремої держави або навіть регіону. Інформаційній зброї властиві такі особливості, як: атакуючий характер, універсальність, прихованість, багатоваріантність форм реалізації (у тому числі програмно-апаратної й технічної), радикальність впливу, достатній вибір часу та місця застосування і, нарешті, економічність. Усі ці особливості роблять інформаційну зброю надзвичайно небезпечною (Перепелиця, 2005.).

Отже, питання інформаційної безпеки є вкрай актуальними для української наукової думки. В роботі представлені лише окремі доробки, присвячені загальним питанням інформаційної безпеки. Водночас, незважаючи на те, що проблема інформаційної безпеки є і залишається актуальним питанням для наукових розвідок

багатьох науковців, експертів та аналітиків, досвід країн Азії представлений лише в окремих працях і не має системного характеру дослідження. Переважно увага сфокусована на діяльності такого геополітичного літера, як КНР та суперечності відносин Китаю та США. Але стратегії інформаційної безпеки інших регіональних акторів, як правило, залишаються поза увагою науковців. Серед робіт, присвячених окремим питанням інформаційної безпеки азійського регіону в рамках АСЕАН та ШОС, слід назвати дисертацію Ю. Романчука «Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти». У роботі автора зазначається, що « сутнісні характеристики політики інформаційної безпеки регіональних організацій Азійсько-Тихоокеанського регіону виявляють пріоритети співпраці на політичному рівні між всіма державами АТР з метою вироблення комплексної стратегії протидії інформаційним загрозам і розвитку регіональної системи інформаційної безпеки, а також удосконалення законодавства відповідно до міжнародних норм і принципів» (Романчук, 2009). Сучасні пріоритети у сфері інформаційної безпеки КНР також представлено у дисертації М. Копійки «Політика інформаційної безпеки у сучасних міжнародних відносинах». Так, авторка зазначає, що стратегічними напрямами політики інформаційної безпеки Китаю є забезпечення національних інтересів і захист внутрішнього інформаційного простору і кібернетичної інфраструктури, а також подолання непропорційності політико-безпекового розвитку КНР у порівнянні з розвиненими країнами, які виступають потенційними супротивниками в інформаційному протистоянні (Копійка, 2020)

1.3. Поняттєво-категоріальні характеристики інформаційної безпеки

Еволюція теоретичних підходів та практичної діяльності провідних акторів міжнародних відносин суттєво вплинули на термінологію у сфері інформаційної безпеки, окресливши тенденції, процеси та явища, що характеризують сучасні стратегії розбудови стійкої і безпечної інформаційної екосистеми. У роботі використовується термінологія, зафіксована у документах міжнародних організацій, до пріоритетів діяльності яких відносять проблеми безпеки в умовах

швидкоплинного інформаційного та науково-технологічного розвитку, дослідженнях провідних аналітичних центрів, що спеціалізуються на питаннях глобальної та регіональної інформаційної безпеки, а також у наукових працях відомих фахівців у сфері інформаційної безпеки.

Дослідження феномену регіональної політики інформаційної безпеки обумовило потребу звернення до поняття « міжнародна інформаційна безпека» , яку доцільно тлумачити як стан міжнародних відносин, що передбачає співробітництво акторів міжнародних інформаційних відносин з метою захисту міжнародної інформаційної інфраструктури, міжнародного інформаційного простору та суспільної свідомості від різного типу інформаційних загроз, джерелом яких можуть бути державні, недержавні актори або окремо діючі особи. Слід зазначити, що нині не тільки у наукових працях, але й на рівні міжнародних інституцій існує певна термінологічна неузгодженість щодо тлумачення феномену міжнародної інформаційної безпеки і кібербезпеки. Однією з причин цього стали процеси, ініційовані Російською Федерацією наприкінці 1990-х рр., пов’язані з проектом конвенції про міжнародну інформаційну безпеку. Спираючись на діючі нормативно-правові документи у сфері національної інформаційної безпеки, російська сторона запропонувала тлумачити інформаційну безпеку у більш розширеному форматі, включаючи до неї не тільки заходи, спрямовані на захист інформаційної інфраструктури від різноманітних інформаційних загроз, але й методи протидії засобам впливу на свідомість громадян шляхом поширення інформації деструктивного характеру, наприклад, через традиційні медіа. Такий підхід нині частково підтримує лише Шанхайська організація співробітництва, на діяльність якої продовжує суттєво впливати Російська Федерація та КНР. Водночас, навіть на рівні ШОС нині відбувається перегляд пріоритетів діяльності, а питання кібербезпеки набувають самостійного значення у контексті зростання масштабів наслідків застосування саме кіберзасобів у протиборстві між державами. Так, в Угоді між урядами держав-членів Шанхайської організації співробітництва про співпрацю в сфері забезпечення міжнародної інформаційної безпеки (Єкатеринбург, 2009 р.) інформаційна безпека тлумачиться як стан захищеності суспільства і

держави, їх інтересів 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 держави і світової спільноти в інформаційному просторі (SCO, 2009). Натомість в працях західних експертів « інформаційна безпека» здебільшого розглядається як безпека інформації, гарантія її цілісності і неушкодженості. Тобто, цей термін загалом використовується переважно як технічний і у міжнародних або національних документах у сфері безпеки і оборони зустрічається нині нечасто, за виключенням документів ООН, пов'язаних із подальшим процесом обговорення резолюції ГА ООН «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки». Водночас, в окремих країнах АТР термін «інформаційна безпека» використовувався лише на початковому етапі розробки стратегії і сьогодні, незважаючи на поширення нового терміну – кібербезпека, він може вживатися у значенні захисту усієї системи інформації, необхідної для подальшого поступального розвитку держави (CCDCOE, 2021).

Термін «кібербезпека» дедалі частіше використовується як у міжнародних нормативно-правових актах, так й національних стратегічних і доктринальних документах, а також різноманітних аналітичних досліджень та авторських наукових працях, які переважно визначають даний феномен як безпека критичних технологій і мереж. Тобто йдеться про безпеку, що передбачає створення ефективних механізмів захисту національного інформаційного середовища від різних видів протиправної діяльності кібезлочинців, хакерів, хактивістів, оскільки в умовах подальшої цифровізації країн і регіонів світу, появи все більшої кількості сучасних технологій та їх проникнення у суспільство, створення систем електронного державного урядування, втілення нових моделей економічної діяльності, поширення технології Інтернету речей і для речей, штучного інтелекту, побудова « розумних» міст безпека використання мереж і технологій стає фундаментальним питання подальшого розвитку сучасної цивілізації.

Слід підкреслити, що в рамках ООН нині відбувається переосмислення феномену кібербезпеки, оскільки дослідження практика застосування різноманітних

кібератак показало, що зловмисники активно використовують методи соціальної інженерії, спрямовані на маніпулювання свідомістю людей та їх поведінкою шляхом поширення незаконно добитої персональної інформації. Значного поширення такі методи набули під час пандемії COVID-19 (Callejas, Afifi and Lozinskiy, 2021). Отже, в рамках дослідження особливості регіональної політики інформаційної безпеки можна використовувати тлумачення «кібербезпеки», запропоноване МСЕ, як сукупність інструментів, політик, концепцій безпеки, заходів безпеки, керівних принципів, підходів до управління ризиками, дій, спрямованих на захист кіберсередовища та інформаційних ресурсів державних структур, організацій, приватних компаній та користувачів (ITU, 2010).

Останнім часом набуло поширення поняття «кібердипломатія», яке визначається як діяльність акторів міжнародних відносин, спрямована на використання дипломатичних інструментів та ініціатив для досягнення національних інтересів держави у кіберпросторі, які зазвичай окреслюються у національних стратегіях кібербезпеки (Manantan, 2021; Barrinha, A., Renard, 2020; Riordan, 2019). Кібердипломатія передбачає встановлення зв'язків не тільки між офіційними представниками держав та їх урядів, але й між державними і недержавними суб'єктами з метою запобігання мілітаризації кіберпростору, гонки озброєнь у кіберпросторі, розробки міжнародних норм у сфері кібербезпеки, які регулюють поведінку державних і недержавних акторів у кіберпросторі, просування національних інтересів у кіберпросторі через політику кібербезпеки та стратегії багатостороннього співробітництва. Як зазначає М.Б.Ф. Манантан, основою кібердипломатії виступає концепт «м'якої» сили, який вважається найбільш ефективним засобом для зменшення негативних наслідків поширення економічної і політичної невизначеності, ризиків та потенційних конфліктів, що виникають у кіберпросторі, а фундаментальним елементом інструментарію кібердипломатії є розбудова кіберпотенціалу, заходи із зміцнення довіри та розробка кібернорм (Manantan, 2021). Так, нарощування потенціалу в галузі кібербезпеки мотивується кінцевою метою стримування загроз. Держави розвивають кіберпотенціал для зменшення негативного впливу загроз у кіберпросторі або звичайних загроз з

використанням кібернетичних засобів протиборства з боку країн-супротивників. Це передбачає удосконалення технічного, управлінського та дипломатичного потенціалу, необхідного для забезпечення стійкості до кіберзагроз, впровадження національних стратегій кібербезпеки, створення груп реагування на кіберінциденти та удосконалення правоохоронної діяльності. Проте нині масштаби розвитку потенціалу вийшли за межі стандартних технічних міркувань або нормативних рамок і включають також підвищення рівня інформаційної грамотності та обізнаності (Manantan, 2021).

На думку Е.О. Голдман, кібердипломатія – це використання дипломатичних інструментів для вирішення питань, що виникають у кіберпросторі або внаслідок його використання. Вона охоплює такі сфери: безпека, економіка та права людини, включаючи міжнародні стандарти кібербезпеки, доступ до Інтернету, конфіденційність, свободу Інтернету, інтелектуальна власність, кіберзлочинність, ініційовані державою кіберконфлікти та конкуренція, етичне використання цифрових технологій і торгівля. Так само, як і в інших дипломатичних зусиллях, кібердипломатія працює шляхом побудови стратегічного партнерства з іншими країнами в усьому світу для посилення колективних дій та співпраці проти спільних загроз, формування коаліцій держав-союзників, які зацікавлені у вирішенні питань, пов’язаних з використанням кіберпростору, обміну інформацією та національними ініціативами, а також реалізації спільної стратегії протистояння загрозам у кіберпросторі (Goldman, 2021).

До понятєвих категорій інформаційної безпеки відносять також поняття «кібероборона» , щодо якого науковці не мають однозначної думки, оскільки самий феномен часто ототожнюють переважно з військовою сферою. Так, на думку експертів, кібероборона пов’язана з фундаментальною функцією держави захищати національний інформаційний простір від загроз ззовні. Водночас, як зазначає М. Да Сілва, кіберпростір не є класичним виміром з чіткими державними кордонами, а тому захист не може здійснюватися лише військовими засобами і має включати цивільні інструменти. Тому найбільш поширеним є тлумачення кібероборони як системи воєнних, політичних, правових, економічних, соціальних,

культурних та науково-технологічних заходів, використання яких спрямоване на захист національного інформаційного суверенітету. На думку експертів НАТО, кібероборона складається з проактивних заходів для виявлення та запобігання кібервторгнень, атак і вживання проактивних заходів для реагування на кіберзагрози з метою захисту критичної інфраструктури, мереж, об'єктів та інформації. Зазначимо, що кожна країна по-різному тлумачить поняття, виходячи з пріоритетів національної інформаційної безпеки, а деякі з них (наприклад, Велика Британія) вважають термін синонімом кібербезпеки (CCDCOE, 2021).

Поняття « кібермогутність» , яке у роботі розглядається як здатність держави використовувати кіберпростір для досягнення геополітичної переваги та впливу на інших акторів міжнародних відносин та міжнародні події, розглядалося у працях багатьох фахівців з проблем використання сили в сучасному інформаційному протиборстві (Дж. Ная, С. Старра, Г. Реттрея, А. Клімбурга, Д. Шелдона та ін.). Так, на думку Дж. Ная та С. Старра, кібермогутність – це здатність використовувати кіберпростір для створення переваг і впливу на події та діяльність інших акторів за допомогою інструментів влади. Кібермогутність можна використовувати для отримання бажаних результатів у кіберпросторі або як кіберінструменти для отримання бажаних результатів в інших сферах за межами кіберпростору (Starr, 2017; Nye, 2010). О.Клімберг також зазначає, що термін «кібермогутність» доцільно використовувати тоді, коли йдеться про кіберчинники міждержавних відносин. При цьому передбачається використання не тільки традиційних чинників сукупної потуги держави, але й нетрадиційних, які стосуються сфери освіти, науки, культури (Klimburg, 2013).

Ще одним терміном, який активно обговорюється у різноманітних фахових дослідженнях з питань інформаційної безпеки у військовій, політичній та економічній сферах, є «цифровий суверенітет». Зазначимо, що єдиного підходу до визначення цього феномену немає, а в науковій літературі він часто використовується як синонім інших понять, зокрема, «кібермогутність» або «інформаційний суверенітет», що ускладнює процес виокремлення його базових характеристик. Так, спираючись на широке коло досліджень, Д. Дубов і М. Ожеван

зазначають, що «цифровий суверенітет» пов'язаний з забезпечення ІКТ-незалежності держави, а « інформаційний суверенітет» – більш широке поняття, яке включає також питання контенту, що поширюється в інформаційному просторі держави (Дубов, Ожеван, 2017). Автори виокремлюють американський, східноазійський і європейський підходи до тлумачення феномену «цифрового суверенітету», кожен з яких базується на аналізі практики держав у нарощування кібермогутності та забезпеченні власного суверенітету у кіберпросторі. Так, американській підхід базується на чотирьох ключових елементах, які держава має забезпечити для формування цифрового суверенітету – технічний прогрес, швидкість та масштаби операцій, контроль ключових елементів та національна мобілізація. Для східноазійського підходу характерним є тлумачення цифрового суверенітету як синоніму кібермогутності, яка пов'язана із здатністю держави вести кібервійну. Отже, цифровий суверенітет в рамках цього підходу, пов'язаний з такими ключовими факторами: 1) розвиток можливостей інтернету та ІКТ, рівень розвитку інноваційного потенціалу та можливість здійснювати наукові дослідження і впровадження їх результати у промисловість; 2) нарощування можливостей ІТ-індустрії; 3) нарощування можливостей інтернет-ринку, 4) вплив інтернет-культури; 5) розвиток інтернет-дипломатії; 6) нарощування кіберскладової військової потужності; 7) прагнення держави розробляти і реалізовувати стратегії участі у боротьбі за кіберпростір. В рамках європейського підходу також спостерігається ототожнення понять «кібермогутність» та цифровий суверенітет» , основними складовими якого є: 1) інтегровані урядові можливості держави ефективно розпоряджатися своїми ресурсами у кіберсфері та чітко формулювати пріоритети діяльності у кіберпросторі; 2) інтегровані системні можливості держави використовувати формалізовані структури для досягнення своїх цілей; 3) інтегровані національні можливості, що передбачають реалізацію ефективної моделі співпраці з усіма зацікавленими сторонами для досягнення цілей безпеки у кіберпросторі (Дубов, Ожеван, 2017; Klimburg, 2013).

Як свідчить аналіз особливостей регіональної політики інформаційної безпеки, держави не тільки по-різному тлумачать феномен «інформаційного

суверенітету», «цифрового суверенітету» та «кібермогутності» , але мають й власне бачення шляхів їх досягнення. Так, КНР та РФ виступають за встановлення всеосяжного контролю над національним інформаційним простором та жорстких механізмів регулювання діяльності у кіберпросторі, демократичні держави намагаються діяти в рамках правового поля і встановлювати системи фільтрування інформації лише в інтересах національної інформаційної безпеки, чітко аргументуючи таку діяльність перед громадянами, щоб не бути звинуваченими у порушенні демократичних прав і свобод, а Індія прагне поєднати обидва підходи для підвищення ефективності стратегії у сфері кібербезпеки (Demchak, Dombrowski, 2011; Bagga, 2018).

Як підкреслюють експерти, нині між державами розгорнулася масштабна боротьба за «цифровий суверенітет», що передбачає використання різноманітних кібернетичних засобів для встановлення контролю над даними, програмним забезпеченням (наприклад, у сфері штучного інтелекту), стандартами та протоколами (у сфері 5G-зв'язку та розподілі доменних імен), процесами (у сфері хмарних обчислень), обладнанням (у сфері використання пристроїв мобільної телефонії), послугами (у сфері використання соціальних мереж та послуг електронної комерції) та інфраструктури (кабельні мережі, супутниковий зв'язок, технології « розумних міст»). Боротьба за цифровий суверенітет має глобальний характер і передбачає формування ситуативних альянсів держав для протистояння іншим союзам у кіберпросторі. Найбільш масштабним нині виступає протистояння між приватними компаніями та державами, яке набуває асиметричного характеру, оскільки кожен з учасників має свої переваги у формування ресурсів кібермогутності (приватні компанії – на рівні інноваційного науково-технологічного розвитку, а державні установи – на рівні регулювання діяльності цих компаній). Особливого значення таке протистояння набуває тоді, коли одні держави використовують вітчизняні компанії для боротьби з іншими державами (Floridi, 2020).

Важливою понятійною категорією регіональної інформаційної безпеки є поняття « інформаційної війни» , яка активно використовується у геополітичному

протистоянні між державами АТР. Так, Д. Стейн вважає, що інформаційну війну слід розглядати як конфлікт на рівні суспільства або між націями, що розгортається на стратегічному рівні, а Р. Шафранскі визначає інформаційну війну як військову діяльність, спрямована проти будь-якої системи знань чи передбачень ворога. При цьому важливою характеристикою феномену вважається трансформація іншого поняття – «простір ведення бойових», який поділяється на тактичний (операціональний) і стратегічний рівні. До того ж в рамках ведення інформаційної війни стає можливим досягнення важливих цілей національної безпеки без застосування військової сили (Stein, 1995; Szafranski, 1995). Інформаційна війна може здійснюватися або як частина більшого і повнішого набору військових дій – мережної війни чи кібервійни, або як єдина форма ведення військових дій (Szafranski, 1995).

На думку іншого відомого дослідника, М. Лібікі, поняття інформаційної війни є настільки багатогранним явищем, що говорити про його концептуальні рамки майже неможливо. Таким чином, вивчення феномену доцільно здійснювати лише через дослідження його форм (командно-адміністративна війна; розвідувальна війна; радіоелектронна війна; психологічна війна; хакерська війна; економічна інформаційна війна; кібервійна) (Libicki, 1995).

У розвиток теорії інформаційної війни на основі дослідження сучасних тенденцій інформаційного протиборства в різних країнах світу Д. Арквілла, Д. Альбертс, Б. Берковіц, Д. Гарстка, А. Ечеваррія, М. ван Кревельд, В. Лінд, Д. Ронфельдт, А. Себровскі, Е. Сміт, Г. Уілсон, Т. Хеммс, Ф. Хоффман, Д. Шміт, Ф. Штейн запропонували нові понятєво-категоріальні підходи, розгляд яких дає можливість охарактеризувати сучасні види та методи інформаційного протиборства на глобальному та регіональному рівнях. Так, «кібервійну», на думку Д. Арквілли і Д. Ронфельдта, слід тлумачити як конфлікт, пов’язаний зі сферою знання на військовому рівні, а «мережну» війну – як конфлікт низької інтенсивності за участю недержавних акторів (наприклад, терористичні угруповання або наркокартелі), пов’язаний із соціальною боротьбою (Arquilla, Ronfeldt, 1993). А. Себровскі та Д. Гарстка досліджують феномен «мережноцентрованих» війн, який вони тлумачать

як новий тип війни, що передбачає формування мережноцентрованого способу мислення та його використання у військових операціях. Впровадження мережевого принципу дозволяє швидко досягати необхідної бойової потужності завдяки взаємодії географічно розподілених сил, формування спільного усвідомлення бойового простору та реалізація спільних мережноцентрованих операцій (Cebrowski, Garstka, 1998; Alberts, Garstka and Stein, 2000). Е. Сміт пропонує у розвиток теорії мережноцентрований війн концепцію « операції із досягнення ефективності» (Smith, 2002). Така форма протиборства передбачає активне використання досягнень науки і техніки, що суттєво змінює підходи до здійснення військових операцій. Здійснення « операції із досягнення ефективності» відбувається із застосуванням потенціалу мережноцентрованих війн навіть у традиційних конфліктах задля посилення ефекту, а також супроводжується виходом за межі лише кінетичних засобів протиборства, залученням інформаційної і когнітивної сфер для створення більшого ефекту. Протиборство може вестися як у мирний час, так і під час відкритого військового протистояння, в умовах криз, конфліктів. Б. Берковіц, досліджуючи інформаційне протиборство, виокремлює чотири ключові фактори, які характеризують новий тип війни: асиметричність загроз, конкуренція в інформаційних технологіях, гонка у циклах ухвалення рішень та мережева організація (Berkowitz, 2007).

В. Лінд визначає сучасне інформаційну війну як війну «четвертого покоління», яка характеризується втратою монополії держави на саму війну, а учасниками протиборства виступають недержавні актори, терористичні і злочинні угруповання, релігійні групи та етнічні спільноти. Нове покоління війн є найбільш небезпечним, оскільки призводить до кризи легітимності держави і уможливлює вторгнення на територію іншої держави без офіційного оголошення війни (наприклад, імміграція, що руйнує систему національної безпеки держави). В таких умовах традиційні засоби ведення війни не можуть бути ефективними (Lind, 2004). М.ван Кревельд характеризує війну « четвертого покоління» як « нетринітарну» , що поєднує інформаційну війну, економічну війну та кібервійну, і характеризується як асиметричний конфлікт «низької інтенсивності». В такій війні беруть участь

різноманітні квазідержавні та недержавні актори, зокрема, приватні військові компанії, терористичні угруповання, партизанські об'єднання тощо. При цьому фактор широкого використання сучасних технологій сприяє розмиванню межі застосування військових технологій, які швидко проникають у сучасне суспільство і можуть стати доступними для використання усіма учасниками протистояння (Creveld, 2005). Т. Хеммс оцінює війну «четвертого покоління» як один з найбільших викликів для сучасної системи міжнародної безпеки, оскільки уможливлює використання усіх доступних засобів – політичних, економічних, соціальних, військових – для того, щоб переконати ворога, який ухвалює рішення, у тому, що їх стратегічні цілі недосяжні (Hammes, 2006).

Для аналізу понятєвих категорій інформаційної безпеки важливим є тлумачення поняття «гібридна війна», яка на думку Ф. Хоффмана, є таким типом конфлікту, в якому супротивник використовує унікальні комбіновані загрози, спрямовані на найбільш вразливі елементи системи національної безпеки держав. У гібридній війні можуть брати участь як держави, так й недержавні суб'єкти, а також можуть бути використані різні групи учасників (злочинні групи або терористи, повстанці, нерегулярні війська), що робить війну багатоваріативною і непередбачуваною. Важливою складовою сучасних гібридних війн є широке використання технологічних та інформаційних інновацій, що значно розширює спектр дії та руйнівний ефект гібридних загроз (Hoffman, 2009).

Іншим важливим для аналізу понятєвих категорій інформаційної безпеки є поняття «м'яка сила», яку, на думку Дж. Ная, слід тлумачити як здатність формувати привабливий образ того, хто володіє інструментами сили. Основними елементами «м'якої сили» є зовнішня політика і дипломатія, політична ідеологія, культура і цінності. За допомогою такого інструменту можна впливати на процес ухвалення рішення у сфері міжнародних відносин, досягаючи поставленої мети у сфері зовнішньої та безпекової політики без застосування «жорстких» методів примусу та нав'язування (Nye, 2004). Важливою складовою «м'якої сили» є інформаційні та технологічні переваги, які дозволяють державам не тільки досягати лідерських позицій, але й використовувати їх для формування системи так званої «

інформаційної парасолі» з метою зміцнення інтелектуального зв'язку між зовнішньої політикою та воєнною могутністю, формування альянсів та тимчасових коаліцій (Nye, 2002; Nye and Owens, 1996). «Розумна сила», на думку Дж. Ная та Р. Армітіджа, передбачає ситуативне поєднання «м'якої» і «жорсткої» сили для підвищення ефективності реалізації стратегій у міжнародних відносинах (Armitage and Nye, 2007). «Розумна сила» передбачає впровадження інтегрованої стратегії, створення ресурсної бази та набору інструментів для досягнення цілей держави, спираючись ситуативно як на «жорстку», так і на «м'яку» силу. Використання саме «розумної сили» дозволяє перетворити наявні ресурси на стратегію, що уможливлює досягнення бажаних результатів (Nye, 2011). У розвиток теорії м'якої» і «розумної» сили було також запропоновано теорію «гострої» сили, яка пов'язана із зовнішньополітичною діяльність авторитарних режимів і передбачає використання прийомів маніпулювання громадською думкою в демократичних країнах з метою підриву їх політичної системи (Nye, 2011).

Важливим для типології понятєвих категорій інформаційної безпеки є також поняття «інформаційна зброя», яку, на думку Р. Шафранскі, на відміну від традиційної (набір смертельних і несмертельних засобів ведення збройного конфлікту), можна використовувати як проти внутрішніх, так й проти зовнішніх ворогів. Інформаційна зброя є універсальною та багатоваріативною, тривалий час може залишатися непомітною, а також є значно менш витратною у порівнянні з традиційною зброєю (Szafranski, 1995). У цьому контексті доцільно звернутися ще до одного тлумачення – «перегорнутої мілітаризованої дипломатії», що передбачає використання мілітаризованих активів (тобто кіберзброї) задля доступу до необхідних ресурсів, покладаючись при цьому на діяльність дипломатів, які повинні обмежити потенційну ескалацію протистояння (Andres, 2014).

Як правило, інформаційні методи протиборства зорієнтовані на завдання школи по «критично важливій структурі» супротивника, яку доцільно тлумачити як інфраструктури, що мають критичне значення для підтримки життєво важливих суспільних функцій, безпеки, економічного чи соціального добробуту людей, а порушення або знищення яких може мати серйозні наслідки для подальшого

розвитку суспільства в цілому. Тоді самий «захист критичної інформаційної інфраструктури» можна розглядати як діяльність, спрямовану на захист ресурсів (реальних та віртуальних), систем та їх функціонування, які є життєво важливими для країн (наприклад, національна система безпеки та оборони, банківські структури та фінанси, інформаційні та телекомунікаційні структури, сфера енергетики, транспортні комунікації, система водопостачання, сфера надання медичних послуг, урядові комунікації, аварійні служби та система продуктової безпеки) і руйнування або виведення з ладу яких може мати негативний вплив на національну економічну потужність, імідж держави, систему національної безпеки та оборони, функціонування урядових систем тощо.

Ще однією понятійною категорією у сфері інформаційної безпеки є поняття «інформаційні загрози» та «кіберзагрози». Як й у випадку з співвідношенням понять «інформаційна безпека» та «кібербезпека», у співставленні тлумачення термінів також спостерігається певна синонімія як на рівні міжнародних організацій, так і на рівні національних держав. Наприклад, в Угоді між урядами держав-членів Шанхайської організації співробітництва про співпрацю в сфері забезпечення міжнародної інформаційної безпеки (Єкатеринбург, 2009 р.) вживається термін « загроза інформаційній безпеці», яку визначено як сукупність чинників, що створюють небезпеку для особистості, суспільства, держави та їх інтересів в інформаційному просторі. У Додатку до документу міститься Перелік основних видів загроз у сфері міжнародної інформаційної безпеки, їх джерел та ознак. Так, до основних загроз віднесено: 1) розробка та застосування інформаційної зброї, підготовка та ведення інформаційної війни; 2) інформаційний тероризм; 3) інформаційна злочинність; 4) використання інформаційного домінування для ущемлення інтересів і безпеки інших держав; 5) поширення інформації, що завдає шкоду суспільно-політичній та соціально-економічній системам, духовному, моральному та культурному середовищу інших країн; 6) загрози безпечному, стабільному функціонуванню глобальних і національних інформаційних інфраструктур, що мають природний та/або техногенний характер (SCO, 2009). Отже, «інформаційні загрози» розглядаються в рамках діяльності ШОС у більш

широкому значення, ніж кіберзагрози. В рамках ООН та її спеціалізованих установ переважно використовується термін « кіберзагрози» , які визначаються як шкідливі дії, спрямовані на користувачів інформаційних систем (через фішинг, крадіжку особистих даних, схеми «людина посередині» тощо) або на інфраструктуру (зловмисне програмне забезпечення, відмова в обслуговувані). Основними видами кіберзагроз визначено кіберзлочинність, кібертероризм, кібершпигунство та кібератаки. Як зазначають експерти, визначення поняття кіберзагроз більше відповідає сучасному ландшафту загроз для системи міжнародної безпеки (CCDCOE, 2021).

Висновки до першого розділу

Сучасна парадигма міжнародної безпеки формується під впливом прискорених процесів інформаційного і науково-технологічного розвитку. Впровадження технологій Четвертої індустріальної революції не тільки відкриває нові можливості для поступального розвитку глобального суспільства, але й призводить до виникнення нових викликів і загроз, на появу яких сучасна система підтримання миру і безпеки не може адекватно відповідати. Це викликало потребу переглянути діючі норми міжнародного права у сфері регулювання використання досягнень науки і технологій в контексті міжнародної безпеки та впровадити нові механізми забезпечення відповідальної поведінки держав в кіберпросторі. Водночас самі держави, прагнуть використати високі технології для посилення власного військового потенціалу з метою обстоювання національних інтересів. Найбільш серйозним викликом для сучасної системи міжнародного миру і безпеки нині виступає проблема використання кіберпростору як нового виміру геополітичного протистояння.

Трансформація парадигми міжнародної безпеки в умовах швидкоплинних технологічних зрушень обумовила потребу теоретичного переосмислення питань міжнародної безпеки, еволюції форм і методів ведення війни, появи нових засобів протиборства, балансу сил та політики стримування. Це призвело до виникнення

цілої низки досліджень з питань інформаційної геополітики та формування кібервестфальської системи, формування цифрового суверенітету, трансформації фактору сили у міжнародних відносинах, формування інформаційного потенціалу та кібермогутності держав, еволюції феномену війни та появи нових форм протиборства – інформаційної війни, кібервійни, когнітивної війни, гібридної війни, війни четвертого покоління, мережевої війни і мережноцентрованої війни, тринітарної війни тощо, нових форм і методів протиборства, появи інформаційної зброї та «перегорнутої мілітаризованої дипломатії». Як свідчить аналіз теоретичних і концептуальних розробок зарубіжних авторів, проблема інформаційної безпеки нині є надзвичайно актуальною, що обумовлює постійний інтерес науковців до неї. Питанню інформаційної безпеки присвідчено також значну кількість теоретичних і прикладних досліджень українських фахівців, що свідчить про зростання актуальності тематики й для України.

Дослідження тенденцій розвитку феномену інформаційної безпеки обумовило звернення до його базових понятєво-категоріальних характеристик. Так, у роботі розглянуто поняття, як «міжнародна інформаційна безпека», «кібербезпека», «кібердипломатія», «кібероборона», «кібермогутність», «цифровий суверенітет», «інформаційна війна», «кібервійна», «мережна війна», «мережноцентрована війна», «війна четвертого покоління», «гібридна війна», «перегорнута мілітаризована дипломатія» та ін., аналіз яких дозволяє визначити сучасні тенденції розвитку феномену інформаційної безпеки, які потребують відповідної систематизації та переосмислення із врахуванням подальшого інформаційного та науково-технологічного розвитку і появи нових викликів і загроз для системи підтримання міжнародного миру і безпеки.

РОЗДІЛ 2
ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ РЕГІОНАЛЬНИХ ІНСТИТУТІВ АТР

2.1. Інформаційна складова сучасної архітектури безпеки АТР

В умовах бурхливого інформаційного та науково-технологічного розвитку країн АТР питання інформаційної безпеки набувають визначального значення, оскільки суттєво впливають на трансформацію регіональної архітектури безпеки. Геополітичні зміни, що відбулися у регіоні та світі з кінця XX ст., поставили на порядок денний питання трансформації моделей співпраці країн регіону у сфері безпеки, що було обумовлено пошуком нових, більш ефективних стратегій, які б відображали реалії сучасної системи міжнародних відносин в регіоні. Як зазначають експерти, основними характеристиками регіональної архітектури безпеки є наявність значної кількості довготривалих конфліктів, наявність територіальних суперечностей та претензій між різними державами регіону, політико-ідеологічні суперечки між провідними регіональними гравцями та особлива роль США у підтриманні регіональної архітектури безпеки, в першу чергу, шляхом створення двосторонніх альянсів та розвитку стратегічного двостороннього партнерства. В таких умовах інформаційний та науково-технологічний фактори виступають і як каталізатор існуючих проблем, що значно ускладнює процес вироблення ефективних механізмів мирного врегулювання суперечностей та формування системи безпеки регіону, і як інноваційний механізм, який дозволяє поєднати зусилля акторів із створення більш безпечного регіонального інформаційного простору та реалізовувати стратегії розбудови електронного державного урядування, розвитку інформаційної економіки та електронного бізнесу, які є важливою передумовою для подальшого економічного зростання регіону.

Сучасна архітектура безпеки АТР формувалася в умовах тривалого економічного зростання, у тому числі, за рахунок активного впровадження сучасних інформаційно-комунікаційних технологій, що призвело до зменшення масштабів

бідності та зростання торгівельної інтеграції. Саме масштаби позитивних зрушень дозволили експертам стверджувати, що держави регіону будуть дедалі активніше формувати систему регіональної безпеки і намагатися уникати ескалації конфліктів. Водночас, як показує практика, в регіоні ускладнюються умови для забезпечення безпеки, що суттєво збільшує ризик загострення вже існуючих конфліктів або появи нових. Таким чином перед державами регіону постає питання вироблення більш ефективних механізмів забезпечення безпеки, які б, з одного боку, дозволили б запобігти виникненню нових конфліктів або загострення старих, а з другого, підготуватися до нового типу загроз стратегічній стабільності, виникнення яких тісно пов'язане із інформаційних та науково-технологічним прогресом (Asia Society Policy Institute, 2017). Архітектура безпеки АТР базується на багаторівневій мережі взаємовідносин, діяльності політичних інститутів та різноманітних форумів, за допомогою яких держави виробляють спільні підходи до розбудови системи безпеки, загальні правові норми, вживають заходи для впровадження міжнародних стандартів у сфері безпеки, у тому числі, у сфері інформаційної безпеки.

На думку експертів, однією з основних характеристик сучасної азійсько-тихоокеанської регіональної системи безпеки є домінування концепту Realpolitik у взаємовідносинах між державами регіону, зокрема, у питаннях регіональної інтеграції, оскільки система безпеки АТР побудована переважно на державо-центристському підході і дестабілізується давніми територіальними суперечками та політикою великих держав. Тому двостороннє співробітництво, стратегічне партнерство у найбільш важливих питаннях безпеки та використання неформальних комунікацій, з одного боку, уможливлює вирішення складних проблем регіональної безпеки, а з другого, робить держави більш чутливими до політичних викликів (Asia Society Policy Institute, 2017).

Важливою характерною рисою сучасної архітектури безпеки АТР виступає дестабілізація регіонального порядку внаслідок постійної напруги у відносинах між США та Китаєм. Із зростанням глобальної економічної потуги КНР виникає нова динаміка, в якій азійські країни вбачають потенційну небезпеку зростання розходжень між своїми безпековими інтересами та економічними імперативами.

Тобто, з одного боку, тісна співпраця зі США дає більшу впевненість у можливостях національної системи безпеки та оборони, але, з другого, постійно зростає економічна залежність від Китаю. Така ситуація може поставити країни АТР перед складним вибором пріоритетів співробітництва (Asia Society Policy Institute, 2017). Особливого значення це питання набуває у контексті поширення практики науково-технологічного трансферу та зростання рівня технологічної залежності країн регіону від інноваційних розробок США та Європи. Водночас, спостерігається й інша тенденція – інформаційно-технологічна експансія Китаю на сусідні країни регіону, що суттєво впливає на збільшення залежності від китайських розробок і технологій.

У цьому контексті вкрай важливим є розширення регіональної системи безпеки АТР завдяки концепту Індо-Тихоокеанського регіону. Цей елемент міжнародно-політичного дискурсу зазвичай оцінюється як нова стратегія, що повинна відобразити зростання та взаємопроникнення сфер впливу Китаю та Індії. Розробка цього політико-безпекового концепту найбільш відповідає геополітичним та геоекономічним інтересам Індії, США, Австралії та Японії. Наприклад, для Індії – це можливість легітимізувати зростання стратегічних інтересів держави у Східній Азії та західній частині Тихого океану. Важливу роль у цьому відіграють демографічний та науково-технологічний фактори, які дозволяють суттєво збільшити потенціал Індії у цьому двосторонньому суперництві. Для США просування концепту Індо-Тихоокеанського регіону уможливлює реалізацію політики стримування впливу КНР у Східній Азії. Зокрема, завдяки виведенню американських стратегічних інтересів за межі східноазійського узбережжя у бік Індійського океану, поступово «розмивається» вплив Китаю і вводяться нові геополітичні гравці. Так, у Стратегії національної оборони США 2018 р. (National Defense Strategy of United States of America, 2018) підкреслювалася необхідність «зміцнювати союзи та залучати нових партнерів», а також прагнення трансформувати архітектуру безпеки, щоб вона функціонувала подібно мережі, яка здатна ефективно стримувати агресію, підтримувати стабільність та забезпечувати вільний доступ до спільних ресурсів, задля збереження вільної і відкритої міжнародної системи. У своєму зверненні до слухачів Військово-морського коледжу

27 серпня 2019 р. тодішній міністр оборони США Марк Еспер заявив, що Індо-Тихоокеанський регіон є «пріоритетним театром воєнних дій». Союзники Америки в регіоні (Австралія, Нова Зеландія, Японія, Південна Корея, Монголія) постійно висловлюють занепокоєння щодо зростання ролі Китаю у регіоні, особливо в контексті реалізації концепції «Один пояс, один шлях». Для підтримки союзників потрібно, щоб США були присутні в ключових точках системи безпеки регіону (Secretary of Defense Esper Tells U.S. Naval War College Students His Focus is Great-Power Competition, 2019). Згодом, в іншому концептуальному документі – «Вільний та відкритий Індо-Тихоокеанський регіон» (2019 рр.), – було зазначено, що політика США у регіоні має бути спрямована на впровадження ефективних механізмів стримування зростаючої ролі Китаю, що свідчить про загострення стратегічного суперництва між Вашингтоном та Пекіном (A Free And Open Indo-Pacific, 2019). Окрім цього, у формування даного концепту зацікавлені й провідні країни регіону, оскільки Австралія прагне позбутися регіональної ідентичності периферійної країни та перетворитися на активного актора регіональної системи безпека, а Японія – реалізувати концепцію «стратегічного діаманту».

Таким чином, взаємодія США, Японії, Австралії та Індії в рамках Чотиристороннього діалогу з питань безпеки (QUAD), який виник ще у 2004 р. для подолання наслідків стихійних лих в Індійському океані, нині зорієнтована на зміцнення системи регіональної безпеки шляхом розвитку партнерських відносин на основі спільних цінностей та інтересів, зокрема, поваги до територіальної цілісності, суверенітету, мирного врегулювання територіальних конфліктів, верховенства права тощо (Орлик, 2021). Водночас, як зазначають експерти, цей альянс передусім слід розглядати як геополітичний інструмент стримування Китаю. По суті, йдеться про одним з головних регіональних проектів Вашингтону із створення так званого «азійського НАТО», що може ще більш загострити боротьбу за лідерство в регіоні між КНР та США. Слід зазначити, що найбільш зацікавленими в утворенні такого формату співпраці є Японія та Австралія, які виступають військово-політичними союзниками Америки, натомість Індія залишається лише партнером в альянсі,

незважаючи на розширення американо-індійського військового та військово-технічного співробітництва в останні роки.

Підкреслимо, що останні два роки в рамках QUAD набирає обертів новий напрям діяльності – партнерство учасників задля формування власної системи кібербезпеки в умовах зростання взаємозалежності держав Індо-Тихоокеанського регіону у соціально-економічній, гуманітарній та безпековій сферах. Так, у вересні 2021 р. лідери країн Чотиристороннього діалогу з питань безпеки оголосили про новий напрям співробітництва – забезпечення кібербезпеки. Країни домовилися про створення спеціальної групи експертів, яка опікуватиметься проблемами розробки програмного забезпечення у сфері кібербезпеки, вироблення загальних принципів і стандартів у цій сфері, зміцнення цифрової інфраструктури, особливо у контексті подальшого розвитку якості зв'язку і появи мереж 5G, а також забезпечення обміну необхідною інформацією між Групами швидкого реагування на кіберінциденти (CERT) країн QUAD. (The countries of the QUAD four will start cooperating in the cybersphere, 2021).

Діяльність держав-учасників альянсу в рамках проголошеного Партнерства у сфері кібербезпеки має на меті сформувати високий потенціал стійкості інформаційної інфраструктури з метою усунення вразливостей для кібербезпеки та вироблення ефективних механізмів протидії кіберзагрозам, зосередившись на захисті критичної інфраструктури (під керівництвом Австралії), стійкості та безпеці ланцюга постачання (під керівництвом Індії), розвитку кадрового потенціалу (під керівництвом Японії) та виробленні і впровадженні стандартів безпеки програмного забезпечення (під керівництвом США) (Patil, 2022). Основними принципами проголошеного Партнерства стали: посилення співпраці у сфері кібербезпеки критичної інфраструктури, управління ризиками, безпека програмного забезпечення, підготовка кадрового потенціалу; організація ефективної співпраці між усіма зацікавленими сторонами у сфері кібербезпеки критичної інфраструктури, формування системи інформаційних обмінів між усіма задіяними у формуванні кібербезпеки структурами (державними, приватними) для вчасного інформування про появу нових кіберзагроз, здійснення кібератак та інших небезпек; поглиблення

співпраці у сфері програмного забезпечення з метою посилення кібербезпеки регіону тощо (Quad Cybersecurity Partnership: Joint Principles, 2022).

Прогрес QUAD у досягненні пріоритетів стратегії кібербезпеки після саміту у Вашингтоні у вересні 2021 р. був визнаний як експертами, так й самими країнами, які спільно пообіцяли «сприяти державно-приватному партнерству» та продемонструвати вже у наступному 2022 р. значні досягнення у сфері кібербезпеки. Тоді ж була запущена робота Quad Senior Cyber Group. Під час зустрічі міністрів закордонних справ у лютому 2022 р. члени «четвірки» підтвердили свою підтримку стратегії «зміцнення стійкості та протидії дезінформації», а також схвалили стратегію допомоги індійсько-тихоокеанським партнерам у протидії різним формам кіберзлочинності.

Згодом, вже у березні 2022 р. відбулася зустріч експертів, на якій обговорили стратегії покращення кібербезпеки в умовах подальшої цифровізації світу та виникнення все більш складних кіберзагроз. Оцінка ініціатив QUAD у сфері кібербезпеки вказує на те, що вони розроблені передусім з урахуванням кіберзагроз з боку Китаю, а стратегія, спрямована на формування «кіберстійкості», а не на «наступальних кіберможливостях» була визначена як більш надійний спосіб вирішення широко кола проблем кібербезпеки в Індо-Тихоокеанському регіоні. Показовими в цьому контексті є проблеми безпеки ланцюгів постачання критичних технологій, зокрема, напівпровідників, виробництво яких залежить від рідкоземельних елементів Китаю, та диверсифікації постачальників послуг 5G-зв’язку, що обумовлено постійним зростанням тиску з боку китайських телекомунікаційних компаній Huawei та ZTE (Patil, 2022).

На зустрічі лідерів «четвірки» у вересні 2021 р. також було розроблено технологічний порядок денний. Держави-учасниці наголосили, що і надалі будуть продовжувати формувати відкриту, доступну та безпечну технологічну екосистему, що базується на спільних демократичних цінностях та повазі до універсальних прав людини. Просуваючи цей порядок денний, країни «четвірки» у вересні 2021 р. випустили заяву про принципи проектування, розробки, управління та використання технологій, які стануть основою для формування як в регіоні, так й за його межами

відповідальних, відкритих і високих стандартів безпеки інновацій. Ключовими ідеями стали: підтримка загальнолюдських цінностей; формування довіри та стійкості технологічної екосистеми; сприяння прозорій конкуренції та міжнародному співробітництву для просування передових досягнень науки та технологій. Співпраця держав у сфері розробки інноваційних критично важливих технологій може стати основою для подальшої реалізації стратегії безпеки Індо-Тихоокеанського регіону. При цьому зусилля QUAD будуть зосереджені на таких пріоритетних напрямах: розвиток технологій 5G-зв'язку (у тому числі із застосуванням технології Open RAN), розвиток технологій штучного інтелекту, а також розвиток біотехнологій та генної інженерії (Rajagopalan, 2022).

Важливою характеристикою архітектури регіональної безпеки АТР є система альянсів зі США, яка утворила своєрідну «віялову» структуру, що сходилася у «хабі» стратегічного співробітництва з американською державою. Така система співіснує з регіональними інститутами, що зростають та зміцнюються, зокрема, в рамках поглиблення співробітництва між країнами, зорієнтованими на АСЕАН або на утворення неформальних міні-коаліцій. Така вільна архітектура надала країнам певні можливості обирати найбільш відповідний їх цілям та інтересам спосіб вирішення проблеми. Водночас, це не дозволило досягнути більш стійкого регіонального консенсусу щодо норм і правил взаємодії, дозволяючи країнам самостійно визначати їх, відповідно до власних інтересів (Asia Society Policy Institute, 2017). Показовим у цьому контексті є двостороннє співробітництво між США та Японією, у тому числі, у сфері кібербезпеки (Сябро, 2019b).

Ключову роль у системі регіональної безпеки АТР відіграють регіональні інститути, до пріоритетів діяльності яких нині увійшли питання інформаційної безпеки, що розглядаються як фундаментальні, оскільки впливають на подальший поступальний розвиток регіону в цілому. Наприклад, АСЕАН виступає своєрідною платформою для вироблення спільних підходів до вирішення проблем у сфері кібербезпеки. Але, незважаючи на достатньо ефективну діяльність держав-учасниць альянсу, залишається проблема існування напруженості між її учасниками. Так, у системі, де домінує політика великих держав, саме цей регіональний інститут дав

право голосу невеликим державам та можливість впливати на формування порядку денного діяльності альянсу. Водночас підхід АСЕАН, заснований на консенсусі, останнім часом зазнає потужних впливів як з середини організації, так і ззовні. Отже, виникає суперечлива тенденція: великі держави намагаються використати АСЕАН для ствердження власних лідерських позицій, і «невеликі» та «середні» держави найчастіше виступають з ініціативами із зміцнення інститутів безпеки в Азії, сподіваючись на те, що вони дозволять об'єднати їх зусилля і можливості у виробленні консенсусу та спільного бачення шляхів вирішення проблем у сфері безпеки. Тому основним завданням Альянсу у найближчий перспективі є відновлення внутрішньої єдності та стратегічної незалежності, щоб зміцнити його здатність і надалі відігравати провідну роль у регіоні, який дедалі більше поляризується (Asia Society Policy Institute, 2017).

Важливим чинником формування сучасної архітектури безпеки виступає зростання стратегічної конкуренції між основними гравцями в регіоні (Asia Society Policy Institute, 2017). Зокрема, одним з найбільш динамічних є підйом Китаю, який намагається постійно використати стратегічні переваги для збільшення тиску на інші держави регіону, що неоднозначно сприймається і часто визначається як нова форма експансії – економічна чи технологічна – і призводить до зростання напруженості у двосторонніх та багатосторонніх відносинах. Наприклад, ініціатива «Один пояс, один шлях» оцінюється американськими експертами як інструмент економічної експансії китайських приватних і державних компаній, що дає можливість КНР посилити свою роль у вирішенні питань не тільки регіональної, але й глобальної безпеки (Asia Society Policy Institute, 2017). Політика Китаю, спрямована на розширення участі держави в різноманітних інвестиційних проектах в різних сферах і різних країнах, призводить до зростання занепокоєння з боку провідних акторів міжнародних відносин, зокрема, США, які вбачають в такій політиці спробу створити систему регіонального і глобального геоекономічного впливу КНР, що може негативно відбитися на інтересах як самих західних країн, так й їх союзників в АТР – Японії та Південній Кореї. Як зазначається у колективній доповіді Центру нової американської безпеки «Відповідаючи на китайський виклик.

Оновлення американської конкурентоздатності в Індо-Тихоокеанському регіоні» (2020), така політика Китаю може призвести до ерозії національного суверенітету держав регіону, якщо за умовами договорів про співпрацю (про пайову участь, довгострокову оренду, або про довгострокову оренду) Пекін отримує контроль над важливими національними об'єктами інфраструктури або стратегічними ресурсами чи покладами. Небезпечним стає узалежнення національних телекомунікаційних мереж від китайських технологій, оскільки вони можуть бути використані для здійснення шпигунської діяльності або атаки хакерів на критично важливі елементи інфраструктури (Ratner, 2020).

Отже, суттєвим чинником формування нової архітектури безпеки регіону виступає бурхливий інформаційний та науково-технологічний розвиток, що обумовило загострення традиційних викликів і загроз, а також появу нових, нетрадиційних, високотехнологічних, які суттєво впливають на подальший поступальний розвиток усіх держав регіону (Сябро, 2021в).

Як свідчать чисельні аналітичні дослідження, країни регіону не тільки мають значні досягнення у сфері науки і технологій, але й активно їх впроваджують у всі сфери життєдіяльності суспільства. Так, у рейтингу «Індексу мережевої готовності 2020. Прискорення цифрової трансформації у світовій економіці після COVID», країни АТР хоча і посідають різні позиції, але відрізняються постійною динамікою зростання показників. Так, до переліку країн-світових лідерів за рівнем цифрової і мережевої готовності входять провідні країни АТР – Сінгапур (3), Австралія (12), Південна Корея (14), Японія (15), Нова Зеландія (16), Гонконг/Китай (22), Малайзія (34) і Китай (40), які відповідно є лідерами і на рівні регіону (The Network Readiness Index, 2020). За даними іншого аналітичного дослідження – Digital 2021: Global Overview Report 2021 у Сінгапурі станом на початок 2021 року 5,29 млн. осіб (90 % населення) є користувачами інтернету, з них 4,96 млн. (84,4 % населення) використовували різні соціальні мережі. Незважаючи на незначне падіння показників користувачів мобільними телефонами, рівень проникнення мобільної телефонії залишається достатньо високим і становить 145,5 % від загальної кількості населення. В Японії нині 117,4 млн. (93 %) населення користується інтернетом, 3/4 з

яких активно використовують різноманітні соцмережі, постійно зростає кількість користувачів мобільних гаджетів, а отже й мобільного інтернету. На початку 2021 р. у Південній Кореї користувачами мережі Інтернет були 97 % усього населення (показники зросли на 539 тис. у порівнянні з даними за 2020 р.), зросла кількість користувачів соцмережами до 89,3 % від усього населення та кількість користувачів послуг мобільної телефонії до 118,3 % від загальної кількості населення (Digital 2021: Global Overview Report, 2021).

Кількість користувачів інтернетом продовжує зростати й у Китаї. Нині цей показник становить 939,8 млн.осіб. (або 65,2 % загальної кількості населення). У період з січня 2020 р. до січня 2021 р. показник користувачів соцмереж збільшився на 110 млн. до 930,8 млн. осіб (64,6 % від загальної кількості населення держави), а користувачів мобільними телефонами – на 8 млн. і становить 1,61 млрд. (тобто 111,8 % усього населення). В Індії також фіксується постійне збільшення показників користувачів інтернетом, кількість яких зросла на 47 млн. за останній рік і досягла 624 млн.осіб (або 45 % усього населення), користувачів соціальними медіа (нині зросла на 78 млн. і нараховує 448 млн, що становить 32,3 % населення) та мобільною телефонією (1,10 млрд. або 79 % населення у 2021 р.) (Digital 2021: Global Overview Report, 2021). Країни АТР також включилися у процес модернізації мереж зв’язку, зокрема, у розгортання 5G-мереж, що суттєво розширить можливості використання онлайн-сервісів. Так, серед країн-лідерів опинилися Південна Корея, Японія, Китай, Сінгапур, Таїланд, Австралія і Нова Зеландія (Fogg, 2021).

Показовими для аналізу інформаційного та науково-технологічного розвитку регіону є також данні щодо інноваційного розвитку. Так, згідно з «Глобальним індексом інновацій-2020», країни АТР або увійшли до переліку країн-лідерів інноваційного розвитку, зокрема, Сінгапур (8-ма позиція у рейтингу) і Південна Корея (10), Китай (14) і Японія (16) , Австралія (23) і Нова Зеландія (26), або мають значний потенціал інноваційного розвитку, наприклад, Малайзія, Індія, Філіппіни тощо (World Intellectual Property Organization, 2020). Таким чином, розвиток інноваційного потенціалу держав регіону, з одного боку, стимулює активне впровадження досягнень у сфери життєдіяльності людини, а з другого, – можуть

стати основою для подальшої модернізації військового потенціалу, що містить загрозу ескалації існуючих конфліктів та новий тип гонки озброєнь – високотехнологічних і наукомістких.

Одним з найбільш вагомих чинників, що впливає на зміну архітектури регіональної безпеки, є стрімка політична та економічна трансформація, обумовлена передусім технологічним прогресом. Згідно з аналітичними дослідженнями Департаменту ООН з економічних і соціальних питань «Дослідження ООН: Електронний уряд 2020», країни АТР входять до групи лідерів розбудови електронного уряду та розвитку системи надання електронних послуг. Так, у доповіді всі країни поділені на 4 групи, які відповідають рівням розвитку електронного уряду – дуже високий, високий, середній та низький. Показовим є те, що провідні країни АТР входять переважно до першої і другої групи і посідають провідні позиції у глобальному рейтингу. Так, Південна Корея є світовим лідером у наданні онлайн-послуг, за нею розміщуються Сінгапур та Японія (United Nations, 2020). Високий рівень розвитку електронного уряду також відзначається на регіональному рівні, де країни Азії сукупно посіли друге місце після європейського регіону (United Nations, 2020).

Наприклад, Південна Корея є регіональним і світовим лідером у наданні послуг електронного уряду. Як зазначається у Генеральному плані розвитку електронного уряду Республіки Корея, держава орієнтується на подальшу розбудову «розумного» уряду, що базується на широкому впровадженню досягнень науки і техніки у систему державного управління, зокрема, штучного інтелекту, що уможливить охоплення різноманітними онлайн-послугами всіх груп населення. Стратегічні пріоритети «розумного» уряду відображені також у Стратегії сприяння економіки даних та штучного інтелекту, спрямованої на розбудову стійкої цифрової економіки, Генеральному плані з розвитку сфери блокчейн, Стратегії впровадження «розумного» міста та Новій промислово-технологічній дорожній карті, впровадження яких сприяє прискоренню розвитку нових технологій в інтересах суспільства та покращення електронного державного управління. Реалізація зазначених ініціатив здійснюється на основі створення різноманітних цифрових

платформ, зокрема, платформа для електронної участі (e-People), відкритих даних (data.go.kr), електронних закупівель (KONEPS), а також розвитку правової бази, спрямованої на підвищення стандартів захисту персональних даних та інформації, системи цифрової ідентифікації особи, а також формування ефективних механізмів забезпечення цифрової безпеки держави, що є вкрай важливим для подальшого розвитку стратегій у сфері електронного державного управління (United Nations, 2020).

Сінгапур з 2014 р. почав впроваджувати ініціативу «Розумна» нація, важливою складовою якої виступає розбудова електронного уряду. У розвиток ініціативи у 2018 р. було розроблено Проект електронного уряду для покращення використання даних та впровадження нових технологій з метою розбудови цифрової економіки та цифрового суспільства. Для досягнення поставлених цілей було створено цифрові платформи, зокрема, портал «єдиного вікна» (Gov.sg) для спрощення доступу до ресурсів, що забезпечують електронну участь (reach.gov.sg), електронні послуги (citizenconnectcentre.sg), доступ до відкритих даних (data.gov.sg) та прозорість державних закупівель (gebiz.gov.sg) (United Nations, 2020).

В Японії План переходу на цифрові технології зосереджений навколо використання нових технологій і розвитку людських ресурсів, щоб удосконалювати систему державного управління, підтримувати розвиток електронного бізнесу та підвищувати рівень життя громадян. Для цього у державі створено центральний портал електронного уряду (e-gov.go.jp), додаткові цифрові платформи електронного урядування для електронної участі (e-Testimony), доступу до відкритих даних (data.go.jp) та державних закупівель (geps.go.jp). Відповідно розроблено й законодавство у сфері захисту інформації і даних (United Nations, 2020).

Китай також став країною, яка продемонструвала значні досягнення у реалізації стратегії електронного державного урядування і увійшла до групи країн з дуже високим рівнем розвитку електронної держави. Китайський уряд намагається активно використовувати наукові і технологічні досягнення для підвищення рівня інноваційного потенціалу держави, який сприяє зростанню можливостей впливати

на політичний, економічний та військовий розвиток країн регіону та за його межами. Нині Китай активно реалізує стратегії електронної держави, « розумних» міст та цифрової економіки, сприяє широкому впровадженню технологій штучного інтелекту, Big Data, технологій блокчейн, мереж 5G-зв'язку тощо. Уряд також намагається максимально використовувати соціальні платформи та цифрові медіа для покращення взаємодії між урядовими структурами, бізнесом та населенням (наприклад, WeChat та Alipay) (United Nations, 2020).

Отже, стрімке впровадження сучасних технологій у всі сфери життєдіяльності суспільства ставить на порядок денний питання про безпеку мереж і даних, що стають об'єктами ворожих чи протиправних дій, наслідки яких можуть спостерігатися як в самих країнах-об'єктах атак, так й за їх межами завдяки інтеграції до глобальної інформаційної інфраструктури. Отже, високі темпи інформатизації робить держави АТР вразливими для економічно та політично мотивованих атак з боку інших держав, різноманітних злочинних та терористичних угруповань або окремо діючих осіб, що суттєво актуалізує питання інформаційної безпеки в регіоні.

Як показано у «Рейтингу країн світу за рівнем вразливості у сфері кібербезпеки 2020», у новій пост-COVID-19 реальності необхідність розробки і реалізації стратегії кібербезпеки для забезпечення безпеки цифрової інфраструктури та інформаційного простору постала як вкрай актуальна проблема. У дослідженні зазначається, що сучасні кіберзагрози можуть бути надзвичайно різноманітними – від атак на конкретні пристрої, націлених на отримання несанкціонованого доступу, крадіжки даних і вимагання грошей шляхом блокування доступу до файлів або комп'ютерних систем, до атак на хмарну інфраструктуру, кінцева мета яких – компрометація віртуальних машин і використання їх в якості зброї (Cybersecurity Exposure Index, 2020). Отже, згідно з дослідженням, на Азійсько-Тихоокеанський регіон припадає 60 % країн світу з надзвичайно високим рівнем вразливості кіберпростору та інформаційної інфраструктури, з яких 40 % – з високим і надзвичайно високим рівнем вразливості, а отже з найнижчим рівнем кіберзахищеності. Серед країн регіону, які все ж мають достатньо високий рівень

кібербезпеки, були названі Австралія, Японія, Нова Зеландія, Сінгапур. (Cybersecurity Exposure Index, 2020; Frisby, 2020)

Представлені аналітичні дані свідчать про зростання небезпеки протиправного використання сучасних досягнень науки і технологій в умовах дедалі більшого узалежнення ефективності реалізації стратегій модернізації економіки та розбудови електронного урядування держав регіону від гарантій безпеки мереж і технологій. Враховуючи високі показники динаміки проникнення технологій, з одного боку, та вразливості кіберпростору, з другого, виникає обґрунтоване занепокоєння з боку держав та регіональних інститутів щодо розширення практики використання методів інформаційного протиборства для досягнення геополітичних та геоекономічних переваг на регіональному та глобальному рівнях.

Наприклад, поступове наближення регіонального військового балансу до показників паритету ставить під загрозу можливості США стримувати китайську загрозу і допомагати країнам-союзникам реалізувати стратегії національної безпеки. Нині ж Китай готовий обійти США за ВВП, одночасно прагнучі отримати технологічну перевагу у таких галузях, як штучний інтелект, квантові обчислення та геноміка (Ratner, 2020). Це цілком відповідає амбіційній стратегії, проголошеній під час XIX з'їзду Комуністичної партії, – перетворити Китай на світового лідера з погляду сукупної національної потуги і міжнародного впливу вже до середини XXI ст. Пріоритетними сферами діяльності для досягнення поставлених цілей було визначено технологічний розвиток і модернізація збройних сил (Saran, 2020).

В цьому контексті показовою є діяльність дипломатів з науки і технологій (S&T diplomats), які слідкують за науковими і технологічними досягненнями у країнах перебування, визначають інвестиційні можливості для китайських компаній, виступають посередниками у купівлі технологій, яких потребує держава. Дипломати з науки і технологій виступають складовою системи передачі китайських технологій, а також здійснюють постійних моніторинг наукових відкриттів та появи технологічних новацій, які можуть становити інтерес для уряду КНР. Понад 140 китайських дипломатів з науки і технологій працює у 52 кранах світу. На думку експертів Центру безпеки і нових технологій Джорджтаунського університету,

найбільшими « донорами» нових технологій нині виступають США, Велика Британія, Японія та Росія, а найбільш привабливим сферами є біофарма та медичне обладнання, інформаційні технології та нове матеріалознавство (Fedasiuk, 2021).

Отже, інформаційний та науково-технологічний розвиток нині виступає важливим чинником геополітичне і геоекономічне протистояння Китаю зі США, що також впливає на архітектуру безпеки АТР. Наприклад, показовою є реакція США на діяльність китайської компанії Huawei, яка була і все ще залишається одним з лідерів у сфері інформаційних технологій, зокрема, у виробленні обладнання для електронної ідентифікації, «розумних міст», мобільних пристроїв (нині посідає друге місце за показником продажів смартфонів у світі після Samsung), устаткування для хмарних сервісів, а також бере активну участь у розгортанні мереж п’ятого покоління. Звинувачення у промисловому шпигунстві компанії розпочалися ще у 2003 р., коли компанія Cisco звернулася до суду з позивом щодо порушення своїх патентів та незаконного копіювання операційної системи Cisco IOS, вимагаючи припинення використання її інтелектуальної власності та відшкодування збитків, отриманих внаслідок протиправних дій.

У 2008 р. уряд США звинуватив китайські компанії Huawei та ZTE у здійсненні шпигунської діяльності у військовій та військово-промисловій сферах, що загрожує системі національної безпеки Америки. Водночас це не завадило компанії Huawei вийти на американський ринок смартфонів та почати реалізовувати спільні проекти з американськими компаніями, зокрема, з Google. Ситуація кардинально змінилася у 2018 р., коли Пентагон заборонив військовим купувати засоби зв’язку виробництва Huawei та ZTE, а Конгрес звернувся з вимогою до Google припинити співпрацю з компанією Huawei, яку звинуватили у здійсненні крадіжки інформації державного призначення. Згодом від співробітництва з компанією відмовилися й інші країни – Австралія, Японія та Велика Британія, використовуючи безпекові аргументи. У тому ж році у Канаді була заарештована фінансова директорка Huawei Мен Ваньчжоу, якій вже у США пред’явили звинувачення у співробітництві з Іраном, незважаючи на ембарго на постачання телекомунікаційного обладнання. Отже, США включили до вимірів торгівельної

війни с КНР високотехнологічний сектор, і якщо за часів адміністрації Б. Обами США пасивно реагували на факти мілітаризації Південно-Китайського моря та випадки використання кібершпигунства, то за Д. Трампа ситуація значно загострилася.

Намагаючись протистояти високотехнологічним амбіціям Китаю, адміністрація Д. Трампа розпочала активний наступ і заборонила використання телекомунікаційного обладнання компанії Huawei, яке становить загрозу для національної безпеки держави, а також ввела обмеження на використання електронних компонентів та запчастин у американських компаніях без узгодження оборудок з представниками уряду США. Така політика суттєво вплинула не тільки на фінансові показники діяльності компанії та її позиції на світовому ринку телекомунікаційних товарів та послуг, але й на реалізацію амбіційної стратегії « Зроблено у Китаї 2025» . Отже, поширення торгівельних війн між США, і КНР на високотехнологічний сектор свідчить про те, що обидві держави переконані, що контроль над високими технологіями визначає майбутнє світового порядку (Saran, 2020). Результатом стало створення списку компаній, щодо яких було введено санкції (загалом 48 технологічних і оборонних компаній, в які американським компаніям було заборонено інвестувати), оскільки їх діяльність суперечить національній безпеці США. Під санкції потрапила не тільки компанія Huawei, яка втратила доступ до сервісів Google, але й 70 пов’язаних з нею компаній.

Показовим є рішення, ухвалені в інших державах світу. Так, у червні 2020 р. уряд Данії проголосив, що держава повинна мати можливість обрати постачальників 5G серед компаній країн, що мають високі стандарти безпеки, а тому провідна телекомунікаційна компанія обрала таким постачальником не Huawei, а Ericsson, тоді ж Singapore Telecommunication Company, контрольний пакет акцій якої належить державній інвестиційній компанії, обрала Ericsson і Nokia замість Huawei для забезпечення розбудови інфраструктури 5G-зв’язку. Але в деяких країнах такі заборони супроводжувалися погіршенням відносин з Китаєм. Так, на тлі спалаху насильства у червні 2020 р. на кордоні між КНР та Індією, яке призвело до загибелі 20 індійських солдат, в останній почалися заклики до байкотування китайських

товарів. Тому наприкінці червня уряд Індії повідомив про заборону доступу в країну 59 китайських програмних додатків, у тому числі WeChat та TikTok, а також звернувся до національних телекомунікаційних компаній із закликом використовувати обладнання не китайського, а місцевого виробництва, що суттєво вдарило по позиціям компанії Huawei (Sherman, 2020). Нова ж адміністрація Дж.Байдена розширила перелік компаній, які потрапили під санкції в інтересах безпеки. Переважно обмеження були впроваджені по відношенню до компаній, які використовують системи спостереження за межами Китаю, що може призвести до порушення прав людини, поширення шкідливого програмного забезпечення, порушення права власності, а також здійснення інформаційних атак на особи, які причетні до управління військами, розвідки та кібершпигунства, що призводить до витоку конфіденційної урядової інформації, комерційної інформації та персональних даних, у тому числі, про стан здоров'я та генетичні дані тощо (The White House, 2021). КНР відразу заявила у відповідь, що ухвалить дзеркальні санкції задля захисту прав і інтересів китайських компаній (Biden expands US investment ban on Chinese firms, 2021). Це змусило Huawei перейти на розробку і продаж програмного забезпечення, щоб обійти санкції США.

Інформаційні та науково-технологічні досягнення стали також важливим фактором збільшення «дефіциту довіри», який виникає внаслідок наявності значної кількості давніх територіальних спорів та конфліктів. Нині особливістю більшості традиційних територіальних конфліктів у регіоні є те, що поступово силові засоби протистояння витісняються інформаційними (Asia Society Policy Institute, 2017). Так, у звіті компанії Recorded Future, яка займається питаннями кібербезпеки, описується складна кіберкампанія китайських агентів, націлена на індійські цілі. Як зазначається у документі, китайське угруповання Red Echo встановило шкідливе програмне забезпечення у системі критично важливої цивільної інфраструктури Індії, зокрема, у сфері енергетики та управління транспортом. На думку експертів, ця атака напряму пов'язана з китайсько-індійським конфліктом вздовж гірського північного кордону. Практично кіберзіткнення відбувалося паралельно реальним військовим подіям. Китай, використовуючи наступальні кіберзасоби, здійснив

руйнівну атаку на фізичний простір цивільної інфраструктури, що стало свідченням не тільки ескалації конфлікту, але й виходу протистояння на новий рівень. Отже, китайська держава продемонструвала, що готова до активного використання нових засобів протиборства, що суттєво вплине на традиційний баланс сил у системі регіональної безпеки усього Індо-Тихоокеанського регіону. Водночас кібератаки Китаю мають наслідки, які виходять за рамки китайсько-індійського конфлікту, оскільки демонструють готовність використовувати кіберфізичні методи протиборства в політичному протистоянні Китаю в інших регіональних конфліктах (Burgers, 2021).

Китай нині також активно просуває стратегію домінування в інформаційному просторі АТР, яку він називає «силою дискурсу», шляхом поглинання підприємств медіаіндустрії, створення та поширення маніпулятивної інформації чи дезінформації через новинні сайти і діяльність кібертролів. Наприклад, в Японії, де переважна кількість громадян не розглядають соціальні платформи як джерело новин, Китай використовує замасковані японські новинні сайти, пов’язані з китайською державою, через які завдяки чисельним агрегаторам, поширює прокитайський новинний контент. Так, японська компанія SearChina, яка займається поширенням новин та редакторських матеріалів про Китай, дозволяє знайомитися з інформацією про політичне життя КНР, фінансовий та економічний розвиток країни, соціальний і культурний розвиток. Водночас, як показує більш глибокий аналіз контенту, що поширюється через SearChina, відбувається значна кореляція між новинами, пов’язаними з Китаєм, та використанням таких термінів з позитивним значенням, як «безпека», «перевага», «гарний» тощо. SearChina повідомляє про зміст політики партії, цитуючи переважно матеріали агентства Toutiao, яке відоме своєю суворою самоцензурою і відповідністю наративам КПК, поширюючи інформацію прокитайського змісту. Іншим прикладом є діяльність новинного онлайн-сайту Record China, який відкрито поширює інформацію політичного і дипломатичного характеру в інформаційному просторі Японії, повторюючи позицію китайського уряду. Наприклад, проблема уйгурів висвітлюється не як порушення прав людини, а крізь призму інтерпретації проблеми з позиції терористичної загрози. Матеріали,

представлені Record China, сформовані на основі китайських джерел або інформації, що поширюється державними китайськими ЗМІ або приватними, які підтримують КПК. Більш того, сайт часто просуває контент, спрямований на досягнення ключових геополітичних цілей Китаю, наприклад, для погіршення відносин між Японією та Південною Кореєю шляхом цілеспрямованого поширення інформації переважно про проблеми у взаємовідносинах між державами – корейський бойкот японських товарів, експортні суперечки, проблеми виконання двосторонньої Угоди про безпеку воєнної інформації тощо (Ichihara, 2020).

Ще одним важливим чинником, що впливає на архітектуру безпеки в регіоні, виступає подальша мілітаризація та модернізація збройних сил завдяки досягненням у сфері науки і технологій (Siabro, 2021). Швидкі темпи технологічних зрушень та поширення інноваційних військових технологій і технологій подвійного призначення трансформують відносини у сфері безпеки в АТР. В умовах відсутності прозорості процесу поширення і використання високих технологій та досягнень наукового прогресу, постійно зростає рівень недовіри між країнами в регіоні, що змушує держави інвестувати у нарощування військового потенціалу задля зміцнення національної системи безпеки та захисту держави від агресивних дій сусідів. Отже, розгортається потужна конкуренція у військовій сфері, яка впливає на зміну форм, методів та характеру протиборства між державами. Так, технології штучного інтелекту, нейромереж, Інтернет військових речей, імерсивні технології, адитивне виробництво, робототехніка, Великі дані та аналітика, 5G-зв’язок, квантові технології, блокчейн нині активно використовуються для підсилення військової могутності збройних сил багатьох країн регіону (Top 10 Military Technology Trends & Innovations for 2022, 2022). При цьому, сучасні технології можуть виробляти самі держави Азії, поступово послаблюючи залежність від західних партнерів. Наприклад, Китай розвиває технології штучного інтелекту як національний проект, метою якого є підвищення якості ухвалення рішень на полі боя (Kato, 2019).

2.2. Сутнісні характеристики міжнародного співробітництва у сфері інформаційної безпеки в рамка Асоціації держав Південно-Східної Азії

Поява нових, нетрадиційних викликів і загроз для регіональної системи безпеки, пов'язаних із постійним зростанням темпів науково-технологічного розвитку та масштабу змін внаслідок впровадження сучасних інформаційно-комунікаційних технологій, обумовили потребу включення питань інформаційної безпеки до пріоритетів діяльності регіональних інститутів, які прагнуть побудувати більш міцну та ефективну регіональну архітектуру безпеки.

Так, одним з провідних регіональних інститутів, до пріоритетів діяльності якого входять питання інформаційної безпеки, є Асоціація Південно-Східної Азії (АСЕАН). Саме в рамках АСЕАН у вересні 1999 р. на саміті у Манілі лідери країн регіону ухвалили комплексну стратегію цифрового розвитку, до якої було включено питання інформаційної безпеки як чинника розбудови нової цифрової економіки, а у 2000 р. було підписано Рамкову угоду, яка стала правової базою для еАСЕАН (ASEAN, 2000). Слід зазначити, що в рамках цього документу проблемі інформаційної безпеки ще не надавалося критичного значення, але вже було визначено тісний зв'язок між поступальним економічним розвитком країн регіону на основі широкого використання ІКТ і забезпеченням безпеки інформаційних мереж і технологій. Ситуація почала змінюватися у 2001 р., коли було ухвалено Декларацію про транснаціональну злочинність. Держави АСЕАН, які дедалі частіше почали стикатися з проблемою неправомірного використання високих технологій та мереж, що суттєво впливало на розвиток цифрової економіки та електронної комерції, почали включати питання кіберзлочинності до порядку денного самітів і нарад на різних рівнях співробітництва. З 2003 р. проблема інформаційної безпеки вже розглядалася як самостійний напрям діяльності організації. Такі зрушення пов'язані з формуванням спеціальних механізмів для врегулювання питань кібербезпеки, зокрема, регулярних Міністерських нарад з питань транскордонної злочинності, Міністерських нарад з питань розвитку телекомунікацій та інформаційних технологій, Міністерських конференцій з питань кібербезпеки,

Програми формування кіберпотенціалу, Регіонального форуму АСЕАН (Lung, 2018). Зокрема, у Сінгапурській декларації, ухваленій в рамках Третьої Міністерської наради з питань розвитку телекомунікацій та інформаційних технологій, зазначалося, що слід прискорити розвиток системи безпеки інформаційної інфраструктури АСЕАН шляхом створення до 2005 р. в усіх державах-членах національних груп швидкого реагування на кіберінциденти (CERTS); розробки до 2004 р. спільної структури для обміну інформацією між національними CERTS про інформаційні загрози та оцінки вразливості інформаційного простору країн та регіону в цілому, включаючи розробку систем стандартних операційних процедур; вживання зусиль з розбудови потенціалу для надання допомоги країнам-членам, які ще не створили CERTS або не розробили політику у сфері кібербезпеки, в тому числі, шляхом використання заходів щодо розвитку потенціалу в рамках таких форумів, як АРЕС, АРТ і APCERT; запуску «Віртуального форуму з кібербезпеки АСЕАН», в рамках якого представники національних груп швидкого реагування на кіберінциденти можуть обмінюватися інформацією з питань кібербезпеки в режимі реального часу; узгодження позицій щодо регулювання у сфері електрозв'язку (ASEAN, 2003). Водночас, процес вироблення спільних механізмів реагування та протистояння новим типам загроз продовжував гальмуватися внаслідок нерівномірності інформаційного і науково-технологічного розвитку країн регіону, що стало причиною відмінності в усвідомленні проблем інформаційної безпеки для національної економіки та суспільства і прагненні виробити спільні механізми для протидії інформаційним ризикам і загрозам на регіональному рівні.

Ситуація суттєво змінилася після 2007 р., коли кіберінциденти в Естонії та Грузії наочно продемонстрували можливості завдання масштабного удару по державі та наслідки інформаційних атак для державних інститутів та бізнеса (Сябро, 2021). Отже, у регіоні, де бурхливий розвиток залежав передусім від технологічних новацій та інвестицій у науково-технологічну сферу, виникла нагальна потреба інтенсифікації зусиль у сфері інформаційної безпеки та вироблення спільних універсальних механізмів запобігання інформаційним викликам і загрозам.

Поступово проблема вийшла за межі кола питань економічної стійкості та безпеки і почала набувати політичного та оборонного значення (ASEAN, 2021b). Про це свідчить ухвалення Плану дій у сфері безпеки на X саміті АСЕАН та започаткування у 2006 р. практики проведення Щорічної наради міністрів оборони країн АСЕАН (ADMM). Пріоритетними напрямами діяльності Наради стали питання оборонного характеру, боротьба з тероризмом, миротворчі операції, гуманітарна допомога та допомога під час природних лих, розвиток військово-промислового комплексу та безпека інформаційної інфраструктури (ASEAN, 2017a).

Важливим етапом стало також ухвалення державами-членами АСЕАН у 2007 р. Конвенції про боротьбу з тероризмом. У статті VI документу, зокрема, йшлося про співробітництво держав-членів, яке повинне забезпечувати консолідований підхід та спільні дії (обмін інформацією, зміцнення потенціалу, створення баз даних, груп швидкого реагування тощо) щодо боротьби з усіма формами транскордонної терористичної діяльності у регіоні, у тому числі, з кібертероризмом. Слід зазначити, що АСЕАН на той час була одним із небагатьох геополітичних регіональних об'єднань, які ще не прийняли регіональну нормативну базу з питань боротьби з тероризмом і потребували відповідних правових механізмів (Rose, Nestorovska, 2005). Незважаючи на це, Конвенція набула чинності лише у 2011 р., а остаточно процес ратифікації було завершено у 2013 р. Таким чином, проблема боротьби з кібертероризмом як одним з видів інформаційних загроз для системи безпеки регіону увійшла до пріоритетів діяльності АСЕАН.

Подальше поглиблення співпраці у сфері безпеки передбачало розширення кола учасників за рахунок країн-партнерів АСЕАН, зокрема, США, Канадою, Австралією, Новою Зеландією, Японією, Південною Кореєю, Індією, Росією та КНР, задля формування нової архітектури регіональної безпеки, стійкої до нових, нетрадиційних викликів та загроз. Результатом стало створення у 2010 р. оновленої платформи для співпраці у сфері безпеки і оборони – Наради міністрів оборони країн АСЕАН-Плюс (ADMM-Plus), до пріоритетних напрямків діяльності якої увійшли питання кібербезпеки як важливої складової стратегії розширення діалогу та співпраці між країнами регіону та їх партнерами в умовах постійного

ускладнення архітектури регіональної безпеки (ASEAN, 2017b). Саме в рамках цієї платформи у 2016 р. було ухвалено рішення про створення Робочої групи експертів у сфері кібербезпеки Наради міністрів оборони країн АСЕАН-Плюс задля вироблення спільних підходів до боротьби з кіберзагрозами та розвитку кіберпотенціалу регіону (ASEAN, 2016b). Як підкреслюється у підсумковому концептуальному документі Наради, кіберзагрози стали критичними для всіх сфер життєдіяльності сучасного суспільства, охопивши і державний, і приватний, і громадські сектори. Кіберпростір почали активно використовувати для доступу до інформації з метою незаконного використання активів, скоєння актів тероризму, ведення війн та шпигунства. Небезпечною є також діяльність різноманітних екстремістських груп, що використовують кіберпростір для вербування нових членів та розширення мереж своїх організації.

Особливого значення набувають кіберзагрози, які можуть завдати шкоду критичній інфраструктурі держави, що призведе до виникнення серйозних проблем для енергетичного сектору, систем водопостачання, транспортних мереж, комунікаційних систем і банківських мереж. Все це свідчить про зростання значення кібербезпеки для розбудови регіональної системи безпеки, що обумовлює включення цього питання до пріоритетів діяльності не тільки Наради міністрів оборони країн АСЕАН-Плюс, а й організації в цілому. Отже, створення Робочої групи експертів мало суттєво підвищити ефективність співробітництва у сфері кібербезпеки оборонних і воєнних відомств не тільки країн-членів, а й країн-партнерів, а також сприяти розробці політичних і правових рамок у сфері кібербезпеки регіону (ASEAN, 2016b).

У 2016 р. була запущена Програма з розвитку кіберпотенціалу, яка мала підвищити здатність регіону реагувати на мінливий ландшафт кіберзагроз і створити безпечний і стійкий кіберпростір АСЕАН. У Програмі було передбачено реалізацію ініціатив, спрямованих на розвиток технічних, політичних і стратегічних можливостей держав-членів АСЕНАН. Основними напрямами програми було визначено кіберполітику, зміну законодавства, розробку стратегії, а також формування системи оперативного реагування на кіберінциденти (ASEAN, 2016a).

З 2016 р. в рамках АСЕАН стали також регулярно проводиться міністерські конференції з питань кібербезпеки. Так, під час Першої міністерської конференції з питань кібербезпеки у Сінгапурі (2016 р.) було оприлюднено регіональну стратегію кібербезпеки, що стало переконливим свідченням усвідомлення реальних і потенційних наслідків інформаційних загроз і потреби вироблення механізмів співробітництва для їх нейтралізації. Отже, як підкреслювалося у вступній промові Я. Ібрагіма, міністра комунікацій та інформації, відповідального міністра з питань кібербезпеки, країни АСЕАН нині вже стикаються з повним спектром кіберзагроз – кіберзлочинністю, кібератаками на урядові і неурядові системи і технології, шпигунством та іншими видами протиправної діяльності з використанням високих технологій. На жаль, ця тенденція буде постійно зростати, оскільки відбувається пришвидшення процесів цифрової трансформації в країнах регіону, а отже кіберзагрози ставатимуть дедалі більш серйозним викликом для економіки, політики, безпеки і суспільства в цілому. Тому слід особливу увагу приділяти співробітництву між країнами регіону та їх партнерами за межами регіону у сфері кібербезпеки.

Актуальним питанням також залишається нарощування потенціалу країн-членів АСЕАН у сфері кібербезпеки, що передбачає розробку і впровадження ефективних механізмів оперативного реагування на кіберзагрози, нарощування технічних можливостей протистоянням новим типам загроз, розвиток структур протидії кіберінцидентам, а також робота з громадянами країн з метою підвищення рівня обізнаності з проблеми кібербезпеки. Важливим також є створення більш надійного і безпечного кіберсередовища, оскільки транскордонний характер кіберзагроз робить вразливими критично важливі елементи інфраструктури країн регіону незалежно від їх розташування і кордонів. Цьому також має допомогти реалізація проекту CyberGreen – глобальної ініціативи, спрямованої на захист кіберпростору, моніторинг кіберздоров’я та стану кібергігієни у регіоні, а також визначення потенційних вразливостей інформаційного середовища. Реалізацію ініціативи дає можливість не тільки підвищити рівень обізнаності з різних питань

проблеми кібербезпеки, але й вживати превентивні заходи для попередження виникнення реальних загроз і кіберризиків.

Для досягнення окреслених пріоритетів вкрай потрібним є не тільки розвиток співпраці між усіма державами регіону у сфері кібербезпеки, але й співробітництво на рівні міжнародних інститутів. Так, країни-члени АСЕАН підтримали ініціативи ООН щодо правил поведінки держав у кіберпросторі, що має суттєво підвищити рівень відповідальності за кібербезпеку, але зазначили, що такі норми мають співвідноситися с нормами, які вироблені на регіональному рівні і не суперечити їм. Значний внесок може зробити й співпраця у сфері кібербезпеки з міжнародними інформаційними компаніями, наприклад, Microsoft (ASEAN, 2016c).

Під час відкриття Другої міністерської конференції з питань кібербезпеки у Сінгапурі (2017 р.) Я. Ібграгім у своїй промові особливу увагу приділив питанням взаємозв'язку між динамічним економічним розвитком країн регіону на основі впровадження високих технологій та розбудови цифрової економіки, і підвищенням стандартів у сфері кібербезпеки. Показовими прикладами в цьому контексті стали масштабні кібератаки на компанії HBO і Sony, які не тільки втратили інтелектуальну власність, але й зазнали суттєвих економічних збитків. Для ефективного протистояння викликам у сфері кібербезпеки, на думку Я. Ібрагіма, слід працювати над підвищенням кіберстійкості критичних інформаційних інфраструктур як на рівні кожної держави-члена, так й на рівні регіону в цілому, стимулювати розвиток динамічної екосистеми кібербезпеки, розвивати міжнародне партнерство задля зміцнення регіонального кіберпотенціалу та стійкості до кіберзагроз (ASEAN, 2017b).

В рамках Третьої міністерської конференції (2018 р.) основну увагу було приділено обговоренню питань удосконалення системи регіональної кібербезпеки, у тому числі, із залученням держав-партнерів АСЕАН (ASEAN, 2018b). У розвиток Заяви лідерів держав АСЕАН щодо співробітництва у сфері кібербезпеки, представленої на 32-гому саміті АСЕАН, учасники конференції ухвалили рішення про вироблення гнучкого офіційного механізму забезпечення кібербезпеки регіону, який дозволить розглядати та ухвалювати рішення із взаємопов'язаних питань

кібердипломатії, політики та оперативної діяльності у сфері кібербезпеки (ASEAN, 2018a; 2018c). Таким чином, було запропоновано реалізовувати комплексний підхід, який дозволив врахувати різноманіття кіберризиків та загроз. Під час конференції було також заявлено про значні успіхи у досягненні раніше ухвалених рішень, зокрема, щодо нарощування регіонального кіберпотенціалу та побудови регіональної системи управління ризиками і загрозами у кіберсередовищі. Важливу роль у цьому відігравали встановлені двосторонні партнерські відносини з країнами-сусідами, зокрема, Австралією та Японією (Koh, 2020). Таким чином, стало очевидним, що вирішальне значення для зниження рівня вразливості від кіберзагроз та ризиків держав-членів АСЕАН є регіональні ініціативи, але їх може виявитися недостатньо, якщо вони мають вузьку специфіку (наприклад, суто технологічну, спрямовану на пом'якшення наслідків кібератак) або пропонуються для реалізації державам регіону, в яких відсутні правові акти у сфері кібербезпеки чи немає відповідних агенцій, що займаються питаннями кібербезпеки. Тому було ухвалено рішення про залучення до реалізації концепції регіональної кібербезпеки таких структур, як Міністерська нарада АСЕАН з питань транснаціональної злочинності, Зустріч міністрів зв'язку та інформаційних технологій (TELMIN) та Регіональний форум АСЕАН, що дозволило розглядати проблему кібербезпеки як комплексну, яка торкається усіх сфер життєдіяльності держав регіону. Важливим стало також включення до пріоритетів діяльності питань державно-приватного партнерства, що дозволить залучати необхідні фінансові, технічні та людські ресурси для реалізації стратегії кібербезпеки (Putra, 2018).

Упродовж 2019 р. АСЕАН продовжив роботу з розвитку регіональної системи кібербезпеки, актуальність якої дедалі зростала із розвитком цифрової економіки та активним впровадженням сучасних технологій у всі сфери життєдіяльності суспільств. Стало зрозумілим, що стійка екосистема кібербезпеки набуває вирішального значення для подальшого використання електронних комунікацій та послуг в умовах постійного удосконалення та модернізації інформаційних загроз. Для подальшої роботи над впровадженням регіональної стратегії кібербезпеки із стійкою інформаційною екосистемою, розробки і реалізації відповідних

національних стратегій, було проведено дослідження ландшафту кіберзагроз, які є найбільш небезпечними для подальшого динамічного розвитку країн регіону. Як зазначається у спільному дослідження ІНТЕРПОЛУ та АСЕАН, швидкий розвиток цифрових економік регіону призвів до збільшення масштабів та різноманіття інформаційних загроз – починаючи від масового витоку інформації і даних та руйнівних атак програм-вимагачів до стрімкого зростання криптоджекінгу. Так, найбільш небезпечними були визначені п’ять типів загроз: ботнети та хостинг CnC серверів, які спрямовані переважно на фінансовий сектор та його клієнтів з метою отримання віддаленого доступу до комп’ютерів – об’єктів атаки, викрадення персональних даних або поширення шкідливих програмних продуктів; фішингові кампанії (на країни АСЕАН припадає 5 % усіх фішингових атак у світі); шкідливі програмні продукти, особливо у банківському секторі (наприклад, Emotet16), кількість яких зросла на 50 % за один рік; шкідливе програмне забезпечення, яке постійно розвивається і удосконалюється, особливо із зростанням популярності криптовалют (наприклад програма-вимагач і шантажист Ransomware, що використовує методи шифрування інформації або блокування доступу до комп’ютерних програм для вимагання грошей за відновлення доступу до інформації та даних), більш досконала версія шкідливого програмного забезпечення Cerber, яка має додаткові функції таймеру зворотного відліку, лічильник збільшення суми викупу, якщо вона не надходить у встановлений вимагачем час, WannaCry (або WannaCrypt, WCry, WanaCrypt0r 2.0 і Wanna Decryptor) – шкідлива програма-вимагач, що використовує вразливості операційної системи MS Windows для проникнення на комп’ютер і шифрування даних, розблокувати які можна лише після сплати викупу у криптовалюті); криптоджекінг або шкідливий майнінг – шкідливе програмне забезпечення для здійснення прихованого майнінгу криптовалют шляхом використання чужих пристроїв – комп’ютерів, смартфонів або навіть серверів без відому їх власників (ASEAN, 2020).

Такий сплеск кібератак в усьому Індо-Тихоокеанському регіоні поставив на порядок денний діяльності АСЕАН питання продовження реалізації ініціатив із зміцнення кібербезпеки як на національному, так і на регіональному рівні для

ефективного протистояння більш досконалим інформаційним загрозам. Саме про це йшлося під час Четвертої міністерської конференції з питань кібербезпеки (2019 р.), провідною темою якої було визначено «Регіональні рамка взаємодії: майбутнє стратегій кіберстійкості АСЕАН». В результаті зустрічі були розроблені документи про механізм координації кібербезпеки АСЕАН та ухвалені рішення про підтримку центрів кібербезпеки у Сінгапурі та Тайланді (Indo-Pacific Defense Forum, 2019).

У вступній промові С. Ісварана, міністр зв'язку та інформації, відповідальний міністр з питань кібербезпеки АСЕАН, зазначав, що інформаційні атаки продовжують модернізуватися і перетворюватися на більш ефективний інструмент деструктивного впливу на держави регіону. Відтепер такі атаки мотивовані не тільки економічної вигодою, але й прагненням зруйнувати критично важливу інфраструктуру в цілому. У той же час ускладняються й об'єкти кіберзахисту, які включають більш складні системи комунікації, Інтернет речей та 5G-зв'язок. Зокрема, посилаючись на дослідження Cisco Systems, проведені ще у 2018 р., було заявлено, що країни усього Індо-Тихоокеанського регіону кожні 10 секунд зазнають кібератаки, від яких страждає і державний сектор, і приватні компанії, і окремі громадяни. За даними дослідження діяльності 200 компаній регіону було встановлено, що вони щороку внаслідок кібератак втрачають понад 1 млрд.дол.США (Singapore Government Agency, 2019). Прикладом можуть слугувати атаки на сервери Toyota Motor Corp. в Тайланді та В'єтнамі (2019 р.), на ресурси філіппінської фінансової компанії Cebuana Lhuillier (2019 р.), внаслідок якої постраждало 900 тис. клієнтів, викрадення персональних даних 14200 осіб з діагнозом ВІЧ у Сінгапурі (2019 р.), розкриття документів, що підтверджують особу, 45 тис. клієнтів True Corp., другої за розміром мобільної мережі Тайланду (2018 р.) тощо. Тому слід поєднати зусилля приватного сектору і державних структур з новим міжсекторальним координаційним комітетом задля ефективної реалізації спільних ініціатив у сфері кібербезпеки (Indo-Pacific Defense Forum, 2019).

Під час зустрічі було оголошено про запуск Центру передового досвіду з кібербезпеки АСЕАН-Сінгапур, основними напрямами діяльності якого визначено: здійснення досліджень та тренінгів з питань міжнародного права у сфері

кібербезпеки, розробки кіберстратегій, кіберконфліктів, розробки законодавства та вироблення норм права інформаційної безпеки, інших питань політики у сфері кібербезпеки; забезпечення навчань, пов'язаних з діяльністю CERT, а також сприяння обміну інформацією, пов'язаною з кібератаками та кіберзагрозами, обмін позитивним досвідом у сфері кібербезпеки; проведення віртуальних тренінгів та навчань з кіберзахисту (Singapore Government Agency, 2019).

П'ята міністерська конференція (2020 р.) відбулася вже в умовах пандемії COVID-19. У своїй традиційній вступній промові С. Ісварана підкреслив, що пандемія не тільки значно прискорила процеси інформатизації та розбудови інформаційного сектору економіки, але й актуалізувала питання кібербезпеки, вирішити які можливо тільки спільними зусиллями всіх країн регіону та їх партнерів. Основними темами дискусій під час зустрічі стали, по-перше, розвиток кіберпростору регіону, що базується на правилах і нормах, спільних для усього регіону; по-друге, зміцнення регіональної кіберстійкості за рахунок удосконалення технологій, які є базовими для формування регіональної інформаційної інфраструктури (зокрема, йшлося про технології Четвертої індустріальної революції).

Щодо першого напряму дискусій, обговорювалися не тільки спільні правові норми, які регулюють сферу кібербезпеки, але й питання їх узгодження з нормами права міжнародної інформаційної безпеки. Учасники зустрічі також продовжили обговорювати правила відповідальної поведінки держав у кіберпросторі, запропоновані ООН з метою узгодження національних підходів до розробки і впровадження стратегій кібербезпеки. Другий напрям дискусії, присвяченої обговоренню механізмів захисту критично важливих елементів інфраструктури регіону, був зосереджений на питаннях удосконалення механізмів кібербезпеки у сфері операційних технологій та Інтернету речей. Як підкреслив С. Ісварана, ландшафт операційних технологій та Інтернету речей розвивається надзвичайно високими темпами, формуючи як нові можливості, так й нові ризики та загрози для подальшого цифрового розвитку держав регіону. Успішні кібератаки на систему базових операційних технологій можуть призвести до значних втрат у

кіберфізичному просторі, зокрема, у сфері енергопостачання та транспорту. Щодо Інтернету речей, проблема полягає у масштабності наслідків атак, оскільки «розумні» пристрої, об'єднані мережею Інтернет, стали необхідним елементом повсякденного життя багатьох громадян країн регіону. Показовим у цьому контексті є досвід Сінгапуру щодо впровадження спеціального маркування (Cybersecurity Labelling Scheme, CLS), яке містить позначення рейтингу кібербезпеки зареєстрованих «розумних» пристрої, що впливає на рішення споживачів придбати їх. До того ж, враховуючи транскордонний характер атак, наслідки можуть не обмежуватися однією країною. Таким чином, для держав-членів АСЕАН вкрай важливим залишається продовження і подальший розвиток ініціатив у сфері кібербезпеки, а також залучення міжнародних партнерів для зміцнення кіберпотенціалу регіону (Singapore Government Agency, 2020).

В рамках Шостої міністерської конференції з питань кібербезпеки (2021 р.) було продовжено обговорення проблем захисту кіберпростору регіону та зміцнення кіберпотенціалу задля підвищення ефективності протистояння сучасним викликам і загрозам. У вступній промові новий міністр з питань зв'язку та інформації, відповідальний міністр з питань кібербезпеки АСЕАН Ж. Тео, зокрема, зазначила, що в сучасному світі дедалі більшим стає вплив цифрового середовища на різні аспекти життя (Singapore Ministry for Communications and Information, 2021b). Відключення Facebook, WhatsApp та Instagram усього на два дні спричинило виникнення багатьох проблем у всьому світі, що демонструє зростання залежності сучасної людини від цифрових послуг та стійкості електронних мереж. У промові також підкреслювалося, що нині відбувається стрімка зміна ландшафту кіберзагроз, а популярності продовжує набувати поширення шкідливих програмних продуктів, що використовуються для незаконного майнингу криповалют або програми-вимагачі. Масштаби поширення загроз та їх наслідків настільки значні, що перетворилися на небезпеку для життя людини. Це означає, що слід продовжувати зміцнювати кіберстійкість регіональної інформаційної критичної інфраструктури та посилювати кіберпотенціал, у тому числі, пов'язаний із ефективним протистоянням сучасним викликам та загрозам.

Важливим напрямом діяльності було визначено участь у реалізації міжнародних ініціатив у сфері кібербезпеки, зокрема, долучення країн регіону до обговорення правил поведінки держав у кіберпросторі, запропонованих в рамках ООН. Як зазначалося у доповіді, АСЕАН стала першою регіональною організацією, яка добровільно приєдналася до ініціативи і підтримала 11 необов'язкових норм відповідальної поведінки держав у кіберпросторі, що, на думку представників держав регіону, є важливим кроком на шляху до зміцнення міжнародної системи кібербезпеки. Участь в діяльності ООН у сфері кібербезпеки також була пов'язана з ініціативами АСЕАН щодо поглиблення розуміння проблеми захисту транскордонної критичної інформаційної інфраструктури, у тому числі, через усвідомлення ролі приватних компаній, які є не тільки власниками цієї інфраструктури, але й використовують її для надання послуг користувачам в усьому світі за межами національних кордонів. Тому необхідно розробляти такі механізми безпеки критично важливих елементів інформаційної інфраструктури, які б враховували особливості участі державного і приватного секторів в цьому процесі (Singapore Ministry for Communications and Information, 2021a).

У своїй промові Ж. Тео також відзначила, що перша Стратегія співробітництва АСЕАН у сфері кібербезпеки, що реалізовувалася упродовж 2017-2020 рр. була скоріше дорожньою картою регіонального співробітництва для формування безпечного і захищеного кіберпростору Південно-Східної Азії. Але відтоді ситуація суттєво змінилася, країни регіону досягли значних успіхів у сфері розбудови цифрового суспільства, але модернізувалися й загрози для цифрового середовища. Тому Стратегія потребує подальшої модернізації, особливо у контексті ухвалення Цифрового плану АСЕАН до 2025, в якому передбачено пришвидшення розвитку цифрової економіки та цифрового суспільства на основі більш широкого використання сучасних технологій і різноманітних цифрових послуг. Як зазначається у документі, саме звернення уваги на цифровий сектор як з боку держави, так й з боку приватного сектору, може не тільки допомогти вийти з економічної кризи після пандемії, але й забезпечити подальший поступальний розвиток регіону (ASEAN, 2021) Тому нова ініціатива у сфері кібербезпеки

обов’язково має включати щонайменше п’ять практично орієнтованих напрямків діяльності: поглиблення співробітництво у сфері підвищення рівня кіберготовності, зміцнення регіональної координації у сфері кіберполітики, зміцнення довіри у кіберпросторі та регіонального кіберпотенціалу, поглиблення міжнародного співробітництва у сфері кібербезпеки (Singapore Ministry for Communications and Information, 2021b). Серед сучасних пріоритетів співробітництво між державами-членами АСЕАН у сфері кібербезпеки було визначено: втілення регіональної кіберстратегії, проведення спеціальних кібероперацій та співробітництво у сфері технічного забезпечення, а також зміцнення кіберпотенціалу.

Про координацію підходів держав АСЕАН до проблеми кібербезпеки говорив й Генеральний секретар АСЕАН Лім Джок Хой. Підтримуючи ініціативи, проголошені Ж. Тео, Лім додав, що для формування стійкої регіональної системи кібербезпеки вкрай важливим є питання розробки нормативно-правової бази, стандартів та підходів, що враховують передові методи забезпечення кібербезпеки, що сприяє забезпеченню функціональної сумісності та надійного і стійкого середовища використання цифрових технологій (Choudhury, 2021).

2.3. Особливості політики інформаційної безпека Шанхайської організації співробітництва

На формування регіональної архітектури безпеки значний вплив спричиняє Шанхайська організація співробітництва, утворена у 2001 р. країнами так званої «Шанхайської п’ятірки» – Китаєм, Казахстаном, Киргизстаном, Росією та Таджикистаном для вирішення передусім територіальних конфліктів на пострадянському просторі. Від самого започаткування вирішальну роль у визначенні пріоритетів діяльності у сфері безпеки відігравали КНР та Росія, але бачили їх по-різному. Так, для РФ ШОС розглядалася як безпекова організація, яку згодом можна перетворити на формальний альянс за зразком НАТО. Натомість КНР не прагнула підтримувати мілітаристську інтерпретацію і виступала за більш цілісний та різноманітний підхід (Cobaleda, 2020). Згодом, до пріоритетів діяльності

ШОС поступово увійшли питання інформаційного і економічного співробітництва. Останнє було пов’язане із зростанням глобальних амбіцій КНР та посиленням протиріч між Росією і країнами Заходу (Muratbekova, 2019). Наслідком зміни геополітичних та геоекономічних умов у регіоні стало рішення про розширення кола учасників організації за рахунок включення до неї Індії і Пакистану. Нині Шанхайська організація співробітництва позиціонується як багатостороннє об’єднання, діяльність якого спрямована на забезпечення безпеки та підтримання стабільності регіону, спільне протистояння новим викликам і загрозам, зміцнення торгово-економічного та культурно-гуманітарного співробітництва (Alimov, 2017).

Слід підкреслити, що вступ Індії і Пакистану до ШОС значно зміцнив її позиції і перетворив на одну з найбільших регіональних організацій у світі. Відтепер на долю членів ШОС припадає 44 % населення Землі, бл. 26,6 % земної поверхні, 33 трлн. дол. США сукупного ВВП. До того ж чотири держави мають ядерну зброю. Таким чином ШОС перетворилася на своєрідний коридор, що пов’язує Азійсько-Тихоокеанський та Атлантичний регіони, Південну Азію та Близький Схід (Muratbekova, 2019). Після саміту в Астані у 2017 р. країни-члени ШОС продовжили обговорювати питання розширення організації за рахунок можливого включення нових держав-членів, зокрема, Ірану, Афганістану та Монголії. Водночас питання залишається відкритим, оскільки проявилися суттєві розбіжності між державами-членами. Так, Таджикистан зайняв принципову позицію щодо вступу Ірану через конфлікт у 2015 р., коли Іран запросив М. Кабірі, лідера Партії ісламського відродження, забороненої в Таджикистані, на конференцію Організації ісламської єдності (Muratbekova, 2019). Інша держава – Афганістан – виступає одним з основних викликів у сфері регіональної безпеки. Нині у структурі ШОС створено ефективні механізми для співробітництва, що дозволяє охопити значну кількість проблем регіональної системи безпеки. Так, функції головного керівного органу виконує Рада голів держав, а також Рада голів урядів, які проводять щорічні зустрічі для обговорення нагальних питань у сфері безпеки та інших сферах компетенції діяльності організації. Крім того, проводяться зустрічі на рівні глав законодавчої влади країн-учасниць, представників рад безпеки, міністрів закордонних справ,

міністрів оборони, надзвичайних ситуацій, голів силових структур, верховних та арбітражних судів, генеральних прокурорів, а також інших сфер співробітництва – економіки, транспорту, культури, освіти та охорони здоров'я. Роль координаційного механізму ШОС виконує Рада національних координаторів (Muratbekova, 2019).

Питання інформаційної безпеки офіційно увійшли до пріоритетів діяльності організації з 2006 р., коли було оприлюднено Заяву голів держав-членів ШОС щодо міжнародної інформаційної безпеки. Так, у документі зазначалося, що однією з найсуттєвіших особливостей сучасності є стрімкий розвиток та широке впровадження новітніх інформаційно-комунікаційних технологій. Проникаючи у всі сфери людської діяльності, ІКТ формують глобальне інформаційне середовище, від якого напряму залежить стан політичної, економічної, оборонної, соціокультурної та інших складових національної безпеки та загальної системи міжнародної безпеки і стабільності. Отже, інформаційне середовище перетворюється на системоутворюючий фактор життєдіяльності суспільства, а інформація – на один з найцінніших елементів національного надбання та на один з найважливіших політико-економічних ресурсів. Таким чином, ІКТ, з одного боку, створили значний потенціал для розвитку можливостей людини, додаткові інструменти функціонування суспільства і держави, призвели до формування глобального партнерства з метою сталого розвитку та безпеки, а з другого, перетворилися на джерело нового типу загроз, здатних завдати серйозні удари по безпеці людини, суспільства, держави, порушуючи базові принципи рівноправ'я та взаємоповаги, невтручання у внутрішні справи суверенних держав, мирного врегулювання конфліктів, незастосування сили, дотримання прав людини тощо. До того ж, протиправне використання ІКТ із злочинними, терористичними чи військово-політичними цілями, є несумісним з принципами забезпечення міжнародної безпеки, може відбуватися як у цивільній, так й у військовій сферах, і мати складні політичні та соціально-економічні наслідки як в окремих країнах чи регіонах, так й у світі в цілому. У документі зазначалося, що ця ситуація може призвести до світової катастрофи, яка за своїми руйнівними наслідками зрівняється із застосуванням зброї масового ураження. Саме тому необхідно збільшувати національні зусилля щодо

забезпечення інформаційної безпеки та посилювати спільні дії на двосторонньому, регіональному та міжнародному рівнях. Тільки скоординовані та взаємодоповнюючи дії держав дозволять дати адекватну відповідь сучасним викликам і загрозам безпеки в інформаційній сфері. Тому голови держав ухвалили рішення про створення групи експертів держав-членів ШОС з питань міжнародної інформаційної безпеки для вироблення плану дій та визначення можливих шляхів і засобів вирішення в рамках ШОС проблем у сфері інформаційної безпеки, враховуючи всі її аспекти (SCO, 2006). З метою реалізації принципів, проголошених у Заяві, під час чергового засідання Ради голів держав-учасників ШОС у Бішкеку 16 серпня 2007 р. було підписано Бішкекську декларацію і затверджено План дій щодо забезпечення міжнародної інформаційної безпеки. Так, у Бішкекській декларації зазначалося, що ефективно протистояти новим викликам і загрозам можна лише через поєднання зусиль усієї світової спільноти на основі узгоджених принципів і в рамках багатосторонніх механізмів. Співробітництво у сфері протидії новим викликам і загрозам має здійснюватися послідовно, без використання подвійних стандартів, із суворим дотриманням норм міжнародного права. Саме тому сучасна архітектура безпеки має бути побудована на основі неухильного дотриманням норм міжнародного права і передбачати врахування інтересів усіх зацікавлених сторін, уможливлюючи самостійний вибір кожною державою власного шляху розвитку, що враховуватиме історичний досвід, національну специфіку і національні інтереси, гарантію рівноправної участі держав у міжнародних ініціативах у сфері безпеки тощо. На особливу увагу у контексті забезпечення міжнародної стабільності і безпеки заслуговує проблема розвитку і масового використання інформаційних технологій, у тому числі, у протиправних цілях. Тому держави-члени ШОС оголосили про готовність розвивати співробітництво і активізувати спільні дії із зміцнення міжнародної інформаційної безпеки у всіх її аспектах (SCO, 2007).

У Плані дій щодо забезпечення міжнародної інформаційної безпеки йшлося про поглиблення співробітництва між державами членами у сфері міжнародної інформаційної безпеки та продовження роботи організації над такими питаннями, як: вироблення єдиного підходу до термінологічного тлумачення феномену

інформаційної безпеки та його складових; дослідження нових типів інформаційних загроз, що постійно змінюються і модернізуються, та вироблення ефективних механізмів протидії ним; координація дій держав-членів ШОС, а також спеціалізованих структур для забезпечення інформаційної безпеки регіону; адаптація норм права інформаційної безпеки держав-учасниць ШОС до принципів і норм міжнародної інформаційної безпеки; поглиблення співпраці між державами-членами ШОС та іншими міжнародними структурами у питаннях інформаційної безпеки (Макаренко, 2011). У наступному, 2009 р. ШОС продовжила роботу над розробкою стратегії інформаційної безпеки. Зокрема, ця тематика була включена до порядку денного саміту голів держав ШОС в Єкатеринбурзі у червні 2009 р. В рамках проведення саміту обговорювалася ціла низка питань, пов'язаних з інформаційною безпекою, зокрема, питання регіональної архітектури безпеки в умовах наростання кризи традиційних структур забезпечення безпеки та появи нових викликів і загроз. Результатом проведення зустрічі стало ухвалення Єкатеринбурзької декларації, в якій підкреслювалася актуальність проблеми забезпечення міжнародної інформаційної безпеки як одного з ключових елементів загальної системи міжнародної безпеки. Важливим кроком на шляху формування стратегії інформаційної безпеки в рамках ШОС стало підписання Угоди між урядами держав-членів Шанхайської організації співробітництва про співпрацю в сфері забезпечення міжнародної інформаційної безпеки (Єкатеринбург, 2009 р.). По-перше, у документі було представлено базові тлумачення термінів у сфері інформаційної безпеки, зокрема, «інформаційна безпека» та «міжнародна інформаційна безпека», «інформаційна війна», «інформаційна зброя», «інформаційна злочинність», «інформаційний тероризм», «неправомірне використання інформаційних ресурсів», «несанкціоноване втручання в інформаційні ресурси», «загрози інформаційної безпеки» тощо. По-друге, було представлено перелік основних видів загроз у сфері міжнародної інформаційної безпеки, їх джерел та ознак, у якій увійшли: розробка і застосування інформаційних озброєнь, підготовка та ведення інформаційної війни; інформаційний тероризм; інформаційна злочинність; використання домінуючого положення в інформаційному просторі, що

може загрожувати інтересам та безпеці інших країн; поширення інформації, що завдає шкоди суспільно-політичній та соціально-економічній системам, духовному, моральному та культурному середовищі інших держав; загрози безпечному, стабільному функціонуванню глобальних та національних інформаційних інфраструктур, що мають природний та (або) техногенний характер (SCO, 2009).

Для ефективного протистояння інформаційним загрозам в Угоді було запропоновано такі напрями співробітництва в сфері міжнародної інформаційної безпеки в рамках ШОС: розробка і реалізація спільних заходів у сфері забезпечення міжнародної інформаційної безпеки; створення системи моніторингу та спільного реагування на загрози, що виникають у сфері інформаційної безпеки; спільні зусилля щодо розвитку норм міжнародного права щодо обмеження поширення та застосування інформаційної зброї, що створює загрози для сфери інформаційної безпеки і оборони; протидія загрозам використання інформаційно-комунікаційних технологій у терористичних цілях та протидія інформаційній злочинності; здійснення експертиз та досліджень у сфері забезпечення інформаційної безпеки; сприяння забезпеченню безпечного, стабільного функціонування та інтернаціоналізації управління глобальною мережею Інтернет; забезпечення інформаційної безпеки критично важливих структур держав ШОС; розробка та здійснення спільних заходів, спрямованих на зміцнення довіри, що сприяє забезпеченню міжнародної інформаційної безпеки; розробка та здійснення узгодженої політики та організаційно-технічних процедур щодо реалізації можливостей використання електронного цифрового підпису та захисту інформації при транскордонному інформаційному обміні; обмін інформацією про законодавство держав-учасниць ШОС з питань забезпечення інформаційної безпеки; удосконалення міжнародно-правової бази та практичних механізмів співробітництва держав-учасниць у забезпеченні міжнародної інформаційної безпеки; створення умов для взаємодії компетентних органів держав-членів ШОС з метою реалізації цієї Угоди; взаємодія в рамках міжнародних організацій та форумів з питань забезпечення міжнародної інформаційної безпеки; обмін досвідом, підготовка спеціалістів, проведення робочих зустрічей, конференцій, семінарів та інших

форумів уповноважених представників та експертів ШОС у галузі інформаційної безпеки; обмін інформацією з питань, пов'язаних із здійсненням співробітництва з усіх напрямів міжнародної інформаційної безпеки (SCO, 2009).

Отже, як свідчить аналіз документів ШОС, Організація підтримує на концептуальному рівні підходи щодо інформаційної безпеки, проголошені Росією і Китаєм у національних доктринальних документах. По-перше, на рівні термінології відбувається часткове ототожнення двох понять – «інформаційна безпека» та «кібербезпека», по-друге, прослідковується суттєве наближення понять «інформаційна війна» та «інформаційний тероризм» до того, як його визначають КНР та РФ, але й зберігається наявність впливу багатостороннього підходу та взаємної довіри, який міститься у міжнародних документах, по-третє, у документі по-суті міститься критична оцінка позиції західних держав на чолі зі США у питання управління Інтернетом, а також висловлюється прагнення взяти міжнародну участь в обговоренні питань кібербезпеки або безпеки інформаційної інфраструктури (Alcântara, 2018).

Наступним важливим етапом розвитку стратегії інформаційної безпеки ШОС стала ініціатива чотирьох держав-учасниць ШОС (Росії, Китаю, Узбекистану та Таджикистану), представлена в ООН, щодо встановлення загальних правил поведінки держав з метою забезпечення міжнародної інформаційної безпеки. І хоча проект, представлений Генеральному Секретарю ООН, був відхилений, він містив цілу низку пропозицій, які були включені у нову редакцію документу, представленого вже у 2015 р. (Rõigas, 2015). За цей період в рамках ШОС відбулося дві зустрічі, під час яких продовжували обговорюватися питання інформаційної безпеки – у Бішкеку (2013 р.) і Душанбе (2014 р.). Так, в рамках зустрічі у Бішкеку держави-учасники обговорювали питання інформаційного розвитку регіону, цифровізації і пов'язані з цим проблеми міжнародної інформаційної безпеки та кібербезпеки. Результатом зустрічі стало ухвалення рішення продовжувати « стимулювати побудову мирного, безпечного, справедливого та відкритого інформаційного простору, ґрунтуючись на засадах поваги державного суверенітету та невтручання у внутрішні справи інших країн» , що було зафіксовано у Бішкецькій

декларації (SCO, 2013). Результатом проведення зустрічі у Душанбе у 2014 р. було підписано декларацію, в якій зазначалося, що держави-члени ШОС активізують спільні зусилля із створення мирного, безпечного, справедливого і відкритого інформаційного простору, базуючись на принципах поваги державного суверенітету та невтручання у внутрішні справи інших країн, співпрацюють у сфері запобігання використанню інформаційно-комунікаційних технологій з метою підриву політичної, економічної та суспільної безпеки та стабільності держав-членів, а також загальнолюдських моральних основ соціального життя, з метою пропаганди ідей тероризму, екстремізму, сепаратизму, радикалізму, фашизму та шовінізму. У документі також зазначалося, що держави-члени ШОС виступають за рівні для всіх країн права на мережу Інтернет та суверенне право держав на управління нею у своєму національному сегменті, включаючи питання забезпечення безпеки. Слід підкреслити, що у декларації була знову висловлена підтримка вироблення універсальних правил, принципів і норм відповідальної поведінки держав в інформаційному просторі, що увійшло у нову редакцію «Правил поведінки в галузі забезпечення міжнародної інформаційної безпеки», представленої від імені держав-членів в рамках ООН (CCDCOE, 2014).

Під час зустрічі було також ухвалення рішення про проект «Стратегії розвитку Шанхайської організації співробітництва до 2025 р.», яка визначила пріоритети діяльності організації у сфері інформаційної безпеки на наступні 10 років. Так, у документі зазначалося, що у сучасному світі постійно зростають глобальні виклики та загрози, а також фактори невизначеності та непередбачуваності. Залишаються неврегульованими чимало регіональні та локальні конфліктів, територіальних суперечок тощо. Динамічні зміни у міжнародних відносинах, становлення поліцентричного світоустрою, зміцнення регіонального рівня глобального управління та посилення позицій країн, що розвиваються, стануть визначальними тенденціями наступних років. До того ж глобалізація та технологічний прогрес будуть і надалі сприяти зростанню взаємозалежності держав. Все це призведе до посилення взаємозв’язку між безпекою та процвітанням держав, а комплексний характер викликів та загроз вимагатиме вироблення колективних підходів до

боротьби з ними, а також усвідомлення неможливості забезпечення власної безпеки за рахунок безпеки інших. У цих умовах імперативом стане дотримання всіма державами універсальних принципів рівної та неподільної безпеки, які однаково застосовуються до євроатлантичного, євразійського та азіатсько-тихоокеанського просторів (SCO, 2014).

У проекті Стратегії було також представлено позицію ШОС у сфері міжнародної інформаційної безпеки. Зокрема, у документі зазначається, що ШОС буде прагнути до створення ефективного механізму спільного забезпечення безпеки інформаційного простору з метою запобігання загрозам політичній, економічній та громадській безпеці держав-членів та протидії ним. Спираючись на міжурядову Угоду про співпрацю в галузі забезпечення міжнародної інформаційної безпеки від 2009 року та інші документи, держави-члени будуть зміцнювати співпрацю у сфері управління і контролю за мережею Інтернет, запобігання використанню мережі для здійснення діяльності, що підриває безпеку та стабільність у регіоні, використання ІКТ у терористичних цілях, а також протидії кіберзагрозам безпеки держав-членів ШОС (SCO, 2014). Як й у декларації, у Стратегії було зазначено, що у наступні роки ШОС добиватиметься прийняття в ООН «Правил поведінки в галузі забезпечення міжнародної інформаційної безпеки» і надалі на цій основі спільно з іншими членами світової спільноти працюватиме над формуванням єдиного підходу до міжнародного регулювання сфери ІКТ (SCO, 2014). Саме тому у нову редакцію Правил, представлених Генеральному секретарю ООН, було внесено цілу низку поправок, а головною відмінністю став їх миротворчий характер, з основним наголосом не на процесі врегулювання конфліктів в інформаційному просторі, а на виробленні і застосуванні ефективних механізмів запобігання ним.

Основною метою документу «Правила поведінки у сфері забезпечення міжнародної інформаційної безпеки», представленому на 69-й сесії Генеральної Асамблеї ООН, є визначення прав та обов’язків держав в інформаційному просторі, стимулювання їх конструктивної та відповідальної поведінки та зміцнення співпраці між ними для протистояння спільним викликам та загрозам в інформаційному просторі з тим, щоб створити мирне, безпечне, відкрите та засноване на співпраці

інформаційне середовище, щоб використання інформаційно-комунікаційних технологій та інформаційних та комунікаційних мереж сприяло повномасштабному соціальному та економічному розвитку та добробуту народів, при цьому не суперечило б цілям забезпечення міжнародного миру та безпеки.

Згідно із запропонованими Правилами, кожна держава має добровільно їх дотримуватися і зобов'язатися:

- дотримуватися загальновизнаних принципів та норм міжнародного права, у тому числі, в цифровому просторі, які включають повагу суверенітету, територіальної цілісності та політичної незалежності всіх держав, дотримання прав та основних свобод людини, а також повагу до різноманіття історії, культури та соціального устрою всіх країн;
- не використовувати інформаційно-комунікаційні технології та інформаційні та комунікаційні мережі для здійснення дій, що суперечать завданням підтримки міжнародного миру та безпеки;
- не використовувати інформаційно-комунікаційні технології та інформаційні та комунікаційні мережі для втручання у внутрішні справи інших держав та з метою підриву їхньої політичної, економічної та соціальної стабільності;
- співпрацювати у боротьбі зі злочинною або терористичною діяльністю з використанням інформаційно-комунікаційних технологій та інформаційних та комунікаційних мереж та стримувати поширення інформації терористичного, сепаратистського чи екстремістського характеру, а також розпалює ненависть на національному, расовому чи релігійному ґрунті;
- запобігати використанню іншими державами своєї домінуючої позиції у сфері інформаційних технологій, включаючи, серед іншого, домінування в інформаційних ресурсах, критичній інфраструктурі, ключових технологіях, продуктах та послугах інформаційно-комунікаційних технологій та інформаційних та комунікаційних мережах, для підриву права держав на незалежний контроль над продуктами та послугами інформаційно-комунікаційних технологій або для створення загроз їх політичній, економічній та соціальній безпеці;

- поважати права та обов’язки кожної держави, відповідно до існуючих норм та правил, законно захищати свій інформаційний простір та критичну інформаційну інфраструктуру від завдання шкоди внаслідок реалізації загроз, втручання в інформаційні процеси, атак та актів інформаційної агресії;
- визнавати, що права, які людина має в онлайновому середовищі, повинні також захищатися і в онлайновому середовищі, повною мірою поважати права та свободи в інформаційному просторі, у тому числі на пошук, отримання, передачу та розповсюдження інформації, зважаючи на те, що відповідно до Міжнародного пакту про політичні та громадянські права (стаття 19) користування цими правами накладає особливі обов’язки та особливу відповідальність, пов’язані з певними обмеженнями, встановленими законом (наприклад, щодо поваги прав та репутації інших осіб; для охорони державної безпеки, громадського порядку, здоров’я чи морального стану населення);
- визнавати, що всі держави повинні відігравати однакову роль у міжнародному управлінні Інтернетом та нести рівну відповідальність за управління Інтернетом, його безпеку, безперервність та стабільність функціонування, а також розвиток для того, щоб сприяти створенню багатосторонніх, прозорих та демократичних міжнародних механізмів управління Інтернетом, які дозволять забезпечити справедливий розподіл ресурсів, сприяти доступу для всіх, а також гарантувати стабільне та безпечне функціонування Інтернету;
- співпрацювати з усіма зацікавленими сторонами, сприяти поглибленню усвідомлення державним, приватним сектором та інститутами громадянського суспільства своєї відповідальності за забезпечення інформаційної безпеки, включаючи формування культури інформаційної безпеки та підтримку зусиль із захисту об’єктів критичної інформаційної інфраструктури;
- розвивати заходи із зміцнення довіри з метою підвищення передбачуваності та зниження ймовірності непорозуміння, а також ризику виникнення конфлікту, зокрема, добровільний обмін інформацією про національні стратегії та організаційні структури, спрямовані на забезпечення інформаційної

безпеки країни, публікацію « білих книг» та обмін найкращими практиками в тих випадках, коли це практично можливо і доцільно;

- сприяти країнам, що розвиваються, у «нарощуванні потенціалу» у сфері інформаційної безпеки та подоланні « цифрового розриву»;
- зміцнювати двостороннє, регіональне та міжнародне співробітництво; сприяти тому, щоб ООН і надалі продовжувала відігравати важливу роль у виробленні міжнародних правових норм у галузі інформаційної безпеки, мирному вирішення міжнародних спорів і врегулюванні конфліктів, підвищенні якісного рівня співпраці держав у сфері інформаційної безпеки;
- прагнути, щоб будь-який конфлікт, непорозуміння вирішувалися за допомогою мирного врегулювання, утримуючись від застосування військової сили або загрози силою, що також стосується й конфліктів в інформаційному просторі (United Nations, 2015).

Як зазначають експерти, в рамках ООН проект документу, запропонований ШОС щодо правил поведінки держав, був знову відхилений. Характер політичної дискусії, що розгорнулася між державами, був обумовлений кількома важливими подіями для сфери міжнародної безпеки – проведення Всесвітньої конференції з міжнародних телекомунікацій (2012 р.), на якій йшлося про потребу досягнення міжнародного консенсусу щодо інформаційної безпеки, міжнародної дискусії, що розгорнулася в рамках проведення Всесвітнього саміту з інформаційного суспільства у Дубаї у 2012 р. навколо проблеми управління Інтернетом, де США виступили з чіткою позицією неприпустимості передачі таких повноважень виключно державі та наполягали на моделі управління за участю багатьох зацікавлених сторін, та масштабний витік інформації за участю Е. Сноудена. США та їх партнери в рамках розвідувального альянсу «Five Eyes» були звинувачені у тому, що вони використовують своє «домінування в інформаційному просторі» у власних інтересах, хоча вирішення питання управління Інтернетом та попередження кібератак є також важливими. Натомість західні держави зазначали, що Правила поведінки держав, представлені ШОС, викликають занепокоєння. Окрім наголошення на державному суверенітеті і територіальності в інформаційному

просторі, у документі суттєво розширюються можливості розвідки, а інтереси безпеки і стійкості режимів домінують. Так, держави ШОС, виступаючи прихильниками концепції «цифрового» або «інтернет-суверенітету», розглядають інформаційний простір як територію, яка є спірною між державами та належним чином підлягає внутрішньому контролю. Запропонований принцип суверенітету в кіберпросторі включає такі чинники: власна юрисдикція держав над інформаційною інфраструктурою та діяльністю на їхніх територіях; право національних урядів розробляти державну політику щодо Інтернету відповідно до власних національних умов; недопущення використовувати Інтернет жодною державою для втручання у внутрішні справи інших країн або загрожувати національним інтересам країн. Але найбільшого занепокоєння, на думку експертів, викликав стратегічний ревізіонізм держав ШОС щодо міжнародної системи захисту прав людини. Так, представлені в документі позиції, часто являють собою порушення інформаційних прав і свобод людини, зафіксованих в Міжнародному пакті про громадянські та політичні права, зокрема, щодо свободи слова та свободи вираження поглядів, розширення прав держави здійснювати внутрішній контроль інформації (McKune, 2015).

Водночас слід зауважити, що у редакції Правил 2015 р. все ж були внесені зміни порівняно з документом 2011 р. Наприклад, було вилучено суперечливий термін «інформаційна зброя», оскільки у тлумаченні авторів Правил під таке визначення могли потрапити, наприклад, соціальні мережі – Twitter і Facebook, які використовувалися під час подій так званої «Арабської весни». Водночас залишився широким для тлумачення пункт, в рамках якого будь-яке використання ІКТ та мереж, яке може вплинути на підтримку міжнародного миру і безпеки, є неприпустимим для підписантів. Раніше це стосувалося саме ворожих і агресивних дій, використання інформаційної зброї та поширення пов’язаних з нею технологій. В новому документі також було змінено підхід до визначення «домінуючого положення в сфері інформаційних технологій». Так, відповідно до нової редакції, домінування в сфері інформаційного та технологічного розвитку (у виробництві інформаційних товарів, послуг, ресурсів, технологічних рішеннях для підтримки критично важливої інформаційної інфраструктури, функціонування мереж) не

повинно підривати право інших країн здійснювати контроль над продуктами і послугами, якщо це може загрожувати їх політичній, економічній чи соціальній безпеці. Цей пункт мав відношення й до проблеми управління Інтернетом. Звісно, для західних демократій такий підхід виявився неприйнятним, як й спроба в рамках практичних заходів із зміцнення довіри у кіберпросторі нав'язати політично зобов'язальні норми поведінки держав з метою обмеження кіберзагроз. Водночас, слід зауважити, що саме зусилля із зміцнення довіри у кіберпросторі є однією з небагатьох сфер, де провідні держави все ж змогли досягнути консенсусу (Rõigas, 2015). На думку експертів, ще однією важливою особливістю Правил є те, що на міжнародному рівні в них запропоновано підхід, що суперечить прийнятим раніше документам. Зокрема йдеться про «Талліннський посібник», в якому обстоюється підхід про застосування до сфери інформаційної безпеки принцип lex lata, тобто закону таким, яким він є, а не lex feranda, закону, яким його можна було б побажати. Таким чином для більшості країн, які виступили проти ухвалення запропонованих ШОС Правил важливим є дотримання позиції, що слід не створювати нові принципи для сфери безпеки в контексті подальшого інформаційного та технологічного розвитку, а адаптувати вже існуючи міжнародно-правові норми до сучасних реалій (Alcântara, 2018; Dunlap, 2021).

Подальший розвиток стратегії інформаційної безпеки в рамках ШОС показав, що для більшості країн-учасниць питання формування регіональної системи інформаційної безпеки тісно пов'язані з проблемою обстоювання власних національних інтересів, які не завжди співпадають з регіональними пріоритетами. Більш того, часто між державами-учасницями можуть виникати інформаційні конфлікти, що передбачають використання різноманітних способів інформаційного протиборства. Тому вкрай важливим напрямом діяльності було визнано сприяння більш активним інформаційним обмінам та реалізація різноманітних спільних програм з метою формування системи регіональної інформаційної безпеки на просторі країн-учасниць.

Під час чергового саміту ШОС в Уфі в 2015 р. особливу увагу було приділено обговоренню питань захисту інформації з обмеженим доступом та інформації, що

становить державну таємницю, забезпечення захисту критично важливих об'єктів та інфраструктури, що для свого вирішення потребують вироблення рішень передусім на міжнародному рівні. Крім того, впровадження і розширення використання ІКТ та мережі Інтернет у різноманітних інфраструктурних проектах, у сфері надання державних послуг, у банківській сфері, у сфері соціального розвитку, культури, науки, освіти призвели до усвідомлення, що не тільки політична, але й економічна, енергетична, інфраструктурна сфери критично залежать від безперебійного функціонування інформаційних систем. Саме тому держави звернули увагу на потребу вирішення питань безпеки, стійкості і захищеності інформаційних систем. А отже, досягнення єдиного розуміння специфіки розвитку інформаційного простору та адекватне реагування на кіберзагрози стають центральними темами для всіх держав-членів ШОС (CCDCOE, 2018). Слід зазначити, що на цьому саміті було офіційно розпочато процедуру приєднання до ШОС Індії та Пакистану, двох ядерних південно-азійських суперників, які до цього мали статус. Під час проведення наступного саміту в Астані вже у 2017 р. обидві держави стали повноправними членами ШОС.

За результатами проведення саміту ШОС в Астані в 2017 р. було ухвалено Декларацію, в якій окреслювалися базові пріоритети діяльності організації. Проблема міжнародної інформаційної безпеки визнавалася важливим напрямом діяльності і розглядалася у контексті двох базових напрямів. По-перше, у розвиток Угоди між урядами держав-членів ШОС про співпрацю в галузі забезпечення міжнародної інформаційної безпеки (2009 р.), держави-члени ШОС оголосили про подальшу діяльність, спрямовану на зміцнення практичної взаємодії з питань протидії пропаганді та виправданню тероризму, сепаратизму та екстремізму в інформаційному просторі. Для цього планувалося виробити ефективні механізми координації діяльності усіх зацікавлених країн, регіональних та міжнародних організацій у двосторонньому та багатосторонньому форматах, у тому числі з відповідними структурами ООН. По-друге, пріоритетним напрямом діяльності залишилося й подальше просування ідеї ухвалення універсального кодексу правил, принципів та норм відповідальної поведінки держав в інформаційному просторі,

зафіксованого у проекті, поданому від держав-членів ШОС до ООН у 2015 р. Ще одним важливим напрямом було також визначено розширення співпраці держав-членів у сфері боротьби зі злочинами в інформаційно-комунікаційній сфері, яка передбачає також участь у розробці відповідного міжнародно-правового документу за центральної координуючої ролі ООН (SCO, 2017). На саміті також було ухвалено Конвенцію ШОС з протидії екстремізму, в якій держави-підписанти з метою протидії екстремістській діяльності, яка нині активно використовує досягнення у сфері інформації і комунікації, зобов'язувалися здійснювати постійний моніторинг ЗМІ та Інтернету задля своєчасного виявлення та запобігання поширенню екстремістської ідеології, обмежувати доступ до екстремістського матеріалу, розміщеному в ЗМІК (OSCE, 2020).

Під час засідання секретарів Ради національної безпеки ШОС у травні 2018 р. у Пекіні офіційні особи обмінялися думками щодо безпеки та стабільності в країнах ШОС та обговорили посилення їх спільних зусиль проти тероризму, сепаратизму та екстремізму, незаконному обігу зброї та наркотичних засобів, транснаціональній організованій злочинності, а також зосередилися на питаннях міжнародної інформаційної безпеки. учасники засідання висловили підтримку подальшим зусиллям, спрямованим на створення архітектури спільної, всеохоплюючої, стійкої, рівної та неподільної безпеки. Така безпека, на їх думку, має базуватися на принципах співробітництва, що необхідно для пошуку колективних відповідей на сучасні виклики і загрози та для захисту миру і стабільності, а також для вироблення скоординованого бачення ШОС спільного майбутнього людства. Сторони також заявили, що світ в даний час трансформується, формується більш різноманітний і багатополярний геополітичний ландшафт, тому сфера міжнародної безпеки переживає серйозні і глибокі зміни. Особливо ці зрушення прослідковуються у сфері інформаційної безпеки. Саме тому знову було наголошено на тому, що ІКТ та мережі продовжують активно використовуватися для вчинення різноманітних злочинних дій, зокрема, для пропаганди різноманітних проявів тероризму, сепаратизму та екстремізму, а також для вербування бойовиків, розширення терористичної діяльності та втручання у внутрішні справи інших держав. Саме тому

слід активізувати діяльність під егідою ООН, спрямовану на вироблення універсальних правил, принципів і норм відповідальної поведінки держав у сфері інформації і комунікації. Таким чином, ШОС вкотре наголосив на потребі ухвалення запропонованих в ООН «Правил поведінки у сфері забезпечення міжнародної інформаційної безпеки», що допоможе забезпечити реалізацію стратегій інформаційну безпеку не тільки на національному або регіональному рівнях, але й сприяти зміцненню довіри та формуванню безпечного інформаційного середовища на глобальному рівні (SCO, 2018).

Наступний саміт ШОС відбувся у 2020 р. в онлайн режимі через обмеження, пов'язані із COVID-19. На зустрічі традиційно обговорювалися питання інформаційної безпеки, результатом чого стала Заява Ради голів держав-членів Шанхайської організації співробітництва про співпрацю у сфері міжнародної інформаційної безпеки. У документі, зокрема, зазначалося, що держави-члени організації досягли безпрецедентного прогресу у розвитку та використанні інформаційно-комунікаційних технологій, які формують глобальний інформаційний простір. Зростання впливу ІКТ на повсякденне життя, а також на політичну, економічну, соціокультурну та інші складові, обумовлює підвищення уваги до проблем інформаційної безпеки як на національному, так й на глобальному рівнях. На думку представників ШОС викликає занепокоєння використанням сучасних інформаційно-комунікаційних технологій у цілях, несумісних із завданнями підтримки міжнародного та регіонального миру, безпеки та стабільності. Тому слід й надалі вдосконалювати механізм та заходи, спрямовані на запобігання міждержавним конфліктам та подолання дефіциту довіри між державами, який може виникати внаслідок протиправного використання ІКТ (наприклад, злочинними угрупованнями, терористами, екстремістами, сепаратистами та ін.). Ключову роль представники ШОС в цих процесах відводять саме ООН, в рамках якої мають узгоджуватися підходи до проблеми міжнародної інформаційної безпеки при цьому держави-члени зазначили, що міжнародне та регіональне співробітництво в сфері міжнародної інформаційної безпеки повинні ґрунтуватися на загальновизнаних принципах міжнародного права, включаючи Статут ООН, зокрема, на принципах

державного суверенітету, політичної незалежності, територіальної цілісності, суверенної рівності держав, врегулювання спорів мирними способами, невтручання у внутрішні справи інших держав, а також поваги до основних прав і свобод людини, які мають першорядне значення для формування мирного, безпечного, відкритого та стабільного глобального інформаційного простору.

Водночас, з огляду на транскордонну природу ІКТ, держави-члени визнають важливість міжнародного співробітництва у сфері забезпечення інформаційної безпеки шляхом активізації зусиль одночасно на національному, двосторонньому та багатосторонньому рівнях. Тут показовим є те, що незважаючи на підтримку існуючих принципів і норм міжнародного права, держави-члени наголосили на важливості ініціативи в ООН щодо вироблення правил, норм і принципів відповідальної поведінки держав в інформаційному просторі та підтвердили намір продовжити спільну роботу та координацію зусиль ШОС на цьому напрямі в рамках ключових профільних переговорних майданчиків ООН. Незмінної залишилася й позиція ШОС й щодо удосконалення системи управління мережею Інтернет. Так, держави-члени визнали необхідність посилення координації діяльності в ООН та в рамках інших міжнародних платформ з питань удосконалення управління Інтернетом, у тому числі забезпечуючи рівні права держав на участь у процесі та посилення ролі Міжнародного союзу електрозв’язку.

У Заяві також йшлося про необхідність досягнення балансу між безпекою та розвитком, що вимагає спільних зусиль усіх країн з метою забезпечення рівного, справедливого та недискримінаційного середовища для ведення бізнесу в галузі нових технологій, а також розробки в рамках міжнародних спеціалізованих установ загальновизнаних технічних стандартів для забезпечення інформаційної безпеки (Ministry of Foreign Affairs of the People’s Republic of China, 2020).

17 вересня 2021 р. у Душанбе відбувся ювілейний саміт глав держав ШОС у віртуальному та очному форматі. Головними темами для обговорення стали зміна геополітичного ландшафту в Південній та Центральній Азії, що має потенційний вплив на архітектуру регіональної безпеки, ситуація в Афганістані та входження Ірану до складу країн-учасниць організації. В ухваленій за результатами проведення

зустрічі Душанбінській декларації про 20-річчя ШОС було приділено увагу й питанням міжнародної інформаційної безпеки. Так, у документі окреслено загальні проблеми регіональної безпеки, що залишаються пріоритетом діяльності організації – боротьба з тероризмом у всіх його формах і проявах, сепаратизмом, екстремізмом, незаконним обігом наркотиків, зброї, боєприпасів і вибухових речовин, транскордонною організованою злочинністю, забезпечення міжнародної інформаційної безпеки, посилення безпеки кордонів, об'єднання зусиль у боротьбі з нелегальною міграцією та торгівлею людьми, відмиванням грошей, економічними злочинами та корупцією. Йшлося також й про вдосконалення механізмів протидії сучасним викликам і загрозам безпеці держави-члени ШОС, зокрема, про створення центрів і структур для протидії сучасним викликам і загрозам у сфері для сучасної системи безпеки. У Декларації також була представлена позиція держав-членів ШОС з питань нерозповсюдження ядерної зброї; заборони розробки, виробництва та накопичення запасів бактеріологічної (біологічної) і токсинної зброї; заборони розробки, виробництва, накопичення і використання хімічної зброї та щодо її знищення. Водночас у документі підкреслювалося, що космічний простір має залишатися вільним від будь-якої зброї, а тому важливим є забезпечення суворого дотримання існуючої правової бази, яка гарантує використання космосу виключно в мирних цілях.

У питаннях міжнародної інформаційної безпеки держави-члени ШОС підтвердили попередньо проголошені принципи. Зокрема, у документі підкреслювалася визначна роль сучасних ІКТ для створення конкурентних переваг держав регіону, а також для створення можливості подальшого прогресу усього людства, засуджувалися різноманітні форми дискримінації, які перешкоджають розвитку інформаційної економіки та цифрового суспільства. Водночас держави-члени висловили серйозні занепокоєння щодо зростання загрози для інформаційної безпеки, які включають використання ІКТ з метою вчинення транснаціональних і глобальних злочинів або дестабілізації міжнародного миру та безпеки. Держави також засудили тенденцію мілітаризації ІКТ та кіберпростору і закликали сприяти саме мирному використанню інформаційних і технологічних досягнень задля

створення безпечного, справедливого і відкритого інформаційного простору, побудованого на принципах поваги до суверенітету інших країн і невтручання в їх внутрішні справи.

Враховуючи глобальний характер поширення негативних наслідків злочинного використання ІКТ, вирішальне значення та підвищення ефективності протистояння сучасним викликам і загрозам є поглиблення міжнародного співробітництва. Тому держави-члени вкотре підкреслили ключову роль ООН у протидії кіберзагрозам і знову висловили підтримку процесу вироблення універсальних правил, принципів і положень відповідальної поведінки для країн у цій сфері. Тому представники ШОС висловили готовність і надалі співпрацювати в рамках спеціалізованих переговорних платформ ООН та інших міжнародних інституцій для створення ефективних механізмів забезпечення міжнародної інформаційної безпеки. незмінної залишилася й позиція держав-членів ШОС щодо підтримки рівних права країн на регулювання Інтернету та їхнє суверенне право регулювати національні сегменти Інтернету (Ministry of External Affairs. Government of India, 2021).

Висновки до другого розділу

Сучасна архітектура безпеки АТР, яка формувалася упродовж тривалого часу, набула унікальних характеристик, які мають вирішальне значення для реалізації регіональної політики інформаційної безпеки. Нині вона включає як традиційні, історично-сформовані ознаки, так і нові, обумовлені швидкоплинними процесами інформаційного та науково-технологічного розвитку. Так, значна кількість конфліктів та територіальних суперечок між державами регіону, суттєві відмінності в економічних та політичних моделях розвитку, зіткнення геополітичні та геоекономічних інтересів США та КНР та поширення практики використання двосторонніх стратегічних альянсів між США та державами-союзниками у регіоні продовжують активно впливати на характер дво- та багатосторонніх відносин у сфері безпеки, визначаючи загальні характеристики регіональних підходів до

формування системи безпеки. Значним чинником формування сучасної системи регіональної безпеки також виступає розширення географічного регіону АТР за рахунок геополітичного концепту Індо-Тихоокеанського регіону, що призвело не тільки до збільшення країн, які відтепер співвідносяться з АТР, але й до зростання сукупного потенціалу регіону. Водночас, інформаційний і науково-технологічний розвиток країн регіону не тільки спричинив значний вплив на базові характеристики архітектури регіональної безпеки АТР, суттєво змінивши їх характер, але й призвів до виокремлення в самостійний чинник нових викликів і загроз, пов'язаних власне з інформаційним протиборством, кіберзлочинністю та кібертероризмом.

Ключову роль у формуванні системи безпеки АТР відіграють регіональні інститути, до пріоритетів діяльності яких входять питання інформаційної безпеки, що розглядаються як фундаментальні, оскільки впливають на подальший поступальний розвиток регіону в цілому. Пріоритети діяльності Асоціації Південно-Східної Азії (АСЕАН) у сфері інформаційної безпеки зосереджені на формування стійкого і безпечного кіберсередовища, що вкрай важливо для держав-членів, враховуючи швидкі темпи їх інформаційного і технологічного розвитку та залежність від технологічних інновацій та іноземних інвестицій у НДДКР. Основними напрямами діяльності організації у сфері кібербезпеки є вироблення спільних підходів на рівні АСЕАН до вирішення проблем кібербезпеки із врахуванням інтересів і особливостей різних держав-членів; нарощування регіонального кіберпотенціалу та побудови регіональної системи управління ризиками і загрозами у кіберсередовищі; кібердипломатія і розвиток співпраці між усіма державами регіону у сфері кібербезпеки та співробітництво на рівні міжнародних інститутів, зокрема, в рамках ООН з питань впровадження правил відповідальної поведінки держав у кіберпросторі.

Сучасними пріоритетами політики у сфері інформаційної безпеки в рамках Шанхайської організації співробітництва (ШОС) є розробка і реалізація заходів у сфері забезпечення міжнародної інформаційної безпеки відповідно до зміни типу і характеру інформаційних загроз; забезпечення інформаційної безпеки критично важливих структур держав ШОС; впровадження ефективних механізмів координації

діяльності усіх держав-членів у сфері протидії пропаганді та виправданню тероризму, сепаратизму та екстремізму в інформаційному просторі; співпраця держав-членів у сфері боротьби зі злочинним використанням інформаційно-комунікаційних технологій і мереж; впровадження заходів, спрямованих на запобігання міждержавним інформаційних конфліктів та подолання дефіциту довіри, який виникає внаслідок використання високих технологій та мереж у протистоянні між державами; подальший розвиток норм міжнародного права щодо обмеження поширення та застосування інформаційної зброї; подальше просування ідеї ухвалення універсального кодексу правил, принципів та норм відповідальної поведінки держав в інформаційному просторі, зафіксованого у проекті, поданому від держав-членів ШОС до ООН. Особливу роль у визначенні пріоритетів діяльності організації у сфері інформаційної безпеки відіграють РФ та КНР, які намагаються використати інститут для обстоювання власних національних інтересів у регіоні.

Пріоритетом діяльності у сфері інформаційної безпеки Чотиристороннього діалогу з питань безпеки (QUAD) є формування власної системи кібербезпеки, яка передбачає створення потенціалу стійкості інформаційної інфраструктури, особливо у контексті подальшого розвитку якості зв’язку і появи мереж 5G, з метою усунення вразливостей для кібербезпеки держав-учасниць; вироблення загальних принципів і стандартів у сфері кібербезпеки; впровадження ефективних механізмів протидії різноманітним кіберзагрозам, захист критичної інформаційної інфраструктури; впровадження механізмів боротьби з кіберзлочинністю; розвиток кадрового потенціалу у сфері кібербезпеки; розробка та впровадженні стандартів безпеки програмного забезпечення в рамках QUAD; формування відкритої, доступної та безпечної технологічної екосистеми, що базується на спільних демократичних цінностях та повазі до універсальних прав людини тощо. Стратегія QUAD у сфері кібербезпеки спрямована на створення ефективної системи захисту від кіберзагроз передусім з боку Китаю. Для цього було обрано стратегію формування «кіберстійкості» замість «наступальних кіберможливостей», що вважається більш надійний спосіб вирішення широко кола проблем кібербезпеки в усьому Індо-Тихоокеанському регіоні.

РОЗДІЛ 3
ТРАНСФОРМАЦІЯ ПРІОРИТЕТІВ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯПОНІЇ ТА ІНДІЇ

3.1. Сучасні пріоритети стратегії інформаційної безпеки Японії

Особливості стратегії інформаційної безпеки Японії обумовлені цілою низкою факторів, які характеризують унікальний національних шлях інформаційного розвитку держави в цілому. Так, перехід до нового етапу цивілізаційного розвитку, що базується на широкому впровадженні сучасних інформаційно-комунікаційних технологій, відбувався паралельно з країнами західного світу. Нині на порядку денному постало питання розбудови «Суспільства 5.0» та впровадження сучасних наукових і технологічних досягнень у різні сфери життєдіяльності суспільства. Саме тому проблеми розробки і практичної реалізації стратегії інформаційної безпеки для країни є вкрай актуальними.

Як зазначають експерти, Японія характеризується високим рівнем ефективності поєднання системи державного управління, інвестицій у НДДКР та сприяння поширенню технологій у суспільстві (Сябро, 2019с). Станом на кінець 2021-початок 2022 рр. постійними користувачів Інтернету були 94 % японського населення. При цьому зросла й кількість користувачів соціальних мереж до 102 млн осіб, що становить 81,1 % від загальної кількості населення. Найбільш популярними мережами є LINE, Meta / Facebook, YouTube, Instagram, TikTok, LinkedIn, Snapchat, Twitter. Кількість мобільних з'єднань перевищила показник 202,1 млн (161 % населення), що свідчить про наявність не одного, а кількох приладів на душу населення (Digital 2022: Japan, 2022). Важливим показником значного науково-технологічного прогресу Японії є розвиток її національної інноваційної системи, яка дозволила державі ефективно інтегруватися у глобальні інноваційно-технологічні ланцюжки. Це дозволяє стверджувати, що нині Японія на рівні зі США та країнами ЄС виступає ключовим виробником інноваційних продуктів та базових технологій. Так, в аналітичному дослідженні «Глобальний

індекс інновацій 2021 р. Відстеження інновацій через кризу COVID-19» держава посіла 13-те місце (4-те по регіону) і увійшла до переліку 15 найбільш інноваційних держав світу, демонструючи стійку тенденцію до постійного розвитку інновацій (WIPO, 2021).

Японія активно включилася у Четверту індустріальну революцію, намагаючись використати для цього свої високотехнологічні можливості та інноваційний потенціал. Визначальним фактором, який дозволяє успішно реалізовувати стратегію входження держави до нового технологічного укладу, є передусім ефективне поєднання зусиль усіх зацікавлених сторін – держави, бізнесу, науки та некомерційних структур. Так, у 2010 р., майже одночасно з Німеччиною, урядом було представлено «Білу книгу з питань інформації та комунікації», в якій підкреслювалося, що держава має досвід і можливості для подолання нового типу викликів і загроз, розпочавши перехід до наступного технологічного укладу. У 2016 р. кабінет міністрів Японії оприлюднив концепцію «Суспільства 5.0», яке має базуватися на технологічних досягненнях Четвертої промислової революції. Пандемія COVID-19 суттєво прискорила темпи розробки і впровадження технологій, особливо тих, які дозволили більш ефективно протистояти новій загрозі (Kim, 2021).

Зазначимо, що новий японський план «Суспільство 5.0», виявився більш далекосяжною концепцією, ніж Четверта промислова революція, оскільки він передбачає повну трансформацію японського способу життя шляхом стирання кордону між кіберпростором і фізичним простором. Суспільство 5.0, яке також називають «суперрозумним суспільством», передбачає формування сталої, інклюзивної соціально-економічної системи, що базується на цифрових технологіях, таких як аналітика великих даних, штучний інтелект, Інтернет речей і робототехніка. «Кіберфізична система», в якій кіберпростір і фізичний простір тісно інтегровані, стає поширеним технологічним способом, що підтримує «Суспільство 5.0». (UNESCO, 2019). Таким чином, зростання інформаційно-технологічного та інноваційного потенціалу держави відкривають перед Японією можливості модернізації економічної, політичної та безпекової сфер. Водночас, зростання

залежності від технологій та інновацій призвело до виникнення нових типів викликів і загроз, які вплинули на стратегію національної безпеки держави та обумовили включення до її пріоритетів питань інформаційної безпеки. Японія перетворилася на об'єкт постійних інформаційних атак з боку не тільки злочинних угруповань та шахраїв, але й ворожих держав, які намагалися використати політично мотивовані атаки на інформаційний простір держави як засіб тиску на японський уряд. І незважаючи на те, що держава входить до п'ятірки країн з найкращим рівнем захищеності національного інформаційного простору від різноманітних загроз, кількість атак постійно зростає (Top 14 Cybersecurity Breaches in Japan, 2022).

Згідно із дослідженнями «Глобальний рейтинг кібербезпеки (2020 р.)» МСЕ та «Рейтинг вразливості від кіберзагроз» (2020 р.), Японія входить до числа найбільш кібербезпечних країн (7-ме місце відповідно у першому дослідженні і 6-те – у другому) (ITU, 2020; Global Cybersecurity Exposure Index, 2020). Крім того, за даними Statista у 2021 р., кількість розкритих кіберзлочинів в Японії зросла на 23,6% з історичним максимумом у 12 209 випадків (Top 14 Cybersecurity Breaches in Japan, 2022). Це стало результатом тривалої діяльності уряду Японії, спрямованої на розбудову національної системи інформаційної безпеки та оборони, співпраці усіх зацікавлених сторін. Водночас загроза залишається вкрай критичною, враховуючи ступінь розвитку і темпи проникнення технологій в японське суспільство.

Розвиток стратегії інформаційної безпеки Японії до кінця 1990-х рр. відбувався переважно за ініціативи приватного сектору. Ситуація змінилася на початку 2000-х рр., коли відбулася серія атак саме на урядові веб-сайти, що показало слабкість японської політики інформаційної безпеки. Стало зрозумілим, що необхідно терміново визначати пріоритети і напрями національної політики у цій сфері, а також розробити систему обов'язків і відповідальності державних органів влади за їх реалізацію (Bartlett, 2019). У серпні 1999 р. уряд ухвалив Закон про заборону незаконного доступу, а у вересні цього ж року була проведена Конференція міністерств і відомств з питань інформаційної безпеки. Результатом ініціатив уряду стало ухвалення «Плану дій щодо розвитку інфраструктури для

боротьби з хакерами». У цей же час в рамках нещодавно створеного Стратегічного штабу сприяння розвитку суспільства передових інформаційних і телекомунікаційних мереж була створена Рада із сприяння заходам інформаційної безпеки, головним завданням якої стало встановлення зв'язку між усіма зацікавленими сторонами (органами державної влади, представниками підприємств критичної інфраструктури, представниками приватного сектору), а також ухвалено Спеціальний план дій щодо реагування на акти кібертероризму у критичній інфраструктурі (Bartlett, 2019).

Тривалий час в Японії точилася дискусія щодо того, хто має взяти на себе головну відповідальність за розробку і реалізацію політики кібербезпеки – Агентство національної поліції чи Агентство оборони Японії (пізніше – Міністерство оборони). Агентство національної поліції відносно швидко усвідомило, що кіберзлочинність ставатиме дедалі більшою проблемою. Тому, починаючи з 2001 р. почало скликати регулярні зустрічі з представниками промисловості, науковцями та іншими зацікавленими сторонами для обговорення питань кібербезпеки, а також виступило ініціатором створення Cyber Force Center для надання технічної підтримки у боротьбі з кіберзлочинністю. Натомість експерти були занепокоєні ситуацією і висловлювали побоювання, що перекладання відповідальності виключно на Агентство національної поліції чи Агентство оборони Японії не дасть можливості розробити і реалізувати ефективну стратегію інформаційної безпеки, яка б відповідала існуючим міжнародним стандартам, що може негативно вплинути на подальші можливості Японії технологічно розвиватися та посідати позиції світового лідера інноваційного науково-технологічного розвитку (Bartlett, 2019). Важливу роль у формуванні системи інформаційної безпеки Японії у той час відігравала також група JPCERT/CC, створена ще у 1992 р. як волонтерська оперативна група, що працювала у приватному секторі (хоча й отримували підтримку від Міністерства міжнародної торгівлі та індустрії). JPCERT функціонувала як головна японська група швидкого реагування на інциденти комп'ютерної безпеки (CSIRT) і головним чином відповідала за кібербезпеку Японії до того моменту (Bartlett, 2019).

Для того, щоб урівноважити внутрішні потреби у формуванні ефективної стратегії інформаційної безпеки та необхідність дотримання міжнародних стандартів, було вирішено залучити до процесу вироблення національної стратегії інформаційної безпеки Міністерство економіки, торгівлі та промисловості та Міністерство внутрішніх справ і комунікації. Обидва відомства мали можливість вибудувати потрібний баланс інтересів і були зацікавлені у формування ефективної системи інформаційної безпеки. Наприклад, Міністерство економіки, торгівлі та промисловості було зацікавлене у виробленні ефективних механізмів боротьби з кіберзлочинністю, що негативно впливала на економічну конкурентоспроможність Японії, оцифровування комерційної діяльності та надання інформаційних послуг. Міністерство внутрішніх справ і комунікації було стурбовано наслідками поширення шкідливого програмного забезпечення та кібератак на мережі та інтернет-провайдерів. Крім того, обидва міністерства були зацікавлені в розширенні власної юрисдикції та можливостей впливати на стратегію розвитку економіки держави. На певному етапі міністерства вирішили об’єднати свої зусилля, а також залучити до цього альянсу Агентство національної поліції та Агентство оборони Японії (з 2012 р. було залучено ще й Міністерство закордонних справ), що дало можливість досягти певного консенсусу у питаннях інформаційної безпеки. Зокрема, незважаючи на розбіжності між цими структурами у баченні політики інформаційної безпеки, усі вони погодилися з тим, що захист критичної інфраструктури від кібератак є ключовим пріоритетом держави і важливої передумовою її подальшого поступального розвитку (Bartlett, 2019).

Під час регулярних зустрічей зазначених відомств за участю представників приватного сектору й було вироблене рішення про розробку Першої національної стратегії інформаційної безпеки. Дотримуючись політичних рекомендацій, ухвалених під час зустрічі, у травні 2005 р. прем’єр-міністр розпорядився створити Раду з питань політики інформаційної безпеки на чолі з Головним секретарем кабінету міністрів, до складу якої увійшли: міністр внутрішніх справ і комунікації, міністр економіки, торгівлі та промисловості, голова Національної комісії

громадської безпеки, генеральний директор Агентства оборони Японії (пізніше міністр оборони) і Державний міністр з питань науки і технологій (Bartlett, 2019).

Отже, першу спробу запропонувати механізм забезпечення інформаційної безпеки японський уряд здійснив у 2006 р., оприлюднивши Першу національну стратегію інформаційної безпеки « На шляху до створення надійного суспільства» . У документі, зокрема, підкреслювалося, що Японія в повній мірі усвідомлює роль і значення технологій для подальшого розвитку держави, а також зростання вразливості інформаційного простору та інформаційної інфраструктури. Саме тому уряд ще у 2005 р. змушений був розпочати створення відповідних структур та підрозділів з питань інформаційної безпеки в рамках своєї компетенції. Так, було створено Національний центр інформаційної безпеки (NISC) при Секретаріаті Кабінету Міністрів та Раду з політики інформаційної безпеки при Стратегічному штабі сприяння розвитку суспільства передових інформаційно-телекомунікаційних мереж (Стратегічний штаб ІТ), діяльність яких була спрямована на розробку стратегії і поетапного плану дій для забезпечення національної інформаційної безпеки як складової загальної програми розбудови «Електронної Японії».

Основними принципами національної інформаційної безпеки, згідно із Стратегією, було визначено такі: стратегія інформаційної безпеки має відповідати пріоритетам стратегії економічної модернізації на основі широкого використання сучасних високих технологій, стратегія має сприяти підвищенню якості життя населення шляхом впровадження нових інформаційних сервісів, а також має відповідати на сучасні виклики і загрози, спричинені бурхливим інформаційним та технологічним розвитком. Для цього необхідно реалізувати такі цілі і задачі: створити середовище для безпечного використання ІКТ, досягнути балансу між поняттями «зручність» та «безпека» для громадян, які користуються інформаційними послугами, створити нову модель державно-приватного партнерства у сфері інформаційної безпеки (Information Security Policy Council, 2006).

Для досягнення окреслених цілей у Стратегії планувалося здійснити такі практичні кроки: 1) удосконалення системи державно-приватного партнерства, де

урядові структури на всіх рівнях мають вибудовувати ефективну систему взаємодії із дотриманням вимог до інформаційної безпеки мереж і ресурсів, безперебійного використання об'єктів інфраструктури, сприяти впровадженню сучасних технологій забезпечення інформаційної безпеки, швидко реагувати на кіберінциденти та усувати їх наслідки, удосконалювати системи обміну інформацією, підвищувати рівень інформаційної грамотності чиновників і співробітників державних структур; підприємства мають сприяти розробці заходів, які підвищуватимуть рівень інформаційної безпеки, зокрема, шляхом створення сприятливого середовища для удосконалення системи корпоративного управління, що враховує вимоги до інформаційної безпеки функціонування підприємств, надання високоякісних продуктів і послуг, пов'язаних з інформаційною безпекою, сприяти розвитку людських ресурсів, що займаються питаннями інформаційної безпеки, удосконалювати системи швидкого реагування на інформаційні загрози і атаки; 2) сприяння формуванню і розвитку міжгалузевої інфраструктури інформаційної безпеки; 3) налагодження ефективної системи впровадження установами НДДКР сучасних технологій у сфері інформаційної безпеки (науково-дослідний проект Grand Challenge) і розвиток технологій з метою реалізації фундаментальних технологічних інновацій з довгостроковою перспективою; 4) сприяти розробці нових правових норм у сфері інформаційної безпеки та формування сучасних « стандартів безпеки» ; 5) сприяння міжнародному партнерству та співробітництву у сфері інформаційної безпеки (Information Security Policy Council, 2006).

У Стратегії також зазначалося, що для досягнення окреслених завдань, необхідно удосконалити функціонування Національного центру інформаційної безпеки (NISC), до пріоритетів діяльності якого віднесено: підготовка базових урядових стратегій політики у сфері інформаційної безпеки, розробка технологічних стратегій у сфері інформаційної безпеки із врахуванням досягнень науки і техніки та поширення інновацій у японському суспільстві, моніторинг та оцінка заходів інформаційної безпеки уряду, аналіз впливу ефективності реалізації заходів інформаційної безпеки на систему захисту критичної інформаційної інфраструктури, розробка та перегляд Керівних принципів щодо формулювання

«Стандартів безпеки», настанов тощо, координація діяльності всіх зацікавлених сторін, спрямованої на підвищення рівня національної безпеки, сприяння міжсекторальним заходам у сфері інформаційної безпеки та розширення участі у міжнародних проектах з питань інформаційної безпеки (Information Security Policy Council, 2006).

Таким чином, Перша національна стратегія інформаційної безпеки «На шляху до створення надійного суспільства» стала першим етапом розвитку політики інформаційної безпеки Японії. Саме в рамках її реалізації держава змогла поєднати зусилля усіх зацікавлених сторін, зробити питання інформаційної безпеки ключовим у всі інших політичних ініціативах, пов'язаних з розвитком ІКТ та мереж, змогла визначити інформаційну безпеку як ключове питання не тільки інформаційного і технологічного розвитку, а й економічного та суспільного (поставлені пріоритети досягнути цілей сталого економічного розвитку, підвищення якості життя, гарантувати високий загальний рівень безпеки суспільства за рахунок використання ІКТ), посприяла створенню безпечного середовища ІТ, яке базується на сучасних досягненнях науки і техніки, запровадила власну модель державно-приватного партнерства у сфері інформаційної безпеки. Таким чином Японія намагалася заявити про себе як про державу-лідера у сфері інформаційної безпеки, реалізуючи завдання утвердити « японську модель» безпеки, що базується на поєднанні трьох принципів – «висока якість, висока надійність, високий рівень безпеки» (Information Security Policy Council, 2009).

У 2009 р. було оприлюднено Другу національну стратегію інформаційної безпеки «Прагнення до сильної «особистості» та «суспільства» в епоху «інформаційних технологій» , яка містила цілу низку змін і доповнень у порівняні з попереднім документом. Як підкреслюється у самому документі, нова стратегія була розроблена на основі аналізу впровадження Першої національної стратегії. По суті вона є своєрідним узагальненням політики у сфері інформаційної безпеки, яка доповнювалася й іншими документами, що стосуються інформаційної безпеки діяльності державних органів влади, захисту критичної інфраструктури та постійного моніторингу ефективності реалізації пріоритетів національної

інформаційної безпеки, зокрема, «Стандарт заходів у сфері інформаційної безпеки органів державної влади», «Другий план дій щодо підвищення рівня інформаційної безпеки критичної інфраструктури», План дій «Безпечна Японія» та сприяння раціональному та сталому вдосконаленню політики», «Ідеальне суспільство та оцінка політики інформаційної безпеки в Японії» тощо. У представленій Другій стратегії було подано аналіз ефективності реалізації завдань попередньої стратегії, представлено перспективний аналіз подальшої діяльності держави у сфері інформаційної безпеки, конкретизовано основні принципи і завдання нової стратегії, роз'яснені основні кроки, заплановані на термін до 2012 р., визначено механізми підтримки реалізації стратегії на національному рівні (Information Security Policy Council, 2009).

Зокрема, у документі зазначалося, що слід поступово відходити від загальнотеоретичних рамок Першої стратегії і активно реалізовувати закладені пріоритети на практиці у наступному періоді – до 2012 р. і далі. При цьому обов'язково слід враховувати як нові характеристики інформаційного середовища, так й нові виклики і загрози, які з'явилися з моменту виходу попередньої стратегії. У Другій стратегії було закладено реалізацію таких пріоритетів: створення безпечного IT-середовища, перетворення питання інформаційної безпеки на базовий принцип подальшого технологічного розвитку держави, досягнути статусу передової країни світу у сфері забезпечення інформаційної безпеки, створення ефективної системи швидкого реагування на інформаційні виклики і загрози та запобігання ним, підготовка населення до життя у суспільстві високих технологічних ризиків, розширення програм міжнародного співробітництва у сфері інформаційної безпеки, що дозволить, з одного боку, продемонструвати успіх держави та стати провідною державою-зразком ефективної інформаційної безпеки, а з другого, – орієнтуватися на міжнародні стандарти у сфері інформаційної безпеки та активно їх впроваджувати на національному рівні (Information Security Policy Council, 2009).

Для досягнення поставлених завдань слід і надалі удосконалювати систему державно-приватного партнерства, щоб забезпечити рівноправну участь усіх

зацікавлених сторін (органів центральної і місцевої державної влади, структур, відповідальних за розвиток і підтримку функціонування критичної інфраструктури, підприємств та індивідів) у реалізації стратегії інформаційної безпеки. У сфері державного управління слід у процесі реалізації стратегії електронного урядування створювати безпечне і комфортне інформаційне середовища для надання державних послуг населенню, удосконалювати та систематизувати роботу державних структур з питань управління інформаційною безпекою в органах державної влади, розвивати кадровий потенціал персоналу, що забезпечує інформаційну безпеку у структурі державного управління, посилювати можливості швидкого реагування на інформаційні інциденти та виходу з критичних ситуацій, викликаних порушенням системи інформаційної безпеки, активізувати взаємодію між центральними органами влади та органами місцевого управління у сфері інформаційної безпеки. Для аналізу політики у сфері інформаційної безпеки, базових статистичних показників, визначення ефективності діяльності урядових структур, розробки подальших цілей і завдань діяльності уряду в цій сфері органи державної влади мають розробляти «Річний звіт про інформаційну безпеку» (Information Security Report) (Information Security Policy Council, 2009).

Структури і відомства, відповідальні за розвиток і підтримку функціонування критичної інфраструктури, мають працювати над мінімізацією інформаційних загроз для критичної інфраструктури, співпрацюючи як з державним, так й з приватним сектором, з метою запобігання негативного впливу на громадян, їхню соціально-економічну діяльність, забезпечення стійкості системи надання різноманітних інформаційних послуг, а також швидкого відновлення системи після завдання по ній ударів чи збоїв у діяльності. Для цього слід розширити автономні можливості провайдерів інформаційних послуг оперативно реагувати на виникнення IT-загроз, вживати потрібні заходи та співпрацювати з іншими зацікавленими сторонами задля створення стійкого і безпечного інформаційного середовища, швидкого реагування на загрози та ліквідацію їх наслідків. Важливим також є постійний інформаційний обмін між усіма зацікавленими сторонами щодо потенційного чи реального виникнення IT-загроз, для посилення заходів

інформаційної безпеки соціальної інфраструктури. Слід зазначити, що уряд Японії від самого початку взяв за основу політику неприховування випадків здійснення інформаційних атак та постійного інформування громадян про небезпеку та заходи її усунення, які вживаються усіма задіяними у системі інформаційної безпеки. Наприклад, важливу роль в постійному обміні інформацією між усім зацікавленими сторонами щодо виникнення небезпек і загроз відіграє Секретаріат Кабінету Міністрів, а для оперативної взаємодії з партнерами, зацікавленими сторонами, зовнішніми організаціями працює система CEPTOAR для кожної галузі, Рада ж CEPTOAR повинна інформувати офіційні та неофіційні структури про IT-інциденти (Information Security Policy Council, 2009).

Високі стандарти інформаційної безпеки мають також впроваджуватися й на підприємствах. Як підкреслюється у документі, стрімке старіння нації призвело до виникнення проблеми пошуку нових підходів до втримання балансу у суспільстві. Проникнення сучасних технологій на виробництво, поступове збільшення кількості робототехніки та комп'ютеризація підприємств може на даному етапі допомогти запобігти економічній кризі. Водночас, це стає ще одним важливим виміром політики у сфері інформаційної безпеки для забезпечення стійкості і надійності інформаційного середовища підприємств Японії. Ускладнює ситуацію й зростання залежності виробничих потужностей від іноземних інвестицій та аутсорсингу, а також прагнення Японії й надалі інтегруватися до глобального ланцюжку інноваційного виробництва. Таким чином, в умовах зростання глобальної конкуренції здатність держави гарантувати високі стандарти інформаційної безпеки може стати визначальним чинником присутності на регіональному та глобальному ринку продуктів і послуг. Для цього у стратегії передбачено такі кроки: узгодження підходів до вироблення і реалізації стандартів корпоративної інформаційної безпеки; розвиток системи оперативного реагування на виникнення загроз для підприємств інформаційної індустрії; розробка заходів, що сприяють більшій стійкості бізнесу до інформаційних загроз; впровадження стандартів інформаційної безпеки як на великих, так й на малих підприємствах; впровадження високих стандартів інформаційної безпеки у роботу японських компаній за межами держави

(наприклад, впровадження ефективних механізмів захисту персональних даних клієнтів та партнерів); розвиток системи державно-приватного партнерства у сфері інформаційної безпеки (Information Security Policy Council, 2009).

На індивідуальному рівні планується й надалі підвищувати рівень інформаційної грамотності серед різних вікових груп населення. Це дає можливість, з одного боку, забезпечити активне використання високих технологій населенням та ще більш широке їх проникнення у суспільство, а з другого, підвищити рівень інформаційної безпеки через обізнаність громадян у тому, як і чому слід дотримуватися стандартів безпеки під час використання ІКТ і мереж (Information Security Policy Council, 2009).

У стратегії також йдеться про підвищення рівня технічних спроможностей держави гарантувати високі стандарти інформаційної безпеки. Зокрема, йдеться про антивірусне програмне забезпечення, комп'ютерні програми та програмне забезпечення для мобільної телефонії, про програмне забезпечення у сфері інформаційної безпеки для об'єктів критичної інфраструктури. Особливе значення приділялося роботі з громадянами, особливо літнього віку, щодо актуальності використання програмних продуктів у сфері інформаційної безпеки, що має суттєво зменшити ризики та підвищити рівень довіри до використання ІКТ і мереж. Окрім цього значну увагу було приділено розробці національного законодавства у сфері інформаційної безпеки та узгодженню норм з вже діючими нормами національного права (Information Security Policy Council, 2009).

У 2013 р. Рада з питань політики у сфері інформаційної безпеки (нині – Стратегічний штаб з питань забезпечення кібербезпеки) у розвиток стратегії інформаційної безпеки оприлюднила першу національну «Стратегію кібербезпеки» Японії. У лютому 2013 р., виступаючи на черговій сесії Парламенту, прем'єр-міністр Сіндзо Абе наголосив, що необхідно посилити заходи у сфері інформаційної безпеки у відповідь на зростання масштабів кіберзлочинів та кібератак, спрямованих як проти певних структур чи осіб, так й проти інформаційної інфраструктури в цілому. У березні того ж року були утворені спеціальні поліцейські підрозділи, які мали боротися з кіберзлочинністю та політично мотивованою інформаційною

агресією, яка виникає усередині держави або за її межами. Загони кіберполіції планувалося розташувати в Осаці, Токіо та інших стратегічно важливих районах. До складу загонів входять фахівці, які мають досвід роботи у сфері інформаційної безпеки в приватних компаній, і які вільно володіють англійською, китайською, корейською та російською мовами (Nitta, 2014).

У квітні 2013 р. Міністерство внутрішніх справ і комунікацій організувало Науково-дослідний центр інформаційної безпеки, до пріоритетів діяльності якого увійшла розробка технологій захисту від кібератак із використанням методів їх практичного виявлення. Основними завданнями Центру було визначено: створення спільної платформи для науково-дослідних інститутів кібербезпеки, які стануть центрами зосередження всіх знань та досвіду Японії у цій галузі; розробка основних практичних принципів протидії новим кіберзагроз; впровадження суспільного досвіду у нові розробки; а також розширення співпраці з країнами Європи, Азії та США у галузі міжнародної інформаційної безпеки. Такий підхід, з одного боку, має сприяти оптимізації моніторингу інформаційних мереж, розширенню можливості аналізу та висновків щодо ефективності діючої стратегії у сфері інформаційної безпеки, з другого, – інтенсифікації обміну інформацією та співробітництву для розробки більш рішучих заходів у сфері безпеки (Nitta, 2014).

У проекті нової стратегії 2013 р., представленої для обговорення у травні, зокрема, зазначалося, що за останні роки розмір та масштаб кіберзагроз для Інтернет-простору суттєво збільшився і має тенденцію до подальшого зростання. Тому, в умовах, коли кіберпростір перетворився на невід'ємну частину життя багатьох японців, став важливим механізмом вирішення нагальних проблем у суспільстві та продемонстрував колосальний потенціал для економічного зростання та інноваційної діяльності, кібератаки несуть реальну загрозу для функціонування суспільства і стали однією з першочергових проблем національної безпеки та управління ризиками (Nitta, 2014). Прагнення Японія продемонструвати свій інформаційний і інноваційний потенціал з тим, щоб підтримати образ однієї з найбільш інформаційно-розвинутих держав світу, вимагає від держави не тільки демонстрації успіхів у сфері НДДКР, але й забезпечення високого рівня безпеки

використання сучасних технологій і мереж. Тому на порядку денному постало питання про ухвалення оновленої стратегії інформаційної безпеки, яка б врахувала б нові виклики і загрози і запропонувала б ефективні механізми протидії ним (Nitta, 2014).

Отже, у червні 2013 р. було ухвалено першу Стратегію кібербезпеки Японії, основними цілями якої стали виведення проблеми кібербезпеки на більш високий рівень, підвищення ефективності дій у відповідь на зростання проблеми поширення кіберзагроз, розробка плану дій та зміцнення співробітництва на основі принципів соціальної відповідальності та забезпечення вільного і безпечного обміну інформацією. У стратегії було чітко визначено ролі і завдання всіх зацікавлених сторін – органів державної влади та місцевого самоврядування, підприємств інфраструктури, комерційних організацій, науково-дослідних інститутів, окремих користувачів і компаній, які здійснюють діяльність через Інтернет (The Government of Japan, 2013).

Основними напрямами діяльності на рівні уряду держави на період до 2015 р. було визначено: забезпечення надійності та стійкості кіберпростору шляхом підвищення рівня інформаційної безпеки та забезпечення захисту від кібернападів; створення нових структур, що сприятимуть динамічному розвитку кіберпростору, націлені на стимулювання науково-дослідної діяльності, залучення на конкурентній основі нових кадрів для забезпечення кібербезпеки та освіти громадян з питань кібербезпеки; сформулювати завдання щодо забезпечення безпеки кіберпростору, ґрунтуючись на нормах і принципах міжнародного права у сфері інформаційної безпеки та міжнародному співробітництві (Nitta, 2014).

Важливу роль у реалізації Стратегії кібербезпеки було відведено Національному центру інформаційної безпеки (НЦІБ), який має перетворитися на національну координаційну структуру з подальшою перспективою реорганізації у Центр кібербезпеки. Для Центру було суттєво розширено повноваження та перелік обов’язків. Так, до 2013 р. НЦІБ переважно відповідав за розробку політики та стратегії кібербезпеки, обмін інформацією з вітчизняними та міжнародними партнерами, але йому не вистачало повноважень для того, щоб стати реальним

центром аналізу кіберзагроз, вироблення механізмів їх нейтралізації або попередження. Звісно, Міністерство економіки, торгівлі та промисловості, Міністерство внутрішніх справ і зв'язку та Агентство Національної поліції були включені в канали обміну інформацією з питань кібербезпеки з приватним сектором та міжнародними партнерами, але провідну роль у наданні інформації, її уточненні все ж належить НЦІБ (Matsubara, 2013). Іншим важливим напрямом діяльності в рамках реалізації Стратегії кібербезпеки стала розробка правової бази, зокрема, ухвалення законодавства про захист секретної інформації у сфері національної оборони, розробка норм, що стосуються боротьби зі шпигунством (у тому числі, з кібершпигунством), а також перегляд законодавства у сфері авторського права і суміжних з ним прав (Matsubara, 2013).

У 2015 р. було оприлюднено другу «Стратегію кібербезпеки», яка базувалася на положеннях «Основного закону про кібербезпеку» (2014 р.). Зазначимо, що самий Закон був ухвалений у відповідь на зростання масштабів кіберзагроз для системи національної безпеки. Об'єктами різноманітних протиправних дій у кіберпросторі стали державні органи влади, приватні компанії, провайдери послуг та окремі особи. Так, у 2011 р. найбільший виробник зброї в Японії Mitsubishi Heavy Industries повідомив, що його сервери були зламані програмою-вимагачем, а внутрішні системи були заражені щонайменше вісьмома вірусами. Більшість атак були націлені на завод у Нагої, де компанія проектує та створює системи наведення та рухові установки для ракет, верф у Нагасакі, де виготовляють есмінці, і підприємство в Кобе, яке відповідає за виробництво підводних човнів. У 2013 р. Yahoo Japan повідомила, що один з їхніх внутрішніх файлів, який містить 22 мільйони ідентифікаторів користувачів, ймовірно, був вкрадений у результаті несанкціонованого доступу. Потенційний витік даних міг вплинути на 10% бази користувачів Yahoo, що мало б значний суспільний резонанс. А вже у 2014 р. внаслідок зараження зловмисним програмним забезпеченням Japan Airlines повідомила, що програмі-вимагачу вдалося отримати доступ до особистої інформації 190 тис. пасажирів. (Top 14 Cybersecurity Breaches in Japan). Саме тому ухвалення «Основного закону про кібербезпеку» стало важливою правовою

основою формування збалансованої стратегії національної інформаційної безпеки, яка покликана протистояти новим видам загроз, і при цьому забезпечувати та підтримувати вільний потік інформації, який є основою формування демократії, безпечного та надійного середовища життя людей, економічного та соціального процвітання та миру, водночас захищаючи інтелектуальну власність, яка є результатом діяльності окремих людей і компаній (The Government of Japan, 2015).

Ухвалена у 2015 р. Стратегія кібербезпеки Японії визначає такі базові принципи, яких слід дотримуватися під час її реалізації, зокрема: забезпечення вільного потоку інформації, верховенство права під час регулювання кіберпростору, відкритість кіберпростору, дотримання інтересів усіх зацікавлених сторін та сприяння співробітництву у сфері кібербезпеки на міжнародному рівні (Hathaway, 2016).

Зміст оновленої стратегії якісно відрізняється від попередньої, виданої у 2013 р. Так, у документі зазначається, що зрушення у сфері ІКТ відкривають нові можливості для всіх зацікавлених сторін – держави, приватного сектору та індивідів. Завдяки інноваційним технологіям Японія отримала постійне джерело потенційного економічного зростання (особливо з урахуванням розвитку «Інтернету речей і для речей»). Отже, вільний і справедливий кіберпростір нині є необхідною передумовою для отримання всіх переваг науково-технологічного прогресу, що стає ефективним засобом покращення соціально-економічної сфери життя та забезпечення сталого розвитку суспільства. Таким чином в Японії формується «взаємопов’язане та конвергентне інформаційне суспільство», де фізичний простір і кіберпростір стали інтегрованими, члени суспільства отримали можливість « створювати інноваційні послуги та експоненціально генерувати абсолютно нові цінності» (The Government of Japan, 2015). Водночас досягнення у сфері ІКТ можуть виступати й джерелом ризику та загроз. Наприклад, кіберпростір, який може використовувати будь-хто без географічних і часових обмежень, дає асиметричні переваги саме зловмисникам, а не захисникам. У той же час зростаюча залежність соціально-економічної діяльності від кіберпростору та еволюція організованих і дуже складних методів або modus operandi кібератак, які можуть спонсоруватися державою, спричинили серйозні

збитки та негативно вплинули на повсякденне життя людей. Крім того, у зв'язку з появою взаємопов'язаного та конвергентного інформаційного суспільства зловмисна діяльність у кіберпросторі може спричинити значний вплив на всі типи пов'язаних фізичних об'єктів і послуг, а збиток від кібератак поширюватиметься швидше та ширше у фізичному просторі; отже, очікується, що в майбутньому життя людей буде наражатися на більш серйозні кіберзагрози. Тому для запобігання подальшому загостренню таких загроз, створення « вільного та справедливого кіберпростору» має відбуватися паралельно зі створенням «безпечного кіберпростору» (The Government of Japan, 2015).

Значну увагу у Стратегії було приділено питанням бізнес-можливостей, виникнення яких обумовлене подальшим науково-технологічним прогресом, розвитком інноваційної діяльності та розвитком Інтернету речей, що відповідає пріоритетам інформаційної політики уряду Японії в цілому, яка базується на таких документах, як: «Стратегія зростання ІКТ», «Стратегія пожвавлення економіки Японії», а також «Декларація про прагнення стати найбільш передовою ІТ-нацією у світі». У документі також наголошується, що вкрай важливими є питанням забезпечення безпеки критично важливих елементів інфраструктури (електромережі, водопровід, інформаційно-комунікаційні послуги, фінансові послуги та ін.) як базового політичного пріоритету, досягнення якого можливе лише з урахуванням інтересів усіх зацікавлених сторін (Hathaway, 2016). Відповідальним за реалізацію Стратегії було визначено Стратегічний штаб із забезпечення кібербезпеки, який повинен діяти як командний та контрольний орган у питаннях, пов'язаних з національною кібербезпекою, а також як орган, наділений повноваженнями давати рекомендації у сфері кібербезпеки іншим держустановам (Hathaway, 2016).

У серпні 2016 р. японський Національний центр інформаційної безпеки опублікував документ під назвою « Загальні рамкові положення безпеки систем Інтернету речей» (The Government of Japan, 2016), який є додатком до Національної стратегії кібербезпеки. Показовим є те, що уряд Японії цим документом заявив про

готовність піклуватися про кібербезпеку навіть у тих галузях, які напряму не відносяться до критично важливих елементах інфраструктури (Hathaway, 2016).

Незважаючи на впровадження значної кількості практичних механізмів забезпечення кібербезпеки, постійну роботу усіх зацікавлених сторін, загрози для кіберпростору не тільки не зникли, але й набули подальшого розвитку. Так, у 2016 р. стався масштабний витік даних внаслідок серйозної фішингової атаки на сервери туристичної компанії JTB яка призвела до розкриття персональних даних майже 7,93 млн осіб. З 2017 р. об'єктами атак стали криптовалютні біржі і платформи, зокрема, Coincheck, яка втратила частину своїх віртуальних активів (згідно з офіційною заявою керівника компанії було викрадено майже 523 мільйони NEM). На момент виявлення порушення загальні збитки становили 58 мільярдів ієн (443,2 мільйона доларів), а кількість постраждалих – понад 260 тис. клієнтів. Цей злом також призвів до падіння інших криптовалют: наприклад, біткойн впав на 3,4%, а Ripple – на 9,9%. (Top 14 Cybersecurity Breaches in Japan).

У лині 2018 р. Національний центр готовності до інцидентів і стратегії кібербезпеки (до 2015 р. Національний центр інформаційної безпеки) оголосив про нову Стратегію кібербезпеки, яка має змінити попередню, ухвалену 2015 р. Нова стратегія стала результатом регулярних зустрічей та консультацій усіх зацікавлених сторін і була спрямована передусім на покращення стану кібербезпеки критичної інфраструктури Японії.

У документі, зокрема, зазначається, що подальші технологічні зрушення не тільки розширюють можливості використання кіберпростору, але й суттєво поповнили перелік загроз, які можуть радикально вплинути на стратегію економічного розвитку держави, ефективність реалізації різноманітних програм у сфері наукового і технологічного розвитку, політичних ініціатив або проектів у сфері соціального захисту. Практично слід говорити про зсув парадигми кіберпростору, в якій кіберпростір визначається як «межа для створення нескінченної цінності». Тому Японія використовуватиме всі наявні в її розпорядженні засоби для здійснення ініціатив у сфері кібербезпеки, щоб гарантувати подальші позитивні зрушення (The Government of Japan, 2018).

Як зазначається в Стратегії кібербезпеки (2018), подальший розвиток комп'ютерних технологій, впровадження технологій штучного інтелекту та Інтернету речей і для речей перетворюють кіберпростір на необхідну передумову появи нових продуктів і послуг, використання яких вимагає постійне підвищення рівня інформаційної грамотності та обізнаності населення, зміну його повсякденної поведінки та середовища життя. Це, у свою чергу, викликає трансформацію соціальних систем та промислових інфраструктур разом з алгоритмами та процедурами їх діяльності, моделями та організацією. Оскільки людство переживає чергову зміну парадигми і будує вже «Суспільства 5.0», необхідно змінювати ставлення до кібербезпеки, беручи до уваги ці трансформації (The Government of Japan, 2018).

Отже, нова «Стратегія кібербезпеки» була спрямована, передусім, на подальше розширення заходів у сфері кібербезпеки. Зрозуміло, що для Японії, враховуючи її прагнення закріпити за собою статус високотехнологічної держави з розвиненої інформаційної інфраструктурою та високим рівнем проникнення сучасних технологій у суспільство, проблема кібербезпеки набуває дедалі більшої актуальності. На порядку денному діяльності всіх залучених до розробки і реалізації зацікавлених сторін постає ціла низка актуальних проблем, зокрема, « збільшення масштабів кібератак та збитків, що ними завдаються, неспроможність зайняти активну позицію щодо індивідуальної або колективної самооборони та залучити збройні сили як засіб протидії інформаційному нападу з боку інших держав, складність визначення кібератак, які слід розглядати як збройний напад, відсутність правових механізмів втручання та подальшого блокування комунікаційних каналів, навіть якщо вони містять шкідливе програмне забезпечення, нестача людських та технічних ресурсів для відбиття кібератак і залежність в цьому питанні від інших держав, недосконала система комунікації між спеціально утвореними структурами та підрозділами у питаннях забезпечення кібербезпеки, недостатній рівень усвідомлення проблеми самим населенням Японії. Тому ухвалення нової стратегії стало об'єктивною потребою для формування більш стійкого та безпечного кіберпростору» (Сябро, 2019с).

Найбільшими загрозами для кіберпростору Японії, відповідно до Стратегії, є: втрата контролю за дотриманням норм безпеки постачальників послуг, які передбачають використання технологій штучного інтелекту та Інтернету речей, що може призвести до колосальних економічних і соціальних втрат або збитків, створення кіберфізичних систем та наслідки їх неправомірного використання, злочинне використання технологій штучного інтелекту та блокчейн, атаки на Fintech-платформи та криптовалютні біржі як в самій Японії, так й за її межами. Неспроможність держави ефективно відповідати на зазначені виклики може призвести до зменшення рівня довіри до кіберпростору, до технологій і послуг, які є основою для формування стійкої « екосистеми кібербезпеки» та розбудови нового типу суспільства – «Суспільства 5.0» (The Government of Japan, 2018).

У документі, також зазначалося, що «уряд Японії має створити до 2021 р. високонадійну інформаційну систему для забезпечення безпеки нових технологій, у тому числі, технологій, що відносяться до криптовалютних оборудок та самокерованих транспортних засобів. Уряд також запланував створити п'ятирівневу систему оцінки інтернет-загроз, засновану на аналізі потенційних наслідків кібератак, багаторівневу систему сповіщення населення про можливі злочини у кіберпросторі, створити механізми державно-приватного партнерства з метою формування вільного та стійкого кіберпростору, розвивати безпечну кібернетичну екосистему, забезпечити інвестиції в розвиток технологій кібербезпеки тощо. Особливої актуальності проблема набуває у контексті майбутніх Олімпійських ігор 2020 у Токіо, гарантія безпеки проведення яких потребуватиме додаткових зусиль й у сфері кібербезпеки, оскільки уряд очікував суттєве підвищення масштабів кібератак, спрямованих на сайти урядових інституцій та приватних компаній Японії» (Сябро, 2019с).

Слід підкреслити, що підготовка до проведення Олімпійських ігор у Японії, які були заплановані у 2020 р. (проведені у 2021 р.), супроводжувалася активними заходами у сфері кібербезпеки. Як підкреслюють експерти, в останні роки використання кібератак, щоб зірвати організацію важливих спортивних подій світового масштабу, стало поширеним явищем. Тому Японія вжила різноманітних

заходів для посилення кібербезпеки державних установ, компаній та окремих індивідів (Matsubara, 2021). Водночас це не врятувало державу від масштабного кіберінциденту. Так, під час проведення Олімпійських ігор внаслідок кібератаки було викрадено імена користувачів і паролі, які можна використовувати для доступу до веб-сайтів Олімпіади, персональні дані волонтерів і власників квитків, їх імена, адреси та номери банківських рахунків (Top 14 Cybersecurity Breaches in Japan).

У цьому ж році нападу зазнали постачальник додатків для обміну повідомленнями Line Corp, телекомунікаційний гігант NTT, електронний гігант Panasonic, судноплавна компанія Kawasaki Kisen Kaisha та ін. Були атаковані й урядові установи Японії через інструмент обміну інформацією «ProjectWEB» Fujitsu та файлообмінний сервер Solito. Згідно з офіційними джерелами, атака програми-вимагача на «ProjectWEB» Fujitsu торкнулася одночасно кількох урядових установ: міністерства землі, інфраструктури, транспорту, туризму Японії, секретаріату кабінету міністрів і міжнародного аеропорту Наріта. Зловмисники отримали доступ до 76 тис. електронних адрес і налаштувань системи електронної пошти, захопили проекти, розміщені на ProjectWEB, і викрали конфіденційні дані, дані про рейси з аеропорту Наріта та розкрили навчальні матеріали Міністерства закордонних справ Японії. Цей напад не був фінансово мотивований, але продемонстрував вразливість державних структур до нападів зловмисників (Top 14 Cybersecurity Breaches in Japan).

28 вересня 2021 року Національний центр готовності до інцидентів і стратегії кібербезпеки опублікував ще одну «Стратегію кібербезпеки», яка враховувала нові реалії, пов’язані з важливими економічними, суспільними та екологічними змінами, обумовленими, у тому числі, пандемією COVID-19, поширення цифрової економіки та електронного бізнесу, сприяння подальшій цифровій трансформації суспільства, зростання масштабів віддаленої роботи тощо. У документі, зокрема, зазначається, що пандемія COVID-19, окрім визнаних негативних наслідків для населення Японії та світу, призвела до прискорення розвитку цифрових технологій та їх поширення у суспільстві. Саме тому питання кібербезпеки набули ще більшого значення для японського суспільства. Водночас трансформації, запущені у 2020 р. у сфері

інформатизації та розбудови цифрової економіки, призвели до прискорення реалізації багатьох програм модернізації економіки та розбудови «Суспільства 5.0», в якому остерігатиметься подальше поєднання фізичного і кібернетичного просторів на вищому рівні. За оцінками експертів 2020-ті роки мають стати для Японії «цифровим десятиліттям» (The Government of Japan, 2021).

Разом з цим спостерігається дедалі більша залежність прогресу суспільства від вирішення питань безпеки кіберпростору, а також збільшення рівня взаємозалежності процесів забезпечення високих стандартів інформаційної безпеки та ефективності програм економічної, політичної та соціальної модернізації та прогресу у науково-технологічній сфері. Це призводить до зростання конкуренції між державами у сфері впровадження інформаційно-комунікаційних технологій, розширення практики використання технологій штучного інтелекту, Інтернету речей, 5G-зв'язку, хмарних сервісів, впровадження ІКТ у сферу освіти, поширення практики дистанційної роботи, а також поглиблення взаємозалежності складної економічної та соціальної діяльності (The Government of Japan, 2021).

Окрім традиційних кіберзагроз, визначених ще у попередніх стратегіях, в оновленій редакції значну увагу було приділено питанням інформаційної грамотності населення та недостатньо високі темпи цифровізації як у державному, так і в приватному секторах. З цією метою у вересні 2021 р. було створене Цифрове агентство, яке відповідає за реалізацію ініціатив із створення цифрового суспільства, сприяння цифровій трансформації, подолання цифрового розриву.

У стратегії йдеться також про зростання конкуренції між державами, де технології є визначальним фактором переваги, а технологічний потенціал є важливим фактором сукупної потуги держави. Саме тому технологічні переваги можуть використовуватися й у сфері військового протистояння, а враховуючи існування кіберфізичних систем, це може мати негативні наслідки для суспільства в цілому.

Таким чином, досвід у сфері забезпечення кібербезпеки, отриманий під час боротьби з пандемією COVID-19 та проведення Олімпійських та Паралімпійських ігор в Токіо у 2021 р., є важливим з погляду аналізу ефективності національних

стратегій у сфері кібербезпеки і практики їх реалізації, а також аналізу нових викликів і загроз, що постійно з'являються внаслідок подальшого технологічного розвитку як самої Японії, так й інших держав (The Government of Japan, 2021).

Нова «Стратегія кібербезпеки» також містить аналіз ризиків, які обумовлюють підвищення уваги уряду Японії та всіх зацікавлених сторін до вирішення проблеми безпеки у новому суспільстві – «Суспільстві 5.0». Так, серед небезпек та ризиків визначено зростання обсягів персональної та конфіденційної інформації у кіберпросторі, що, з одного боку, дає можливість надавати громадянам різноманітні онлайнові послуги – державні, комерційні, а з другого, містить потенційну загрозу витоку інформації внаслідок кібератак. Оскільки цифрові послуги починають укорінюватися в житті людей, можна припустити, що методи атак стануть більш різноманітними та досконалими, а прогалини, що утворюються в процесі координації цифрових послуг, можуть стати вразливими місцями для зловмисників. Також у документі наголошується на тому, що зловмисники можуть скористатися технологічними інноваціями, а це у свою чергу призведе до збільшення загроз. Наприклад, якщо зловмисники використовують технології штучного інтелекту, кібератаки відбуватимуться зі швидкістю та в масштабі, які перевищує рівень людських можливостей та їх технічних навичок. У середньостроковій та довгостроковій перспективі також слід враховувати можливість автономних атак, які не покладаються на контроль людини. (The Government of Japan, 2021).

Друга небезпека стосується вразливості економіки та суспільства в цілому. Зокрема, розвиток цифровізації неминуче призводить до залучення дедалі більшої кількості компаній з різних галузей і бізнес-категорій до діяльності в кіберпросторі, а також окремих категорій людей, включаючи молодь і людей похилого віку, які мають недостатньо високий рівень обізнаності у питаннях кібербезпеки. Це суттєво збільшує ризики кібератак з боку зловмисників та зменшує рівня довіри до кіберпростору. Крім того, дефіцит людських ресурсів у сфері технологій та програмного забезпечення може призвести до ситуації, коли Японія буде змушена надмірно покладатися на продукти, послуги і технології, пов'язаних з кібербезпекою, іноземного виробництва. У документі також підкреслюється, що

збільшення використання хмарних сервісів, розширення та активне впровадження продуктів і послуг, що надаються через складні глобальні ланцюжки поставок, більш широке використання пристроїв Інтернету речей у всіх галузях і застосування технології штучного інтелекту призводить до зростання масштабів впливу інцидентів на економічну та соціальну діяльність, на всі зацікавлені сторони, що ускладнює вирішення питань кібербезпеки та демонструє обмеженість традиційної концепції «периметру безпеки» (The Government of Japan, 2021).

Третьою групою ризиків у Стратегії 2021 р. визначено кібератаки ззовні, тобто на національний інформаційний простір держави. Як підкреслюється у документі, спостерігається постійне зростання загрози організованих і складних кібератак з боку держав-спонсорів тероризму або недружніх держав з метою порушення роботи критичної інфраструктури, викрадення особистої інформації та інтелектуальної власності, втручання в демократичні процеси. Отже кіберпростір перетворився на вимір міждержавної конкуренції, яка відображає геополітичну напруженість навіть у мирний час. Серед держав, які можуть стати джерелом загроз для національної системи кібербезпеки, визначено Китай, який активно використовує кібератаки для викрадення інформації про передові інноваційні технології підприємств військово-промислового комплексу, Росія, яка використовує кіберпростір для здійснення впливу з метою досягнення військових або політичних цілей, Північна Корея – для досягнення політичних цілей або атаки на фінансовий сектор. Крім того, зазначається, що Китай, Росія та Північна Корея продовжують нарощувати свій військовий кіберпотенціал. В умовах постійного зростання геополітичної напруженості у відносинах між країнами, які базують свою політику на різних політичних цінностях, виникають конфлікти щодо міжнародних норм у сфері регулювання кіберпростору Японії (The Government of Japan, 2021).

Враховуючи комплекс загроз для системи національної інформаційної безпеки Японії на політичному рівні слід говорити про головну ідею усіх стратегічних ініціатив – створення «кібербезпеки для всіх». Власне це відображує саму специфіку японського підходу до формування середовища безпеки, яке має враховувати високі темпи технологічного розвитку та швидкого проникнення інноваційних технологій у

суспільство Японії, створення передумов для функціонування вільного і безпечного кіберпростору, а також появу нового типу загроз (як внутрішніх, так й зовнішніх). З огляду на це актуальним залишається поєднання зусиль усіх зацікавлених сторін у розробці і реалізації стратегії кібербезпеки, що має в остаточному результаті дати потужний імпульс для подальшого соціально-економічного розвитку та розбудови «Суспільства 5.0» з високими стандартами стійкості і безпеки інформаційного середовища (The Government of Japan, 2021).

У Стратегії представлено основні напрями політики кібербезпеки з детальним обґрунтуванням актуальності кожного з них. Так, важливими напрямами реалізації політики кібербезпеки визначено такі: 1) Реалізація стратегії цифрової трансформації у поєднанні з розробкою і реалізацією заходів у сфері кібербезпеки (йдеться про так звану концепцію «Security by Design», яка представляє ідею забезпечення кібербезпеки на етапах планування і проектування інноваційних високотехнологічних товарів і послуг); 2) В умовах постійного зростання залежності економічних, соціальних і безпекових програм модернізації японського суспільства від відкритості, стійкості і безпеки кіберпростору, вкрай важливим стає питання залежності традиційного простору безпеки і кібернетичного (усім зацікавленим сторонам слід усвідомлювати, що кіберпростір стає таким же важливим простором безпеки, як й традиційний, а отже йому слід приділяти більше уваги і постійно посилювати заходи кібербезпеки, враховуючи особливу природу нового типу загроз); 3) Удосконалення заходів кібербезпеки в умовах пришвидшеної цифровізації економіки і японського суспільства (без гарантів кібербезпеки говорити про ефективність і досягнення у розбудові «Суспільства 5.0.», про підвищення конкурентоспроможності на світовому ринку продуктів і послуг, забезпечення інноваційного лідерства держави буде практично неможливо); 4) Підвищення рівня цифрової грамотності та грамотності у галузі інформаційної безпеки населення Японії; 5) Забезпечення середовища кібербезпеки на основі дотримання принципів вільного потоку інформації, конфіденційності та цілісності інформації, де стандартною практикою для постачальників послуг є комплексне уявлення про взаємозв’язок у кіберпросторі для більш ефективного управління

ризиками; 6) Забезпечення кібербезпеки як невід'ємної складової цифрової трансформації (під керівництвом Цифрового агентства) з метою здійснення «дружньої до людей цифровізації, щоб ніхто не залишився поза процесом»; 7) Сприяння зусиллям зацікавлених сторін з метою формування сучасної соціально-економічної інфраструктури; 8) Підвищення рівня готовності до реагування на масовані кібератаки; 9) Участь дво- та багатосторонньому співробітництві, спрямованому на зміцнення миру і безпеки світового співтовариства. У Стратегії, зокрема, підкреслюється, що на багатосторонньому рівні Японія займає позицію сприяння верховенству права в кіберпросторі і бере активну участь в обговоренні питань ухвалення міжнародно-правових документів у сфері інформаційної безпеки в рамках ООН, зокрема, щодо злочинного використання кіберпростору злочинними і терористичними угрупованнями, регулювання Інтернету. У стратегії також підкреслюється, що держава прагне і надалі розвивати співпрацю зі США, Австралією та Індією, а також АСЕАН та іншими країнами у сфері кібербезпеки в напрямку реалізації «Вільного та відкритого Індо-Тихоокеанського регіону (FOIP)». На двосторонньому рівні важливу роль у формування національної системи інформаційної безпеки та оборони Японії відіграє співробітництво держави зі США. Загалом тут слід говорити про окремий напрямок, пов'язаний із зміцненням кібероборони Японії. За загальну координацію ініціатив, пов'язаних з національною безпекою і обороною, що реалізуються усіма зацікавленими сторонами, у тому числі, Національним центром готовності до інцидентів, Міністерство сил оборони та самооборони та ін. відповідатиме Секретаріат національної безпеки (The Government of Japan, 2021).

Таким чином, у Стратегії 2021 р. представлено комплексний підхід держави до вирішення проблеми кібербезпеки. Нова стратегія містить не тільки глибокий аналіз ситуації, пов'язаної з подальшою цифровізацією суспільства та збільшенням залежності програм соціально-економічного розвитку від стійкості і безпеки мереж і технологій, але й зовнішніх загроз, які йдуть від недружніх країн і які складно передбачити. Саме тому в документі визначено оновлені пріоритети політики Японії у сфері кібербезпеки та представлено організаційну структуру діяльності усіх

зацікавлених сторін. Практично Стратегія 2021 р. є консолідованим представленням еволюції політики у сфері інформаційної безпеки, в цілому, та кібербезпеки, зокрема (Сябро, 2019в).

Зазначимо, що у Стратегії кібербезпеки 2021 р. особливу увагу було приділено так званій кібердипломатії. У документі не тільки визначено кібербезпеку як проблему глобального геополітичного протистояння, але й конкретизовано, які країни для національної безпеки Японії можна вважати недружніми. Для ефективного протистояння загрозам запропоновано поглибити вже існуючи механізми міжнародного співробітництва у сфері кібербезпеки. Так, на регіональному рівні дедалі більшої актуальності набуває співробітництво Японії з АСЕАН у сфері кібербезпеки. На двосторонньому рівні в Стратегії кібербезпеки 2021 р. особливу увагу приділено співробітництву зі США, яке розглядається як складова політики стримування у Азійсько-Тихоокеанському регіоні.

3.2. Еволюція національної політики кібербезпеки Індії

Важливим учасником формування сучасної архітектури безпеки регіону, особливо в контексті формування нової геополітичної парадигми Індо-Тихоокеанського регіону та стратегії стримування Китаю, є Індія, політика інформаційної безпеки якої має суттєві відмінності. Зазначимо, що одним з найбільш вагомих чинників, що впливає на зміст стратегії інформаційної безпеки та ефективність її реалізації, є суперечливий процес цифровізації держави та впровадження інноваційних технологій у всі сфери життєдіяльності суспільства. Наприклад, як свідчить статистика, ще у 2014 р. кількість користувачів Інтернетом в Індії становила менше 20 % населення, яке нараховувало тоді бл.1,2 млрд осіб. Причинами таких низьких темпів проникнення технологій експерти називали високу вартість інформаційно-комунікаційних технологій та послуг зв’язку, а також бюрократизм та занадто широкі можливості втручання держави у роботу телекомунікаційних компаній (Сябро, 2019а). Всього через п’ять років ситуація змінилася докорінним чином. Зокрема, Індія посіла друге місце у світі за кількістю

інтернет-користувачів (понад 560 млн.осіб), а рівень проникнення технологій становив бл. 41% (Internet world stats, 2019). Зросли показники використання мобільних телефонів, і особливо смартфонів (бл. 345,92 млн осіб), які надають можливість користуватися мобільним інтернетом та отримувати онлайн-послуги (Holst, 2019a; Holst, 2019b). Станом на кінець 2021 - початок 2022 рр. кількість користувачів інтернету вже становила 658 млн (з бл. 1,4 млрд. населення держави). Отже спостерігається постійне зростання кількості користувачів інтернетом, але при цьому 742 млн або 53 % населення все ще залишалися офлайн. Показовою є й статистика щодо кількості користувачів соціальних мереж. Так, наприкінці 2021 р. кількості користувачів соціальних мереж становила 467 млн осіб від загальної кількості населення, і ці показники також продовжують зростати. Найбільш популярними соціальними мережами в Індії є Facebook / Meta, YouTube, Instagram, LinkedIn, Snapchat, Twitter. Щодо використання мобільного зв'язку, Індія також демонструє стійке зростання показників. Так, у 2021 р. кількість мобільних підключень становила 79 % від загальної кількості населення, а у 2022 р. – 81,3 % населення (Digital 2021: India, 2021; Digital 2022: India, 2022).

Останнім часом в Індії також спостерігається бурхливий розвиток й в інноваційній науково-технологічній сфері. Так, у 2019 р. Індія посіла 52-ге місце в рейтингу інноваційного розвитку країн світу, який представлений в аналітичній доповіді «Глобальний Інноваційний Індекс». Вже наступного року країна пересунулася на 48-му позицію, а у 2021 р. – на 46-ту. Водночас Індія посідає перше місце серед 10 економік Центральної та Південної Азії (WIPO, 2019; WIPO, 2020; WIPO, 2021). Окрім інноваційної діяльності, Індія включилася й у Четверту індустріальну революцію, намагаючись максимально використати різноманітні технологічні досягнення як у цивільній, так й у військовій сферах. Використовуючи знання і розробки у сфері штучного інтелекту, Інтернету речей, робототехніки, 3D-друку і нанотехнологій інших економічно розвинутих країн, представники промислових підприємств та сільськогосподарського сектору Індії розраховують на отримання можливостей «перескочити» в Четверту індустріальну революцію за умови, що їм вдасться розумно поєднати наявні ресурси, інфраструктуру та

технологічні можливості (India: Opportunity & Role in the 4th Industrial Revolution, 2019). Більш того, Індія, за умови формування належної нормативно-правової бази, освітньої структури та державної підтримки, може у подальшому відігравати навіть провідну роль у такій модернізації. Світове визнання потенціалу Індії стало очевидним, коли Всесвітній економічний форум у партнерстві з урядом Індії створив Центр четвертої промислової революції Індії, провідними напрямами дослідження якого є сприяння розвитку технологій штучного інтелекту та машинного навчання, дронів, блокчейну, Інтернету речей та робототехніки (World Economic Forum, 2022). Нині уряд вже розпочав реалізацію проекту «Make in India», який може модернізувати процес проектування та виробництва в індійській промисловості, дотримуючись вимог Четвертої промислової революції. Інший урядовий проект – «Розумні міста», революціонізований за допомогою Інтернету речей, може дозволити під'єднати всі пристрої через мережу, а послуги надаватимуться за допомогою автоматизації. Міста, стратегічно обрані для цього проекту, можуть забезпечити справедливий розподіл інформаційних та соціально-економічних благ по країні (Karthikeyan, 2022). Таким чином, досягнення у сфері науки і технологій стали важливою складовою стратегії модернізації економіки, розбудови цифрової держави та трансформації індійського суспільства.

Активний інформаційний і науково-технологічний розвиток Індії розпочався у середині 1990-х рр., коли постало питання розбудови електронного урядування та системи надання онлайн-послуг для населення. Поступово з'явилися проекти та ініціативи, спрямовані на подальшу інформатизацію держави, зокрема, комп'ютеризація залізниць та земельних документів з метою розвитку інформаційної інфраструктури. У 2006 р. було започатковано Національний план електронного урядування (NeGP), який передбачав реалізацію 24 проектів і охоплював широкий спектр сфер реалізації, а саме: сільське господарство, земельні записи, охорона здоров'я, освіта, паспортна служба, поліція, суди, муніципалітети, податкові та фінансові структури тощо. У 2014-2015 рр. Індія ухвалила програми «e-Kranti: Національний план електронного урядування 2.0» та «Цифрова Індія» (The Government of India, 2015; Digital India, 2015). Реалізація програм мала забезпечити

кожного можливістю широкосмугового доступу; сприяти поширенню мобільних технологій, створенню системи надання цифрових державних послуг, формуванню нової моделі економічної діяльності, що базується на послугах; сприяти розвитку соціальних медіа, освіти та сучасних підходів до навчання; створювати нові можливості для молоді, сприяти модернізації медичного обслуговування, а також підвищенню загального рівня цифрової готовності держави (Rijksdienst voor Ondernemend Nederland, 2018). Для досягнення окреслених пріоритетів було ухвалено цілу низку додаткових спеціальних цифрових платформ, зокрема, BharatNet – для надання різноманітних електронних послуг у сфері електронної охорони здоров'я, освіти та електронної комерції для сільського населення, «Jan Dhan з нульовим балансом» – для розвитку інфраструктури цифрових платежів у сільській місцевості, MUDRA – для забезпечення кредитування сільського бізнесу за низькими ставками, що у свою чергу, сприяє прискоренню цифрової трансформації середніх, малих і мікропідприємств, поширенню 5G-зв'язку для створення додатків з високою економічною та соціальною цінністю, створює «гіперз'єднане» суспільство, Diksha –для шкільної освіти; інші ініціативи, спрямовані на підтримку IT-індустрії та цифрової економіки, програмного аутсорсингу та діяльності Центрів науково-дослідних розробок тощо (Looking Into The Future, 2021).

Важливим етапом реалізації стратегії цифровізації Індії стало створення у 2016 р. системи цифрової ідентифікації особистості Aadhaar, яка вже у 2019 р. охопила понад 90 % населення. Проект є найбільшою у світі біометричною системою ідентифікації особистості, в якій реєстровано 1,1 млрд користувачів. Система Aadhaar прив'язана до різноманітних біометричних даних користувачів – відбитки пальців, малюнок райдужки ока, фотографії, що уможливлює доступ користувачів до різноманітних фінансових операцій, державних та приватних послуг, а також до програм соціального захисту населення (Unique Identification Authority of India, 2019)

Отже, Індія, успішно втілюючи програми і проекти цифрового розвитку держави, сьогодні демонструє високі темпи економічного зростання на основі використання можливостей інформаційно-комунікаційних технологій та

інноваційних наукових досягнень. Водночас, це призводить до актуалізації питань безпеки суспільства, яке так швидко змінюється. Тим більше, що Індія стала дедалі частіше виступати об'єктом різноманітних інформаційних атак на критично важливі елементи інфраструктури, державні та фінансові установи або на інформаційну особистість громадян. Зазначимо, що при всіх об'єктивних досягненнях у сфері ІКТ, Індія виявила значне відставання у рівні захисту національного інформаційного простору і критичної інформаційної інфраструктури, що суттєво ускладнювало реалізацію програм модернізації державного управління та соціально-економічного розвитку і поставило під загрозу вже існуючи досягнення. Так, за даними експертів, у 2021 році Індія увійшла до трійки країн Азії, які зазнали найбільшої кількості атак типу відмови доступу до серверів і програм-вимагачів. Лише за перші три місяці наприкінці 2021 – початку 2022 рр. в Індії було зафіксовано понад 1,8 млрд кібератак на індійські урядові та фінансові структури, а також освітні та наукові ресурси (Berry, 2022). При цьому значно зростає кількість атак з-за кордону, зокрема, з Китаю, Північної Кореї та Пакистану.

Найбільш показовим випадком зростання небезпеки кіберзагроз вважаються атаки на систему Aadhaar, які продемонстрували численні серйозні прогалини в безпеці. Кіберінцидент призвів до масштабного витоку персональних даних та конфіденційної інформації. Уряду Індії довелося заблокувати близько 5000 офіційних осіб, оскільки до даних системи ідентифікації отримував доступ неавторизований персонал, який працював на уряд. Tribune також повідомила, що її журналістам вдалося відстежити анонімну групу в WhatsApp, яка продавала дані картки Aadhaar усього за 500 рупій (7,2 доларів США). Веб-сайт штату Джаркханд випадково оприлюднив дані про 1,6 млн пенсіонерів, включаючи їхні адреси та реквізити банківських рахунків (Jain, 2019).

Як свідчать чисельні аналітичні дослідження, Індія і нині залишається надзвичайно вразливою для різноманітних інформаційних атак, зокрема, telnet-атак за країною походження, хоча має не тільки високий рівень інформаційного розвитку, але й достатньо розгалужену правову базу у сфері інформаційної безпеки (Bischoff, 2021). Так, згідно із Рейтингом країн світу за рівнем вразливості до

кіберзагроз 2020, Індія посіла 16-те місце серед країн АТР і 55-те – зі 108 досліджуваних країн світу (Global Cybersecurity Exposure Index, 2020). Інформаційні атаки стають дедалі більш руйнівними за масштабами ураження та наслідками їх застосування. Така ситуація може призвести до поглиблення багатьох проблем не тільки у сфері власне інформаційної безпеки, а й у сфері політичної, економічної, суспільної безпеки Індії, оскільки об'єктами нападів стають критично важливі елементи інфраструктури суспільства. А враховуючи той факт, що Індія залишається однією з кращих країн для міжнародного аутсорсингу компаній Apple, Sapient, Citi Bank, HSBC, Bank of America, DSM та ін., які створили свої глобальні центри виробництва, доставки, обслуговування та сервісної підтримки в державі, недостатній рівень інформаційної безпеки може вплинути й на них. Тобто інтереси міжнародних бізнес-партнерів страждатимуть внаслідок кібератак або неефективності стратегій швидкого реагування на них (Rijksdienst voor Ondernemend Nederland, 2018). Тому, проблеми інформаційної безпеки набувають для Індії критичного значення, оскільки напряму впливають на ефективність реалізації програм модернізації системи державного управління, розбудови нової моделі економічної діяльності та побудови нового типу суспільства, в якому за рахунок нарощування технологічних спроможносте з'являються можливості вирішення вкрай гострих проблем соціально-економічного розвитку.

Слід підкреслити, що від початку на рівні урядових ініціатив питанням інформаційної безпеки і оборони приділялося недостатньо уваги. Перші кроки у розробці базових принципів політики у сфері інформаційної безпеки Індія зробила ще у 2000 р., коли був ухвалений « Закон про інформаційні технології» , який і нині залишається базовим правовим актом у сфері регулювання питань національної інформаційної безпеки, постійно оновлюється відповідно до появи нових чинників і пріоритетів національної політики інформаційної безпеки (Ministry of Law, Justice and Company Affairs, 2000; Ministry of Law And Justice, 2008). У документі вперше було представлено класифікацію загроз для системи національної інформаційної безпеки, зокрема: навмисне втручання у роботу систем і мереж, несанкціонований доступ до електронних документів, злом комп'ютерної системи, викрадення

персональних даних, паролів та кодів доступу до персональної і банківської інформації, поширення персональної інформації без дозволу її власника, кібершахрайство, кібертероризм, поширення забороненої інформації порнографічного характеру тощо. На думку експертів, закладені у Законі відносно « жорсткі» норми регулювання інформаційної діяльності в умовах постійного зростання кількості і масштабів інформаційних загроз надало уряду держави широкі можливості впровадження цензури та здійснення державного контролю за інформаційною діяльністю громадян (Ministry of Law, Justice and Company Affairs, 2000).

У 2004 р. за ініціативи уряду Індії було створено цілу низку спеціалізованих підрозділів у сфері кібербезпеки, зокрема:

- «Індійську команду реагування на надзвичайні ситуації в Інтернеті (CERT-In)» – вузлове агентство під егідою MeitY, яке мало функціонувати як національне агентство з реагування на інциденти в кіберпросторі (зокрема, хакерство та фішинг). З 2006 р. агентство почало випускати річні звіти, які містили дані та узагальнений аналіз усіх кіберінцидентів, прогнози та рекомендації для державних установ і приватних компаній. CERT-In також здійснює підготовку IT-фахівців та посадових осіб у сфері боротьби із будь-якими видами зловмисної кіберактивності.
- Національна інформаційна рада (NIB) – вищий орган індійської влади з питань кібербезпеки, який працює під прямим керівництвом Офісу прем'єр-міністра і очолюється Радником з національної безпеки. Будь-які політичні питання, пов'язані з кібербезпекою, обговорюються в Раді та після подальшого затвердження передаються до Ради національної безпеки.
- Національна організація технічних досліджень (NTRO) – служба технічної розвідки Індії, призначена виключно для збору технічної інформації. Організація працює під безпосереднім керівництвом Радника з національної безпеки в Офісі прем'єр-міністра. Національна організація технічних досліджень займається розробкою передових сучасних технологій, які допомагають у зборі даних, дистанційному зондуванні, кібербезпеці та кіберкриміналістиці.

- Національний центр захисту критичної інформаційної інфраструктури (NCIIPC) – національне вузлове агентство із захисту критичної інформаційної інфраструктури, зокрема, у сфері енергетики, телекомунікацій, банківському секторі та секторі фінансових послуг, у сфері транспорту, управління стратегічними та державними підприємствами, а також у сфері державного управління. Він діє для координації, обміну, моніторингу, збору та аналізу інформації, прогнозування загроз на національному рівні для критичної інфраструктури Індії з метою розробки політичних вказівок, обміну досвідом та ситуаційною обізнаністю для раннього попередження або оповіщення.

Активізація програмної діяльності уряду Індії у сфері кібербезпеки відбулася лише у 2013 р. і була пов'язана з інцидентом з Е. Сноуденом та оприлюдненням документів, що свідчили про тотальне спостереження та здійснення кібероперацій спецслужбами США, спрямованими як на вороже налаштовані країни, так й на союзників. Індія, яка також потрапила до переліку держав, які опинилися в зоні уваги американських спецслужб, незважаючи на свій статус держави-союзника, була змушена прискорити процес розробки національної стратегії у сфері кібербезпеки (Сябро, 2020a). Американське відомство використовувало дві програми для збору даних – Boundless Informant для перехоплення телефонних розмов та стеження за діяльністю в Інтернеті в Індії і PRISM для отримання несанкціонованого доступу до мільярдів даних від різних постачальників веб-послуг, зокрема Google, Microsoft, Yahoo, Apple, сайтів соціальних мереж, таких як Facebook та інших. Оприлюднені документи також свідчили, що АНБ вело спостереження й за посольством Індії у Вашингтоні, офісом місії Індії в ООН в Нью-Йорку. Ці події дали поштовх для формування базових підходів та чіткого плану дій боротьби з будь-якою зловмисною кібердіяльністю, спрямованою проти Індії (Singh, 2019).

У 2013 р. Міністерство електроніки та інформаційних технологій Індії (MeitY) оприлюднило документ «Національна політика кібербезпеки 2013», який презентував загальну позицію держави у сфері кібербезпеки і містив дорожню карту кібербезпеки та створення безпечної кіберекосистеми по всій країні. Документ

включав п’ять основних пунктів, що складаються з бачення, місії, цілей, стратегій та шляхів реалізації політики. Так, у «Національній політиці кібербезпеки 2013» визначає сім сфер інтересів, де кіберполітика матиме найбільший вплив:

- Інформаційні та комунікаційні технології (ІКТ). Кіберполітика має бути спрямована на дослідження і розробки у секторі ІКТ, сприяти створенню власних дослідницьких лабораторій та установ із найсучаснішою цифровою інфраструктурою, оскільки країна повинна мати власні надійні, ефективні та дієві технології для протидії будь-якій зловмисній кіберактивності.
- Військова та оборонна сфери. Кіберполітика країни має взаємодіяти з військовою та оборонною сферами. Кібертероризм і кібервійна є двома основними загрозами, з змушена боротися країна, а тому важливим є формування стійкого середовища безпеки. До того ж відбуваються поступові зміни у формі і методах ведення війн. Відтепер стає важливим кіберфронт, тому для країни вкрай важливо мати кіберармію, яка займається питаннями, пов’язаними з кібератаками, кібершпигунством та збором розвідувальних даних.
- Економіка та фінанси. Розвиток глобальної електронної комерції, міжнародні інвестиції, поширення практики використання цифрової валюти потребують розробки і реалізації ефективної кіберполітики для сприяння подальшому розвитку цифрової економіки, що неможливо без гарантій інформаційної безпеки для її захисту. Саме тому Індія, яка зацікавлена у подальшому розвитку нової моделі економічної діяльності на основі широкого використання ІКТ і мереж, потерпаючи від кіберзлочинів та кібершахрайства, зацікавлена у створенні ефективної системи попередження таких небезпек і захист від них.
- Електронне врядування та людські ресурси. Розвиток електронного урядування для надання кращих послуг для суспільного блага є можливим лише тоді, коли країна має потужну інфраструктуру кібербезпеки. Досягнення цілей також передбачає підготовку кваліфікованих спеціалістів у сфері кібербезпеки, здатних захищати та запобігати протиправним діям, спрямованим на критичну інфраструктуру країни.

- Захист інформації та конфіденційності особи. Найвищим пріоритетом кіберполітики країни має бути захист персональної інформації громадян та інтересів осіб, гарантії безпеки громадян як фундаментального права та зобов'язання з боку держави і приватного сектору забезпечувати захист їхніх інтересів від будь-якої зловмисної кіберактивності.
- Державно-приватне партнерство. Приватні організації є ключовими зацікавленими сторонами у формуванні безпеки і стійкості кіберсфери. Найбільшої актуальності це питання набуває у контексті зростання масштабів електронної комерції за участю представників великого бізнесу, транснаціональних компаній, банків та інших організацій. Наприклад, впровадження хмарних технології допомагає компаніям надавати спрощений доступ до продуктів і послуг, а також полегшують ведення бізнесу. Водночас, із розвитком електронних форм ведення бізнесу спостерігається зростання масштабів кіберзагрози та кібератак. Тому необхідно посилити державно-приватне партнерство у сфері інформаційних технологій і безпеки їх використання.
- Міжнародне співробітництво у сфері кібербезпеки. Міждержавні відносини зорієнтовані на забезпечення економічної стабільності та підтримання національної безпеки. Оскільки у кіберсвіті не існує балансу сил, кібератаки мають достатній потенціал, щоб змусити акторів міжнародних відносин розглядати дилему безпеки держав у світлі реалій зростання небезпеки справжніх актів агресії як у кібернетичному, так й у фізичному просторі. Для формування системи глобальної інформаційної безпеки необхідно сприяти посиленню міжнародної співпраці, у тому числі, шляхом розробки і реалізації ефективної національної політики кібербезпеки (Singh, 2019).

У документі також визначено основні принципи стратегії кібербезпеки Індії, зокрема: трансформація сприйняття проблеми кібербезпеки та надання їй першочергового значення; розширення підходів до вирішення проблеми кібербезпеки, яку не слід звужувати лише до технічних питань попередження або ліквідації наслідків кібератак, при цьому система повинна стати гнучкою, динамічною і швидко адаптуватися до нових викликів і загроз; підготовка

спеціалістів, здатних ефективно протистояти загрозам у кіберпросторі; включення безпеки як фундаментального принципу концептуального проектування, у тому числі, у сфері розбудови інформаційної інфраструктури (Сябро, 2019а). Основними цілями стратегії кібезрбезпеки, відповідно до «Національної політики у галузі кібербезпеки», є: створення ефективної системи захисту персональної інформації громадян Індії, фінансової і банківської інформації та даних, що мають значення для державного управління і безпеки, від несанкціонованого доступу та кібератак; досягнення високого рівня надійності роботи ІКТ-систем та їх повномасштабного впровадження в усі сектори економіки; підготовка необхідну кількість (близько 500 тисяч) професіоналів протягом наступних 5 років для підвищення рівня безпеки та надійності інформаційного простору держави (Ministry of Electronics & Information Technology, Government of India, 2013).

Основними сферами практичної діяльності з метою формування національної системи кібербезпеки у «Національній політиці у галузі кібербезпеки» визначено кібербезпеку, кіберзахист та кіберрозвідку. Відповідно до положень документу, кібербезпека розглядається як діяльність, спрямована на захист інформації та інформаційних систем (мереж, комп'ютерів, баз даних, центрів обробки даних та додатків) із застосуванням відповідних процедурних та технічних заходів безпеки. У цьому сенсі поняття кібербезпеки є доволі широким і охоплює усі види діяльності із захисту. Кіберзахист тлумачиться у документі як більш вузький вид діяльності, пов'язаний з певними аспектами та організаціями. Основна відмінність між кібербезпекою та кіберзахистом у мережевому середовищі полягає у характері загроз для того, що має бути захищеним з використанням усього спектру доступних інструментів. Кіберзахист відноситься до оборонних дій, спрямованих на протидію деструктивній діяльності ворожих акторів, які мають політичну, квазіполітичну або економічну мотивацію, що впливає на національну безпеку, громадську безпеку або економічний розвиток суспільства (Ministry of Electronics & Information Technology, Government of India, 2013)

Для досягнення цілей у сфері кібербезпеки запропоновано такі практичні кроки: підвищення рівня обізнаності щодо загроз інфраструктурі ІКТ для

оперативного визначення та реалізація відповідного типу реагування; створення сприятливого правового середовища для підтримки безпечного кіберпростору, підвищення рівня довіри та впевненості в електронних транзакціях, посилення повноважень правоохоронних органів, що має забезпечити можливість підвищення рівня відповідальності за протиправні дії; захист ІКТ-мереж та критично важливих елементів інформаційної інфраструктури; введення механізму оперативного реагування на кіберінциденти, надзвичайні ситуації у кіберсередовищі в режимі 24/7; реалізація політики у сфері кібербезпеки із дотриманням міжнародних норм і стандартів; створення культури кібербезпеки та відповідальної поведінки у кіберсередовищі тощо (Ministry of Electronics & Information Technology, Government of India, 2013).

У «Національній політиці у галузі кібербезпеки» було представлено й організаційну структуру установ та відомств, залучених до формування національної системи кібербезпеки. Тут відразу слід зазначити, що однієї координуючої урядової установи у системі так й не було визначено, що на думку експертів, є одним з найбільших недоліків політики. При цьому було чітко розподілено між установами та відомствами відповідальність за різні напрями формування кіберекосистеми Індії. Так, під загальним керівництвом Офісу прем'єр-міністра Індії працюють: Національна інформаційна рада (розробляє політику щодо кібербезпеки), Національний кіберкоординаційний центр (працює під керівництвом Національної інформаційної ради і відповідає за електронне спостереження в Індії), Національна організація технічних досліджень (спеціалізоване агентство технічної розвідки Індії), Національний центр захисту критичної інформаційної інфраструктури (працює для забезпечення безпеки критичної інфраструктури країни), Об'єднаний розвідувальний комітет (працює під керівництвом Секретаріату Ради національної безпеки у тісній координації з іншими зовнішніми агентствами), Дослідницько-аналітичне управління (зовнішнє розвідувальне агентство Індії також стежить за кіберзагрозами або атаками з іншої території). Інші напрями діяльності здійснюються 4-ма міністерствами, в яких працюють 12 регуляторних органів, зокрема, Міністерством оборони (під його керівництвом функціонують такі

організації, як Управління оборонної розвідки, Управління військової розвідки, Управління повітряної розвідки, Управління військово-морської розвідки, Служба оборонної інформації і дослідницьке агентство, організація оборонних досліджень і розробок, які займаються збором розвідувальних даних і моніторингом кіберактивності); Міністерством внутрішніх справ (під його керівництвом існують такі організації, як Відділ кібербезпеки та інформаційної безпеки, Бюро розвідки і Центральна науково-криміналістична лабораторія, які зосереджені на внутрішніх налаштуваннях кібербезпеки, разом із кіберкриміналістикою); Міністерством електроніки та інформаційних технологій (під його керівництвом працюють такі організації, як Національний інформаційний центр, Індійська команда реагування на комп'ютерні надзвичайні ситуації (CERT-In), Центр розвитку передових обчислень, які відповідають за розробку сучасних технологій моніторингу кіберактивності); Міністерством закордонних справ (під керівництвом міністерства питаннями кібербезпеки займаються посли, верховні комісари, аташе з питань оборони з різних збройних сил Індії та спільні секретарі) (Singh, 2019).

Питання визначення функцій і повноважень державних структур є важливим і з погляду вирішення проблеми регулювання сфери кібербезпеки. Як зазначають експерти, Індія прагне знайти компроміс між системою, зорієнтованою на ринок, яка передбачає перекладання відповідальності (у тому числі, фінансової) за створення ефективної системи безпеки мереж і технологій на приватний сектор, і системою, що передбачає впровадження регуляторної політики, яка надає можливість державним структурам, яким делеговано вирішення питань кібербезпеки, втручатися у роботу інформаційного сектора з метою підвищення рівня кібербезпеки критичної інфраструктури та безпеки послуг електронного урядування (Bagga, 2018). Як надмірне втручання держави, так й висока вартість приватних рішень є неприйнятним для Індії. Зокрема, державний контроль може підірвати довіру до бізнес-інновацій і зробити їх неконкурентоспроможними внаслідок зарегульованості інформаційного сектору економіки. Отже слід шукати механізми для співпраці між приватним і державним секторами через заохочення останнього до впровадження сучасних механізмів у сфері кібербезпеки, наприклад, через

державне фінансування інноваційних проектів, податкові пільги тощо. Про це зазначається в ухваленій «Національній політиці у галузі кібербезпеки», але перелік можливих форм співпраці та механізми її реалізації, на жаль, відсутні (Data Security Council of India, 2013).

Отже, «Національна політика у галузі кібербезпеки» була першим стратегічним документом Індії у сфері формування національної системи кібербезпеки. Вона окреслила не тільки пріоритети, а й визначила практичні шляхи їх реалізації. У документі також представлено організаційну систему кібербезпеки та визначено обов'язки усіх зацікавлених сторін. Водночас, як свідчать данні, незважаючи на існування комплексної стратегії та розроблені практичні заходи, кількість кіберінцидентів в Індії продовжувала зростати і у 2013-2014 рр. досягнула свого піку. Серед найбільш поширених видів кібератак було визначено несанкціонований доступ до інформації, розташованої на веб-сайтах, поширення шкідливого програмного забезпечення, віруси-вимогачі, заражені боти, фішинг, спам, DDoS-атаки тощо. Показовим був й той факт, що джерелами атак все частіше ставали інші держави. Так, відповідно до звітів CERT-In, більшість кібератак (35 %) на офіційні веб-сайти Індії відбувається з Китаю, а також зі США (17 %), Росії (15 %), Пакистану (9 %), Канади (7 %), Німеччини (5 %), Нідерландів (4 %), Північної Кореї (2 %) та Франції (2 %). Атаки (фішинг, спам, шпигунство та пошкодження веб-сайту) були здійснені переважно на офіційні веб-сайти уряду Індії та інших державні установи. Постраждали також індійські компанії, зокрема Oil and Natural Gas Corporation (ONGC), National Informatics Center (NIC), Indian Railways Catering and Tourism Corporation (IRCTC) і Center for Railway Information Systems (CRIS), найбільші державні банки – Національний банк Пенджабу (PNB), Східний торговий банк (OBC) і Державний банк Індії (SBI) (Singh, 2019).

У наступному, 2014 р. стратегія кібербезпеки була уточнена новим документом – «Національна політика інформаційної безпеки та рекомендації», підготовленим Міністерством внутрішніх справ Індії. Основною ідеєю документу стало вироблення практичних механізмів захисту інформації, яка може вплинути на національну безпеку держави. Метою цього документу є покращення стану

інформаційної безпеки передусім у сфері державного управління та національної безпеки. Більш того, урядові структури, згідно з цим документом, можуть не обмежуватися визначеними керівними принципами і вживати додаткових заходів в залежності від ситуації, що складається, важливості інформації, яку необхідно захистити, та критичності елементу інфраструктури, які піддаються атаці. Документ по суті містить комплексний перегляд «Посібника з відомчих інструкцій безпеки» 1994 року з метою вироблення сучасних підходів до вирішення питання інформаційної безпеки, але вже у кіберпросторі. Отже «Національна політика інформаційної безпеки та рекомендації» був підготовлений Міністерством внутрішніх справ на основі досвіду впровадження вже існуючих стандартів і рамок безпеки інформації, найкращих світових практик і досвіду із врахуванням проблеми розширення масштабів нових типів загроз для національної безпеки. Як зазначається у документі, загрози для інформації стають все більш організованими та цілеспрямованими, допомагаючи злочинцям, державним діячам і хакерам отримувати величезні вигоди від компрометації інформації, крадіжки чи шпигунства (Ministry of Home Affairs Government of India, 2014).

Таким чином, як зазначають експерти, Індія вже у 2014 р. спромоглася розробити необхідні механізми для забезпечення кібербезпеки, водночас їх впровадження виявилося не таким ефективним і у сфері кібербезпеки, і у сфері кібероборони. Багато перспективних проектів, запропонованих індійським урядом, так й не були реалізовані, зокрема, щодо організації діяльності спеціально утворених установ, зокрема, Національного центру захисту критичної інформаційної інфраструктури та Національного кіберкоординаційного центру Індії (Jain, 2015). Отже реалізація «Національної політики кібербезпеки Індії» 2013 р. не може вважатися ефективною, оскільки так й не було в повній мірі досягнуто заявлені базові пріоритети, цілі і завдання на практиці. Впровадження механізмів кібербезпеки виглядає слабким у багатьох аспектах, включаючи питання порушення конфіденційності, загалом, і втручання в громадянські права і свободи, зокрема (Parmar, 2018).

Водночас зволікання з впровадженням стратегії кібербезпеки ставало для Індії дедалі більш проблематичнішим, оскільки держава продовжувала потерпати від різноманітних атак на інформаційний простір та критичну інфраструктуру – банки, супутники, електромережі, теплові електростанції тощо. Наприклад, станом на 2014 р. Індія посіла сьоме місце за кількістю кібератак у світі. За даними статистики, кількість кіберінцидентів та кібератак у середині 2014 р. досягнула 62000. Лише за 2013 - 2014 рр. кількість атак на урядові структури зросла на 136 %, на фінансові установи – на 126 %, 69 % атак були спрямовані на великі підприємства, а чотири з десяти були здійснені на сферу послуг. Отже, перед Індією постала очевидна потреба розробити більш ефективний план управління кіберкризою та створити надійну систему безпеки та захисту від нового типу загроз (Parmar, 2018).

Показовим є результати дослідження стану кібербезпеки країн, представлені у щорічній доповіді Міжнародного союзу електрозв'язку у 2017 р., де Індія посіла 23 місце серед 165 країн за рівнем розвитку системи кібербезпеки і отримала оцінку 0,683, тобто була віднесена до категорії «дозрівання» (ITU, 2017). Ці показники свідчать про те, що Індія прагне створювати ефективну систему кібербезпеки, має для цього відповідне політичне бачення та правову основу, володіє необхідним технічним і людським потенціалом. Але при цьому держава не може ефективно використати наявні ресурси для того, щоб захистити інформаційну екосистему і створити сприятливі умови для подальшої модернізації держави. Як наслідок, неготовність Індії ефективно протистояти кіберзагрозам, буде й надалі гальмувати реалізацію інших важливих проектів – електронного урядування, інформаційної економіки та електронної комерції тощо. В іншому дослідженні рівня розвитку кібербезпеки в країнах світу британської компанії Comparitech (2019 р.) Індія посіла 15-те місце з 60-ти досліджуваних країн за показниками рівня зараженості вірусами персональних комп'ютерів та мобільних телефонів, кількості різноманітних кібератак, ступеня готовності країни протистояти таким атакам та рівня розвитку законодавства у сфері кібербезпеки. На думку експертів, країна має достатньо розгалужене сучасне законодавство у сфері кібербезпеки, але ефективність

впровадження стратегій, на жаль, не може бути оцінена позитивно, що призводить до підвищення рівня вразливості держави до кібератак (Moody, 2019).

Так, у першому півріччі 2019 р. Індія знову зазнала найбільшу кількість кібератак серед держав світу. Найчастіше об'єктами кібератак ставали мережа підключених до інтернету пристроїв та інфраструктура (Сябро, 2019а). Як стверджує Subex, індійська телекомунікаційна компанія, яка видає регулярні звіти про кібербезпеку, лише з квітня по червень зареєстровані кібератаки зросли на 22 %, було виявлено 2550 унікальних зразків шкідливого програмного забезпечення (Subex, 2019).

Але найбільш небезпечною тенденцією стали кібератаки на критично важливі елементи інфраструктури – атомну електростанцію Куданкулам та Індійську організацію космічних досліджень. Так, у жовтні 2019 р. з'явилося повідомлення про виявлення зловмисного програмного забезпечення в комп'ютерних системах атомної електростанції Куданкулам у Таміл Наду, найновішої та найбільшої електростанції в Індії. Спочатку керівництво станції спростувало інформацію і звинуватило П. Сінгха, дослідника кібербезпеки, який раніше працював у Національній організації технічних досліджень, індійському агентстві сигнальної розвідки, у поширенні недостовірної інформації про враження програмою критично важливих цілей. Одним з найпереконливішим аргументом стало те, що системи управління електростанцією не підключені до інтерну, існує багаторівнева система захисту, а отже зараження не може відбутися. Але інцидент на іранському заводі зі збагачення урану в Натанзі за допомогою вірусу Stuxnet показав, що зараження може відбутися через USB-накопичувач працівника. Отже атака була цілком можлива. Згодом факт зараження був підтверджений, а шкідливе програмне забезпечення було ідентифіковане як вид DTrack, який дає зловмисникам детальний звіт про те, що роблять жертви, аж до натискань клавіш. Зазвичай він використовується для моніторингу цілі, що полегшує доставку подальших шкідливих програм. На думку британського експерта центру Royal United Services Institute Т. Планта, Північна Корея могла зацікавитися саме Куданкуламом з метою викрадення інноваційних технологій у сфері ядерної енергетики для власних

ядерних електростанцій (A cyber-attack on an Indian nuclear plant, 2019). Хоча суттєвих збитків або шкоди атаки на атомну електростанцію Куданкулам та Індійську організацію космічних досліджень не завдали, цього виявилося достатньо для того, щоб Індія продовжила активну діяльність у сфері кібербезпеки на національному і міжнародному рівнях. Недоліки у реалізації політики у сфері кібербезпеки, відсутність механізмів моніторингу та оцінки ефективності виконання поставлених завдань, певна хаотичність у реалізація пріоритетів стратегії призвели до потреби переглянути підходи держави до проблеми кібербезпеки і запропонувати нові механізми реалізації базових пріоритетів вже у наступній Національній політиці у сфері кібербезпеки на 2020-2025 рр. (Waghre, 2019).

Пандемія Covid-19 обумовила підвищення кількості користувачів сучасними інформаційно-комунікаційними технологіями та онлайн-послугами, що зробило населення Індії більш залежним від технологій та їх проникнення у суспільство. При цьому змінилася не тільки статистика щодо кількості пристроїв, якими користується населення, їх приєднання до різноманітних мереж та використання соціальних платформ, але й щодо онлайн-послуг, що надаються державною і бізнесом, онлайн-зайнятості, онлайн-медицини тощо. Таким чином, рівень залежності від технологій та онлайн-послуг суттєво підвищився, що суттєво вплинуло на поглиблення проблеми забезпечення безпеки інформаційної діяльності та інформаційного простору держави. Під ударом опинилися як окремі користувачі, так і критично важливі елементи інфраструктури. Результатом стало нове суттєве зростання кількості атак. Так, за даними уряду Індії, у 2020 р. було зафіксовано 1,16 мільйона випадків кібербезпеки, що втричі більше, ніж у попередньому році. Майже щомісяця у 2021 р. відбувалися різноманітні атаки, збої у діяльності або витік інформації. Так, на початку року відбувся масштабний витік персональної інформації внаслідок кібератаки, що призвело до появи на урядових сайтах результатів лабораторних тестів на COVID-19 тисяч громадян Індії. У травні цього ж року внаслідок кібератаки на системи постачальника послуг даних авіакомпанії відбувся витік особистих даних 4,5 млн пасажирів авіакомпанії. Того ж місяця відбулося несанкціоноване оприлюднення особистої інформації та результатів тестів

190 000 кандидатів на загальний вступний іспит (Relia, 2021). Найбільшу кількість кібератак (42 % від загальної кількості) було скоєно на штат Махараштра. У звіті американської фірми з кібербезпеки Palo Alto Networks зазначалося, що Індія є одним з найбільш економічно вигідних регіонів для діяльності окремо діючих хакерів та хакерських груп, які використовують віруси-вимагачі для атаки на індійські компаній. Як зазначають аналітики, у 2021 р. кожна четверта індійська організація зазнала атаки програм-вимагачів, що вище середнього світового показника на 21 % (National Cyber Security Strategy, 2022). Об'єктами злочинної діяльності стали також підприємства енергетичного сектору Індії. Так, китайська група Red Echo була звинувачена у використанні шкідливого програмного забезпечення ShadowPad для доступу до серверів енергетичних компаній. Хакерська група також виявила прогалини та вразливі місця в IT-інфраструктурі та програмному забезпеченні ланцюга поставок Bharat Biotech та Serum Institute of India (National Cyber Security Strategy, 2022).

Таким чином стало зрозумілим, що потрібна оновлена комплексна стратегія і політика кібербезпеки, яка враховувала б нові реалії наукового і технологічного розвитку, а також темпи і масштаби оцифровування індійського суспільства та формування розгалуженої інформаційної інфраструктури. Від нової стратегії очікували більш практичну зорієнтованість і конкретні дії, спрямовані на вирішення нагальних проблем у сфері кібербезпеки. У 2020 р. Радою безпеки даних Індії (DSCI) було оприлюднено Звіт з кібербезпеки, в якому йшлося про новий концепт Національної стратегії кібербезпеки, зорієнтований на 21 сферу забезпечення безпечного, захищеного, надійного, стійкого та активного кіберпростору для Індії. Основними напрямами діяльності було визначено: створення безпечного кіберсередовища для надання державних онлайн-послу, безпека ланцюга постачання інтегральних схем (ІКТ) та електронних виробів (передбачає також використання потенціалу країни в галузі розробки напівпровідників у всьому світі на стратегічному, тактичному та технічному рівнях), захист критично важливої інформаційної інфраструктури (інтеграція безпеки контролю та збору даних (SCADA), моніторинг вразливостей, формування загальної системи безпеки і

контролю, аудит та підвищення рівня готовності до загроз, кіберстрахування), безпека цифрових платежів, а також продовження розробки політики кібербезпеки на державному рівні, гарантії безпеки з боку держави для малого та середнього бізнесу (передбачає навіть політичне втручання в кібербезпеку, що має стимулювати підвищення рівня готовності до кіберінцидентів), розробка стандартів безпеки, рамок та архітектур для впровадження технологій Інтернету речей (IoT) та сучасної індустріалізації. Було також запропоновано збільшити державне фінансування сфери кібербезпеки та збільшити інвестиції в інноваційні технологічні розробки у сфері кібербезпеки (Ghosh, 2021).

У 2021 р. урядом було оприлюднено проект національної стратегії кібербезпеки, в якому представлено оновлене бачення механізмів забезпечення стійкості і безпеки функціонування кіберпростору. Стратегія має слугувати орієнтиром для політики управління даними як національним ресурсом, створення місцевих можливостей забезпечення безпеки використання інформаційних ресурсів та мереж і проведення кібераудитів.

На думку експертів, оновлена « Політика кібербезпеки» повинна обов'язково включити три важливі сфери: удосконалення правової бази, розвиток системи кіберреагування та удосконалення системи захисту даних.

1) Удосконалення правової бази. Оскільки Індія не має спеціального закону з кібербезпеки, усі випадки, пов'язані із порушеннями у сфері інформації і комунікації, регулюються Законом про інформаційні технології, Кримінальним кодексом та Правилами компаній (управління та адміністрування), а також нормативними актами для окремих галузей, виданими різноманітними регуляторними органами, в яких міститься вимога до дотримання стандартів кібербезпеки фінансовими структурами та компаніями, що працюють у сфері електронної комерції та інформаційного бізнесу, зокрема, банківськими структурами, страховими компаніями, постачальниками телекомунікаційних та інших цифрових послуг. Важливим є те, що із розвитком сучасних технологій та пришвидшення процесу надання послуг онлайн за рахунок модернізації цифрових пристроїв та якості зв'язку (впровадження 5G-зв'язку), кібератаки також значно

модернізуються і адаптуються до сучасних технологічних можливостей компаній, організацій, населення. Тому, в умовах зростання обсягів послуг онлайн-платежів та онлайн-страхування, які можуть надаватися миттєво, час для реагування на кібератаки у компаній, які працюють у платіжній екосистемі, значно скорочується, а отже потрібні більш досконалі механізми забезпечення безпеки системи надання онлайн-послуг, як на правовому, так й на технологічному рівні (Relia, 2021).

2) Розвиток системи кіберреагування. Будь-яка організація чи структура, відповідальна за управління кіберпростором на національному рівні, повинна мати чітку систему обов'язків та повноважень, щоб всі існуючі ресурси могли використовуватися максимально ефективно. На жаль, в Індії такої системи так й не вдалося створити. В державі існує кілька урядових установ, які займаються різними аспектами кібербезпеки. У кожній оборонній структурі є власні кіберексперти, і навіть державна поліція має своїх кіберрозслідувачів. Отже існує нагальна потреба об'єднати зусилля експертів, які працюють під керівництвом окремих урядових міністерств і відомств, для досягнення спільної мети. Такою структурою під егідою уряду може стати Національне кіберкомандування (Relia, 2021).

3). Удосконалення системи захисту даних. В Індії, як державі, яка оцифровується надшвидкими темпами, інформаційні ресурси перетворюються на важливі національні стратегічні ресурси. Як зазначають експерти, більшість інформаційно розвинених країн мають відповідне законодавство із захисту даних, у тому числі, у кіберпросторі. В Індії Законопроект про захист даних був поданий до парламенту в 2019 р., але, незважаючи на те, що проблема захисту даних для багатьох індійців є надзвичайно актуальною, документ так і не був ухвалений (Relia, 2021).

Таким чином, політика Індії у сфері кібербезпеки має скоріше реактивний характер. Наприклад, на початку 2022 р. міністр внутрішніх справ А. Шах оголосив про створення нового комітету з питань кібербезпеки соціальних мереж. Таке рішення дало підстави для звинувачень у неефективності стратегії та її реалізації з боку представників інших міністерств, а також для закликів перейти нарешті на проактивну політичну діяльність. Саме такий підхід може дозволити реалізовувати

скоординовану політику у відповідь на збільшення кількості кіберзагроз та кіберризиків, що є вкрай важливим в умовах подальшої цифровізації Індії. Стає очевидною потреба трансформації національної політики кібербезпеки, а також формування політичних і правових засад регулювання кіберпростору з метою гарантії його безпеки і стійкості до різноманітних кіберзагроз. Важливим кроком також має стати рішення про те, що Національний кіберкоординаційний центр повинен отримувати постійні звіти кібераудиту від інших структур, які займаються різними питаннями кібербезпеки, що має покращити управління кібербезпекою та удосконалити національну політику кібербезпеки. Варто також зосередитися на подальшому розвитку державно-приватного партнерства на основі довіри та збільшення бюджетного фінансування досліджень у сфері кібербезпеки. Значної уваги також потребує проблема розвитку людського потенціалу та підготовки персоналу для формування потужної кіберекосистеми (Bhattacharjee, 2022).

Зазначимо, що важливим чинником формування національної системи кібербезпеки є зростання кількості політично та економічно мотивованих кібератак з території сусідніх держав. На думку експертів, на даний момент ключовими супротивниками Індії в кіберпросторі вважаються Пакистан і Китай. Наприклад, КНР постійно здійснює повномасштабні кібероперації проти Індії, які вже набули такого розмаху, що іноді можуть бути охарактеризовані як повномасштабна кібервійна. З 2016 р. Індія стала шостою країною за кількістю нападів хакерів з Китаю – після США, Південної Кореї, Гонконгу, Німеччини та Японії. Згідно зі звітом американської компанії з кібербезпеки FireEye, найчастіше атакували державні сайти, а також телекомунікаційні компанії, медіа-компанії, центри високих технологій та системи управління транспортом. Найактивнішими китайськими хакерськими групами на даний момент є APT41 (націлена на 14 країн, включаючи Індію), APT 40 (націлена на країни, які є центральними для ініціативи «Один пояс, один шлях»), APT10 (активна з 2009 р., націлений на Індію, Японію та Північну Європу) і APT19 (атакує юридичні та інвестиційні компанії). Інша група, APT30, щонайменше 10 років збирала розвіддані з Індії та країн Південно-Східної Азії. Але востаннє про це повідомлялося в 2015 р., і наразі невідомо, чи вона досі активна. Як

повідомляє CERT-In, до 2018 р. приблизно 35 % усіх кібератак на індійські сайти було здійснено з Китаю. Тим часом китайські ЗМІ заявили, що індійські хакери атакували медичні організації Китаю під час спалаху COVID-19 (Banerjee, 2020).

Масштабні кібератаки завдала по Індії китайська група кібершпигунів Suckfly. Так, за даними компанія Symantec у 2016 р. кібершпигуни здійснили цілу низку атак на індійські урядові та комерційні організації (China Based Cyber Espionage Group Targeting Indian Companies, 2016). Хакерська група використовувала шкідливе програмне забезпечення під назвою Backdoor.Nidiran з дійсним сертифікатом підпису коду, який зловмисники попередньо викрали в Південній Кореї (Suckfly Hackers Target Organizations in India, 2016; Defence forces on alert after Chinese cyber attack, 2016). У тому ж 2016 р. KasperskyLabs повідомила, що китайська кібершпигунська група Danti, можливо, зламала комп'ютери високопоставлених чиновників у Делі та інших місцях. Представники Департаменту електроніки та інформаційних технологій визнали «велику» кібератаку, але відмовилися розголошувати подробиці, заявивши, що це може зашкодити розслідуванню. Згодом представники уряду визнали злом кількох комп'ютерів у секретаріаті Кабінету міністрів, але відразу повідоми, що наслідки повністю усунуті (Chinese hackers may have stolen government info, 2016).

Ще одним прикладом, який продемонстрував небезпеку застосування кібератак у протистоянні держав, стала атака китайських хакерів на мережі енергопостачання Мумбаї. Так, у жовтні 2020 р після прикордонного зіткнення між Народно-визвольною армією Китаю та збройними силами Індії в Гімалаях відбулася кібератака на системи управління електромережею Мумбаї, що призвело до зупинки потягів, закриття фондового ринку, знеструмлення лікарень (в умовах пандемії лікарням довелося перейти на аварійні генератори, щоб підтримувати роботу апаратів штучної вентиляції легенів) та відключення електроенергії для 20 мільйонів людей. Як показало дослідження американської компанії Recorded Future, шкідливе програмне забезпечення потрапило до систем управління мережами саме під час конфлікту, але було задіяне згодом (Sanger, 2021). Таким чином, збільшення кількості кібератак викликало занепокоєння з боку силових відомств, адже

протистояння між державами могло набувати різних форм – від злому індійських мереж до проявів кіберзлочинності і кібертероризму. При цьому Пекін і Нью-Делі на офіційному рівні продовжують зміцнювати відносини не тільки в політичній і військовій сфері, а й у сфері кібербезпеки.

Але більш масштабним є протистояння у кіберпросторі між Індією і Пакистаном. Незважаючи на те, що експерти оцінюють можливості обох країн вести кібервійну як досить обмежені, вони активно вдаються до різноманітних засобів протистояння, особливо під час ескалації двостороннього конфлікту у політичній площині. Як правило, пакистанські спецслужби або організують злом сайтів індійських відомств і пов'язаних з державою компаній (подібні операції завдають порівняно малий збиток), або через інтернет вербують діючих співробітників індійських силових структур для інсайдерської діяльності. Двосторонній кіберконфлікт часто переходить у форму подання недостовірної інформації, новин або чуток через Facebook та мессенджери, зокрема, WhatsApp, що призводить до проблеми мілітаризації соцмереж. Програмне забезпечення, розроблене Пакистаном та приховане у спеціально створених фейкових блогах та новинних сайтах, може активувати веб-камери, викрадати інформацію, що передається через електронну пошту, робити знімки екрана комп'ютерів жертв. Індія ж розробила складну технологію шпигування, що використовується на платформі Android, яка вважається найбільш популярною мобільною операційною системою в регіоні (Fazzini, 2019.

У двосторонньому кіберконфлікті беруть участь різноманітні хакерські угруповання та хактивісти, які використовують Інтернет для здійснення атак на урядові веб-сайти Індії або Пакистану (наприклад, спотворюють інформацію, представлену на сайті). Як правило атаки посилюються внаслідок фізичного зіткнення між збройними силами обох країн (Mustafa, 2020). Переважно йдеться про зіткнення в районі Кашміру. У листопаді 2008 р. Пакистанська кіберармія (PCA) вперше здійснила напад з метою руйнуванням системи кібербезпеки Індійської нафтової та газової компанії, у 2013 р. – кібератаку на міжнародний аеропорт імені Індіри Ганді, у 2016 р. – фішингову атаку на сайти посольств Індії в Казахстані та Саудівській Аравії, а також реалізувати низку атак з метою кібершпигунства проти

індійських військових протягом місяця (операція « C-Major») тощо (WAQAS, 2016). Як зазначають експерти, пакистанські кіберзлочинці щодня псують майже 60 індійських веб-сайтів, поширюючи через них модифіковану інформацію політичного, фінансового чи релігійного характеру.

В рамках розслідування терористичної атаки 26/11 в Мумбаї було виявлено, що терористи активно використовували під час підготовки і скоєння злочину загальнодоступні електронні системи навігації, завдяки яким чітко знали карти, місцерозташування об'єктів, інфраструктуру навколо. Окрім «Google Earth» вони також користувалися мобільним зв'язком для координації діяльності і контролю виконання завдань, соціальні мережі для відстеження пересування рятувальників та підрозділі правоохоронців, а також технологію «перетворення аудіосигналів на дані», яка унеможливила відстеження джерела інформації силами оборони Індії. Зрештою Уряд Індії був змушений розробити потужний механізм боротьби з проблемою кібертероризму. Як наслідок, до Закону про інформаційні технології 2000 р., Кримінального кодексу та інших правових документів було внесено поправки, які включають розділи про боротьбу з кібертероризмом та іншими пов'язаними з ним питаннями (Raman, Sharma, 2019).

Індійські хакери і хактивісти, які позиціонують себе як програмісти-патріоти, працюють над захистом власного інформаційного простору та інфраструктури, а також здійснюють потужні кібератаки у відповідь. Наприклад, нині ефективно діє відома хакерська група під назвою Mallu Cyber Soldiers – анонімна група експертів з кібербезпеки, які працюють над захистом індійських веб-сайтів від злому (Exclusive: Who are 'Mallu Cyber Soldiers' that hacked Pakistan websites, 2022).

Показовою є тенденція поглиблення співпраці між Пекіном та Ісламабадом у кіберпросторі. Так, між двома країнами був підписаний «Довгостроковий план китайсько-пакистанського економічного коридору (2017-2030)», в якому особливу увагу було приділено розвитку та просуванні електронної комерції в Пакистані. Як зазначають фахівці, поглиблення співпраці у сфері ІКТ може також свідчити про те, що Пакистан виступає як проксі для зловмисної діяльності Китаю у кіберпросторі, особливо у питаннях поширення антиіндійської пропаганди на платформах

соціальних мереж. Так, під час загострення протистояння між Індією і Китаєм пакистанські користувачі Twitter видають себе за китайських громадян і поширюють антиіндійську пропаганду, неправдиву інформацію про жорстокі зіткнення, наприклад, в долині Галван у червні 2020 року, а також про військову готовність Індії (Patil, Bhan, 2022). Отже формується двостороннє взаємовигідне партнерство. Так, китайська сторона виступає з ініціативами надання технологій і підготовки контенту, а Пакистан – в якості виконавця та розповсюджувача. Враховуючи особливості стратегії інформаційної політики і безпеки Китаю, йому потрібен Пакистан, оскільки основні соціальні медіа-платформи, такі як Twitter і Facebook, знаходяться під забороною, а володіння англійською мовою та хінді є дуже обмеженим. Більше того, використання Пакистану як проксі дає можливість уникнути звинувачень у безпосередньому нападі на Індію, роблячи Пакистан активним учасником антиіндійської діяльності. Для Пакистану ж співпраця з Китаєм дає можливість зміцнити двостороннє стратегічне партнерство та отримати значну технічну перевагу, якої Ісламабад не зміг би досягти самостійно (Patil, 2022).

Висновки до третього розділу

Дослідження особливості формування стратегії інформаційної безпеки Японії показало, що держава не тільки має високі показники темпів розвитку інформаційних технологій та їх впровадження у суспільство, але значну увагу приділяє питання безпеки технологій і мереж. В процесі еволюції стратегії держава пройшла кілька етапів: перший (1990-ті рр.) – прискорення інформаційного розвитку та ініціативи приватного сектору у сфері інформаційної безпеки за участю урядових структур, другий (2000-ті рр. – до 2013 р.) – збільшення масштабів кібератак та поява Першої і Другої національної стратегії інформаційної безпеки; третій (2013-2017 рр.) – зростання проблеми поширення кіберзагроз для всіх сфер життєдіяльності японського суспільства та ухваленням Першої (2013 р.) і Другої (2015 р.) стратегій кібербезпеки, четвертий (триває нині) – ухвалення нової стратегії розвитку Японії у 2017 «Суспільство 5.0», яка передбачає трансформацію

японського способу життя шляхом стирання кордону між кіберпростором і фізичним простором, що вплинуло на зміст програм у сфері кібербезпеки.

Базовим пріоритетом сучасної стратегії інформаційної безпеки та механізмів її реалізації виступає формування безпечного інформаційного середовища для розбудови сталої, інклюзивної соціально-економічної системи «Суспільства 5.0», що базується на цифрових технологіях, таких як аналітика великих даних, штучний інтелект, Інтернет речей і робототехніка. Основними напрямами сучасної стратегії кібербезпеки визначено забезпечення реалізації стратегії цифрової трансформації паралельно розробці і реалізації заходів у сфері кібербезпеки; формування відкритого, стійкого і безпечного кіберпростору із врахуванням проблеми залежності традиційного простору безпеки і кібернетичного; удосконалення заходів кібербезпеки в умовах пришвидшеної цифровізації економіки і японського суспільства; забезпечення середовища кібербезпеки на основі дотримання принципів вільного потоку інформації, конфіденційності та цілісності інформації; залучення всіх зацікавлених сторін з метою формування сучасної безпечної соціально-економічної інформаційної інфраструктури; підвищення рівня готовності до реагування на масовані кібератаки; участь у дво- та багатосторонньому співробітництві у сфері інформаційної безпеки, просування ініціатив у сфері кібердипломатії.

Індійська стратегія інформаційної безпеки від самого початку була зосереджена на проблемі лише кібербезпеки і мала переважно реактивний характер. Еволюція стратегії інформаційної безпеки відбувалася у кілька етапів. Перший етап – (2000-ні рр.) – ухвалення «Закону про інформаційні технології», який і нині залишається базовим нормативно-правовим документом у сфері регулювання питань національної кібербезпеки, створення систему спеціалізованих підрозділів у сфері кібербезпеки та визначено напрями їх діяльності; другий (2013-2019 рр.) – ухвалення першої стратегії «Національна політика кібербезпеки» у 2013 р., у якій було окреслено загальну позицію держави у сфері кібербезпеки і запропоновано практичні механізми реалізації пріоритетів політики та створення безпечної кіберекосистеми по всій країні; третій (з 2020 р.) – оприлюднення проекту

Національної стратегії кібербезпеки, в якій представлено оновлене бачення механізмів забезпечення стійкості і безпеки функціонування кіберпростору. Пріоритетами сучасної стратегії у сфері інформаційної безпеки Індії є формування безпечного кіберсередовища для надання державних онлайн-послу, захист критичної інформаційної інфраструктури, кібербезпека малого і середнього бізнесу, кібербезпека у сфері виробництва сучасних технологічних інновацій, моніторинг загроз та кібераудит. Важливим напрямом сучасної індійської стратегії кібербезпеки є розробка і реалізація стратегії кібероборони, що містить заходи, спрямовані на формування ефективної системи захисту від зовнішніх, часто політично мотивованих загроз. На даний момент ключовими супротивниками Індії в кіберпросторі вважаються Пакистан і Китай, які використовують швидкий інформаційний розвиток індійського суспільства та недоліки системи кібербезпеки держави.

ВИСНОВКИ

1. Трансформація парадигми безпеки нині відбувається під впливом прискорених процесів інформаційного і науково-технологічного розвитку. Поява технологій Четвертої індустріальної революції відкриває нові можливості для розвитку суспільства і впровадження нових моделей економічної діяльності, стандартів соціального забезпечення, моделей політичного управління та ухвалення політичних рішень. Водночас, викликає занепокоєння можливості використання окреслених технологічних досягнень з протиправною, злочинною чи терористичною метою, оскільки майже всі вони є технологіями подвійного призначення і можуть бути застосовані, наприклад, для підвищення боєздатності армії та удосконалення озброєнь держав-аутсайдерів, що може призвести до руйнування міжнародної системи миру і безпеки. До того ж у сучасних стратегіях протиборства спостерігається тенденція поєднання різних інноваційних технологій для завдання більш руйнівного удару по супротивникам. На жаль, як свідчить аналіз, сучасна система підтримання миру і безпеки не може адекватно відповідати на появу такого типу загроз, що викликає, з одного боку, прагнення держав включитися у процес розробки нових норм міжнародного права, які б регулювали б використання досягнень науки і технологій в контексті міжнародної безпеки, а з другого – використати доступні технології для посилення свого військового потенціалу та просування власних національних інтересів. У зв’язку з цим виникає питання включення фактору інформаційного і науково-технологічного розвитку до переліку базових характеристик сучасної парадигми безпеки. Особливої актуальності це питання набуває у контексті подальшого прискорення темпів інформаційного та науково-технологічного розвитку в АТР, який нині є регіоном масштабного геополітичного протистояння провідних акторів міжнародних відносин. Серед технологічних зрушень, які найбільше впливають на сучасну систему безпеки, доцільно виокремити процеси інформатизації та комп’ютеризації. Поява нових комп’ютерних технологій та їх подальше удосконалення, модернізація засобів

зв’язку та комунікації, призвели до появи нового простору геополітичного протистояння – кіберпростору.

2. Зміна парадигми безпеки в умовах прискореного інформаційного та науково-технологічного розвитку стала причиною теоретичного переосмислення питань міжнародної безпеки, еволюції форм і методів ведення війни, появи нових засобів протиборства, балансу сил та політики стримування. Це призвело до виникнення цілої низки досліджень з питань інформаційної геополітики, формування цифрового суверенітету, трансформації фактору сили у міжнародних відносинах, формування інформаційного потенціалу та кібермогутності держав, еволюції феномену війни та появи нових форм протиборства – інформаційної війни, кібервійни, когнітивної війни, гібридної війни, війни четвертого покоління, мережевої війни і мережево-центрованої війни, тринітарної війни, нових форм і методів протиборства, зокрема, появи інформаційної зброї та «перегорнутої мілітаризованої дипломатії». Як свідчить аналіз теоретичних і концептуальних розробок зарубіжних авторів, проблема інформаційної безпеки нині є надзвичайно актуальною, інтерес науковців до неї постійне зростає, що призводить до появи нових теоретичний і концептуальних розробок, присвячених дослідженню тенденцій розвитку феномену безпеки в умовах прискореного інформаційного і науково-технологічного розвитку. Питанню інформаційної безпеки присвідчено значну кількість теоретичних і прикладних досліджень українських фахівців, що свідчить про зростання актуальності тематики й для України.

3. Дослідження понятєво-категоріальних характеристик проблеми інформаційної безпеки дозволило виявити новітні підходи до визначення феномену інформаційної безпеки та його складових. Зокрема, було з’ясовано, що на сучасному етапі трансформації системи міжнародної безпеки внаслідок розширення практики використання інформаційних та науково-технологічних досягнень під час війн і конфліктів, виникла потреба переглянути вже існуючі понятійні категорії, зокрема, «міжнародна інформаційна безпека», «кібербезпека», «інформаційна війна», «кібервійна» тощо, із врахуванням реалій глобального геополітичного протиборства. Водночас з’явилися й нові понятєві категорії, пов’язані з сучасними

тенденціями у сфері інформаційної безпеки, наприклад, «мережна війна», «мережноцентрована війна», «війна четвертого покоління», «гібридна війна», «кібердипломатія», «кібероборона», «кібермогутність», «цифровий суверенітет», «перегорнута мілітаризована дипломатія», що свідчить про докорінні зміни у теорії та практиці функціонування системи міжнародної безпеки.

4. Сучасна архітектуру безпеки АТР формується під впливом низки традиційних та інноваційних чинників, що формують унікальні геополітичні характеристики регіону. Зокрема, на формування регіональної структури безпеки впливає наявність значної кількості двосторонніх конфліктів, територіальних претензій, політико-ідеологічних суперечок між провідними регіональними акторами, значний вплив США, який реалізується через механізми двостороннього співробітництва з країнами-союзниками – Японією, Південною Кореєю, Індією та Австралією, а також масштабне протистояння між США та Китаєм, прагнення КНР закріпити позиції геополітичного лідера в регіоні тощо. Інноваційною складовою виступає бурхливий інформаційний і науково-технологічний розвиток країн регіону, який є не тільки каталізатором вже існуючих проблем у традиційних вимірах геополітичного протистояння, але й призвів до появи нових викликів і загроз – інформаційних війн і конфліктів, політично мотивованих інформаційних атак, кіберзлочинності, кібершахрайства та кібертероризму, що обумовило включення питань інформаційної безпеки до пріоритетів регіональної політики безпеки. Показовою в цьому контексті є трансформація стратегії стримування Китаю, яка нині передбачає застосування не тільки класичних політичних або економічних інструментів, але й інформаційних та науково-технологічних.

5. Ключову роль у формуванні системи безпеки АТР відіграють регіональні інститути, до пріоритетів діяльності яких увійшли питання інформаційної безпеки, що розглядаються як фундаментальні, оскільки впливають на подальший поступальний розвиток регіону в цілому. Одним з провідних інститутів, який формує пріоритети політики у сфері регіональної інформаційної безпеки, є Асоціація Південно-Східної Азії (АСЕАН). Пріоритети діяльності Альянсу у сфері інформаційної безпеки зосереджені на формування стійкого і безпечного

кіберсередовища, що є вкрай важливим для держав-членів, враховуючи швидкі темпи їх інформаційного і технологічного розвитку та залежність від технологічних інновацій та іноземних інвестицій у НДДКР. Основними напрямами діяльності організації у сфері кібербезпеки на сучасному етапі є вироблення спільних підходів на рівні АСЕАН до вирішення проблем кібербезпеки із врахуванням інтересів і особливостей різних держав-членів; створення організаційної структури на рівні Альянсу для постійного обговорення проблем кібербезпеки, появи нових типів ризиків і загроз та вироблення механізмів протидії ним; нарощування регіонального кіберпотенціалу, побудови регіональної системи управління ризиками і загрозами у кіберсередовищі; створення регіональної системи кібербезпеки та оперативної протидії кіберінцидентам; боротьба з усіма формами транскордонної кібертерористичної діяльності у регіоні; впровадження гнучкого механізму обговорення та ухвалення рішень і питань кібердипломатії; розвиток співпраці між усіма державами регіону у сфері кібербезпеки та співробітництво на рівні міжнародних інститутів, зокрема, в рамках ООН з питань впровадження правил відповідальної поведінки держав у кіберпросторі. Таким чином, питання кібербезпеки стали важливою складовою стратегії співробітництва між країнами регіону та їх партнерами в умовах постійного ускладнення архітектури регіональної безпеки, а розвиток кіберпотенціалу держав-членів АСЕАН має підвищити здатність регіону реагувати на мінливий ландшафт кіберзагроз і створити безпечний і стійкий кіберпростір АСЕАН.

Іншим важливим регіональним учасником процесу формування системи регіональної інформаційної безпеки є Шанхайська організація співробітництва (ШОС). Сучасними пріоритетами політики у сфері інформаційної безпеки в рамках ШОС є розробка і реалізація заходів у сфері забезпечення міжнародної інформаційної безпеки відповідно до зміни типу і характеру інформаційних загроз; забезпечення інформаційної безпеки критично важливих структур держав ШОС; впровадження ефективних механізмів координації діяльності усіх держав-членів у сфері протидії пропаганді та виправданню тероризму, сепаратизму та екстремізму в інформаційному просторі; співпраця у сфері боротьби зі злочинним використанням

інформаційно-комунікаційних технологій і мереж; впровадження заходів, спрямованих на запобігання міждержавним інформаційних конфліктів та подолання дефіциту довіри, який виникає внаслідок використання високих технологій та мереж у протистоянні між державами; подальший розвиток норм міжнародного права у сфері міжнародної інформаційної безпеки; подальше просування ідеї ухвалення універсального кодексу правил, принципів та норм відповідальної поведінки держав в інформаційному просторі. Особливу роль у визначенні пріоритетів діяльності організації у сфері інформаційної безпеки відіграють РФ та КНР, які намагаються використати інститут для просування власних національних інтересів у регіоні. Для РФ участь в ШОС розглядається як спроба створити альтернативну західній систему інформаційної безпеки, яка б відповідала б пріоритетам діяльності держави у сфері інформації і комунікації, а для КНР – створення сприятливих умов для досягнення амбіційних цілей політичного, військового, економічного та інформаційного домінування в регіоні.

Чотиристоронній діалог з питань безпеки (QUAD), який об’єднує США, Японію, Австралію та Індію, слід розглядати як новий геополітичний інструмент стримування В утворенні QUAD найбільш зацікавлені Японія та Австралія, які виступають військово-політичними союзниками Америки, Індія ж залишається лише партнером в альянсі, незважаючи на розширення американо-індійського військового та військово-технічного співробітництва. Пріоритетом діяльності у сфері інформаційної безпеки четвірки є формування власної системи кібербезпеки, яка передбачає створення потенціалу стійкості інформаційної інфраструктури, особливо у контексті подальшого розвитку якості зв’язку і появи мереж 5G, з метою усунення вразливостей для кібербезпеки держав-учасниць; вироблення загальних принципів і стандартів у сфері кібербезпеки; впровадження ефективних механізмів протидії різноманітним кіберзагрозам, захист критичної інформаційної інфраструктури; впровадження механізмів боротьби з кіберзлочинністю; розробка та впровадженні стандартів безпеки програмного забезпечення в рамках QUAD; формування відкритої, доступної та безпечної технологічної екосистеми, що базується на спільних демократичних цінностях та повазі до універсальних прав

людини тощо. Стратегія QUAD у сфері кібербезпеки спрямована на створення ефективної системи захисту від кіберзагроз передусім з боку Китаю. Для цього було обрано стратегію формування «кіберстійкості» замість «наступальних кіберможливостей», що вважається більш надійний спосіб вирішення широко кола проблем кібербезпеки в Індо-Тихоокеанському регіоні.

6. Стратегія інформаційної безпеки Японії розвивалася під впливом потужних зрушень у сфері інформаційного і науково-технологічного розвитку. На основі аналізу еволюції стратегії інформаційної безпеки держави доцільно виокремити чотири основні етапи розвитку. Перший етап пов'язаний із прискоренням інформаційного розвитку у 1990-х рр. та ініціативами переважно приватного сектору у сфері інформаційної безпеки а участю урядових структур, другий – із зростанням масштабів інформаційних загроз для державного сектору на початку 2000-х рр. і появою Першої і Другої національної стратегії інформаційної безпеки; третій – із у зростанням проблеми поширення кіберзагроз для всіх сфер життєдіяльності японського суспільства та ухваленням Першої (2013 р.) і Другої (2015 р.) стратегій кібербезпеки, четвертий (триває нині) – із ухваленням нової стратегії розвитку Японії у 2017 р. «Суспільство 5.0», яка передбачає трансформацію японського способу життя шляхом стирання кордону між кіберпростором і фізичним простором, що вплинуло на зміст програм у сфері кібербезпеки.

Аналіз діяльності Японії у інформаційної безпеки уможливив висновки про особливості сучасної стратегії та механізмів її реалізації. Так, базовим пріоритетом стратегії інформаційної безпеки Японії на сучасному етапі є формування безпечного інформаційного середовища для розбудови сталої, інклюзивної соціально-економічної системи «Суспільства 5.0», що базується на цифрових технологіях, таких як аналітика великих даних, штучний інтелект, Інтернет речей і робототехніка. Найбільшого занепокоєння викликає утворення «кіберфізичної системи», в якій кіберпростір і фізичний простір тісно інтегровані, що призводить до появи нових ризиків і загроз для системи інформаційної безпеки. Основними загрозами для системи національної кібербезпеки Японії визначено небезпеку

використання технології штучного інтелекту під час здійснення кібератак; підвищення рівня вразливості економіки та суспільства в цілому внаслідок цифровізації суспільства та збільшення масштабів використання хмарних сервісів, впровадження продуктів і послуг, що надаються через складні глобальні ланцюжки поставок, використання пристроїв Інтернету речей у всіх галузях; постійне зростання загрози організованих і складних кібератак ззовні (від КНР, РФ та КНДР) з метою порушення роботи критичної інфраструктури, викрадення особистої інформації та інтелектуальної власності, втручання в демократичні процеси. Основними напрямами сучасної стратегії кібербезпеки визначено забезпечення реалізації стратегії цифрової трансформації паралельно розробці і реалізації заходів у сфері кібербезпеки; формування відкритого, стійкого і безпечного кіберпростору із врахуванням проблеми залежності традиційного простору безпеки і кібернетичного, тобто створення безпечного кіберфізичного середовища; удосконалення заходів кібербезпеки в умовах пришвидшеної цифровізації економіки і японського суспільства; підвищення рівня цифрової грамотності та грамотності у галузі інформаційної безпеки населення Японії; забезпечення середовища кібербезпеки на основі дотримання принципів вільного потоку інформації, конфіденційності та цілісності інформації; залучення всіх зацікавлених сторін з метою формування сучасної безпечної соціально-економічної інформаційної інфраструктури; підвищення рівня готовності до реагування на масовані кібератаки; участь дво- та багатосторонньому співробітництві у сфері інформаційної безпеки, просування ініціатив у сфері кібердипломатії.

7. Важливу роль у формуванні сучасної архітектури безпеки регіону відіграє Індія, яка характеризується як держава з динамічним розвиток інформаційно-комунікаційних технологій та мереж. Індійська стратегія інформаційної безпеки від самого початку була зосереджена на проблемі кібербезпеки і мала переважно реактивний характер. Аналіз еволюції стратегії кібербезпеки свідчить про пріоритетність цифрового розвитку та впровадження сучасних ІКТ у всі сфери життєдіяльності індійського суспільства для стратегії перспективного розвитку держави. Ухвалення низки стратегій мало важливе значення для системи

національної інформаційної безпеки, оскільки окреслило напрями практичної діяльності та визначило механізми впровадження цілей кібербезпеки. До основних пріоритетів сучасної стратегії у сфері кібербезпеки відноситься формування безпечного кіберсередовища для надання державних онлайн-послу, захист критичної інформаційної інфраструктури, кібербезпека малого і середнього бізнесу, кібербезпека у сфері виробництва сучасних технологічних інновацій, моніторинг загроз та кібераудит. Водночас, постійне зростання кількості і масштабів кібератак на державні, приватні та науково-дослідні мережі і ресурси свідчить про недостатню ефективність реалізації стратегії захисту національного інформаційного простору та критичної інфраструктури. До основних недоліків слід віднести відсутність чіткої координації структур, задіяних у реалізації стратегії кібербезпеки, неефективність механізмів моніторингу та аудиту реалізованих завдань, реактивний характер більшості ініціатив уряду у сфері кібербезпеки. Особливістю реалізації стратегії у сфері кібербезпеки є поєднання ринковоорієнтованих та державоцентристських підходів у сфері регулювання кібербезпеки шляхом впровадження державних ініціатив заохочення бізнесу до фінансової і технічної співпраці для досягнення ефективності у формуванні безпечного кіберсередовища. Важливим чинником забезпечення інформаційної безпеки держави є кібероборона, обумовлена проблемою часткового перенесення традиційних територіальних конфліктів і кіберпростір. Джерелами політично та економічно мотивованих кібератак часто виступають КНР та Пакистан, які використовують прогалини у системі кібербезпеки Індії для завдання удару по критично важливим елементам інфраструткури держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арквілла, Д., Ронфельдт, Д., 2005. Ще раз про прихід мережної війни. *Мережі і мережні війни: Майбутнє терору, злочинності та бойових дій* / за ред. Д. Арквілла і Д. Ронфельдт; пер.з англ. А. Іщенкаю. К.: Видавничий дім «Києво-Могилянська Академія».

2. Бєлоусова, Н.Б., 2018. Глобальні міста як джерело «м'якої сили» в XXI столітті. *Вісник МДУ. Серія: Історія. Політологія»* . Вип. 21. Маріуполь: МДУ. С. 85-90.

3. Гондюл, В.П., Макаренко, Є.А., Рижков, М.М., Бєлоусова, Н.Б., Даниленко, С.І., Запорожець, О.Ю., Кучмій, О.П., Романенко, Ю.В., Фролова, О.М. та ін., 2006. *Міжнародна інформаційна безпека: сучасні виклики і загрози*. К.: Центр вільної преси.

4. Горбулін, В., Дубов, Д., Ожеван, М., Литвиненко, О., Гнатюк, С., Яворська, Г. та ін., 2017. *Світова гібридна війна: український фронт / за* ред. В.П. Горбулін. К.: НІСД.

5. Дубов, Д., Бойко, В., Гнатюк, С., Ісакова, Т., Ожеван, М., Покровська, А., 2018. *Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України*: аналіт. доп. / за ред. Д. Дубов. К. : НІСД.

6. Дубов, Д.В., 2014. *Кіберпростір як новий вимір геополітичного суперництва*. К.: НІСД.

7. Дубов Д., 2010. *Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка.* Київ: НІСД. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/suchasni-trendi-kiberbezpekovoi-politiki-visnovki-dlya-ukraini> (дата звернення: 15 липня 2022).

8. Копійка, М.В., 2020. Політика інформаційної безпеки у сучасних міжнародних відносинах : дис. … д-ра філософії. Київський національний університет імені Тараса Шевченка. Київ, 2020. 205 с.

9. Кучмій, О.П., 2016. Інформаційна безпека США у сучасних зарубіжних дослідженнях В: *Регіональні стратегії США та Європи: зовнішньополітичний і безпековий вимір*. К.: Центр вільної преси. С.106-138.

10. Литвиненко, О.В., 2003. *Інформаційні впливи та операції*. Київ: НІСД.

11. Макаренко, Є.А., 2011. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. *Актуальні проблеми міжнародних відносин*. Випуск 102 (Частина І) URL: http://irbis-nbuv.gov.ua/cgi bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/apmv_2011_102%281%29__9.pdf> (дата звернення: 15 липня 2022).

12. Макаренко, Є.А., 2016. Трансформація регіональних безпекових стратегій США: прикладні дослідження. *Регіональні стратегії США і Європи: зовнішньополітичний і безпековий вимір*. К.: Центр вільної преси. С. 172-193.

13. Ожеван, М.А., Дубов, Д.В., 2017. Homo ex Machina. *Філософські, культурологічні та політичні передумови формування конвергентного суспільства*. К : НІСД.

14. Орлик, В.В., 2021. Чотиристоронній діалог з питань безпеки (QUAD) як новий формат партнерства в Індо-Тихоокеанському регіоні. URL: https://niss.gov.ua/doslidzhennya/mizhnarodni-vidnosini/chotiristoronniy-dialog-z-pitan-bezpeki-quad-yak-noviy-format)> (дата звернення: 15 липня 2022).

15. Перепелиця, Г.М., 2005. Асиметричні стратегії у сфері безпеки та оборони. *Асиметрія міжнародних відносин* / за ред. Перепелиця, Г.М., Субтельний, О.М. К.: Видавничий дім «Стилос». С. 468-530.

16. Почепцов, Г., 1999. Информационные войны. *Основы военно-коммуникативных исследоваaний*. Ровно: ППФ « Волинські обереги» .

17. Почепцов, Г., 2015. *Сучасні інформаційні війни*. К.: Києво-Могилянська академія.

18. Почепцов, Г., 2017. Від покемонів до гібридних війн. *Нові комунікативні технології XXI століття*. Київ: Видавничій дім «Києво-Могилянська академія».

19. Почепцов, Г., 2019b. Войны новых технологий. Харків: Фоліо.

20. Почепцов, Г., 2019c. Когнитивные войны в соцмедиа, массовой культуре и массовых коммуникациях. Харьков: Фолио.

21. Почепцов, Г., 2019a. *Виртуальные войны*. *Фейки*. Харьков: Фолио.

22. Рижков, М.М., Сябро А., 2019. Позиції держав Азійсько-Тихоокеанського регіону щодо ухвалення резолюцій з питань міжнародної інформаційної безпеки в рамках ООН. *Актуальні проблеми міжнародних відносин*. Випуск 139. С.13-26.

23. Романчук, Ю., 2009. Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти. Кандидат наук. Національна Академія наук України, Інститут світової економіки і міжнародних відносин. 203 с.

24. Сябро А.В., 2018. Сучасний стан розвитку інформаційно-комунікаційних технологій в Україні. *Гілея: науковий вісник.* 2018. Вип. 135 (№8). С. 364-367.

25. Сябро А., 2019a. Особливості національної стратегії кібербезпеки Індії. *Міжнародні відносини. Серія «Політичні науки».* 2019. № 20. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/4136 (дата звернення: 21 липня 2022).

26. Сябро А.В., 2019b. Пріоритети співробітництва Японії зі США у сфері кібербезпеки. *Гілея: науковий вісник*. 2019. Вип. 150 (№ 11). Ч. 3. С.72-77.

27. Сябро, А.В., 2019c. Мілітаризація кіберпростору як чинник актуалізації проблеми інформаційної безпеки у сучасних міжнародних відносинах. *Міжнародна інформація / Міжнародні комунікації: історія, сучасність і перспективи:* матеріали Міжнародної науково-практичної конференції, 6 грудня 2019 року. *Міжнародні відносини. Серія «Політичні науки».* 2019. № 21. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/3873/3533 (дата звернення: 01 серпня 2022).

28. Сябро, А.В., 2020a. Проблема запровадження обмежень у сфері інформації і комунікації як чинник забезпечення національної інформаційної безпеки. *Стратегічне позиціонування України в сучасному міжнародному просторі*: матеріали Міжнародної науково-теоретичної конференції, 15 жовтня 2020 року. Київ, 2020. С. 72-73.

29. Сябро, А.В. 2020b. Сутнісні характеристики стратегії інформаційної безпеки Південної Кореї. *Актуальні питання суспільних та гуманітарних наук (Глухівські читання-2020)*: збірник матеріалів X Міжнародної науково-практичної інтернет-конференції, 9-11 грудня 2020 року. Глухів: Глухівський НПУ ім. О. Довженка, 2020. С. 113-115.

30. Сябро, А.В., 2021a. Трансформація концепту «м'якої» сили в сучасному інформаційному протиборстві. *Травневі студії 2021: історія, міжнародні відносини, філософія:* збірник матеріалів III Міжнародної наукової конференції студентів та молодих вчених, 23 квітня 2021 року. Вінниця: ДонНУ імені Василя Стуса, 2021. Вип. 6. С. 92-94.

31. Сябро, А.В., 2021b. Інформаційна безпека у стратегіях діяльності міжнародних регіональних організацій (на прикладі АТР). *Шевченківська весна 2021:* матеріали Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених, 29 березня, 2021. Київ, 2021. С. 51-55.

32. Фролова, О.М., 2018. Роль ООН в системі міжнародної інформаційної безпеки. *Міжнародні відносини Серія « Політичні науки»*.. № 18-19. URL: <http://journals.iir.kiev.ua/index.php/pol_n/article/download/3468/3140 (дата звернення: 28 червня 2022).

33. Фролова, О.М., 2019. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. *Вісник Львівського університету. Серія «Міжнародні відносини* . № 46. С.123-136.

34. Шваб, К., 2019. Четверта промислова революція. Формуючи четверту промислову революція /переклад з англ. Н. Климчук, Я. Лебеденко. Харків, 2019.

35. A cyber-attack on an Indian nuclear plant raises worrying questions. India needs better cyber-hygiene in its nuclear industry. So does the world. *The Economist*. 1st Nov. URL: https://www.economist.com/asia/2019/11/01/a-cyber-attack-on-an-indian-nuclear-plant-raises-worrying-questions (Last accessed: 11 August 2022).

36. A Free And Open Indo-Pacific, 2019. Advancing a Shared Vision. URL: https://www.state.gov/wp-content/uploads/2019/11/Free-and-Open-Indo-Pacific-4Nov2019.pdf (Last accessed: 31 August 2022).

37. Alberts, D.S., Garstka, J.J., Stein, F.P., 2000. Network Centric Warfare: Developing and Leveraging Information Superiority. URL: http://www.dodccrp.org/files/Alberts_NCW.pdf (Last accessed: 11 August 2022).

38. Alcântara, B.T. de., 2018. SCO and Cybersecurity: Eastern Security Vision for Cyberspace. *International Relations and Diplomacy*. October 2018, Vol. 6, No. 10, P. 549-555 URL: URL: https://www.researchgate.net/publication/330732964_SCO_and_-Cybersecurity_Eastern_Security_Vision_for_Cyberspace (Last accessed: 11 August 2022).

39. Alimov, R., 2017. *The Role of the Shanghai Cooperation Organization in Counteracting Threats to Peace and Security*. URL: https://www.un.org/en/chronicle/article/role-shanghai-cooperation-organization-counteracting-threats-peace-and-security (Last accessed: 13 August 2022).

40. Andres, R.B., 2014. Inverted-militarized-diplomacy: how states bargain with cyber weapons. *Georgetown Journal of International Affairs. International Engagement on Cyber* IV. P. 119-129.

41. Arquilla, J., Ronfeldt, D., 1993. *Cyberwar is Coming!* URL: https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf (Last accessed: 31 August 2022).

42. Arthur, Ch., 2013. Google Glass: is it a threat to our privacy? *The Guardian* 6 Mar. URL: https://www.theguardian.com/technology/2013/mar/06/google-glass-threat-to-our-privacy (Last accessed: 31 August 2022).

43. ASEAN, 2000. *E-ASEAN Framework Agreement*. URL: http://agreement.asean.org/media/download/20140119121135.pdf (Last accessed: 31 August 2022).

44. ASEAN, 2003. *The Association of Southeast Asian Nations*. Third ASEAN Telecommunications and IT Ministers Meeting. The Singapore Declaration. An Action Agenda. URL: https://asean.org/wp-content/uploads/2012/05/III-18-2003-The-Singapore-Declaration.pdf (Last accessed: 31 August 2022).

45. ASEAN, 2016a. *ASEAN Cyber Capacity Programme* (ACCP). URL: https://cybilportal.org/projects/asean-cyber-capacity-programme-accp/ (Last accessed: 31 August 2022).

46. ASEAN, 2016b. *Establishment of the ADMM-Plus Experts' Working Group On Cyber Security*. URL: https://admm.asean.org/dmdocuments/Concept%20Paper%20on%20Establishment%20of%20EWG%20on%20Cyber%20Security,%20Final,%20as%20adopted%20by%20the%2010th%20ADMM.pdf (Last accessed: 31 August 2022).

47. ASEAN, 2016c. *Opening speech by Dr. Yaacob Ibrahim, Minister for Communications and Information*, Minister-in-charge of Cybersecurity. URL: https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2016/10/the-asean-ministerial-conference-on-cybersecurity (Last accessed: 13 August 2022).

48. ASEAN, 2017a. *About the ASEAN Defence Ministers' Meeting* (ADMM). URL: https://admm.asean.org/index.php/about-admm/about-admm.html (Last accessed: 31 August 2022).

49. ASEAN, 2017b. *About the ASEAN Defence Ministers' Meeting Plus* (ADMM-Plus). URL: https://admm.asean.org/index.php/about-admm/about-admm-plus.html (Last accessed: 31 August 2022).

50. ASEAN, 2017b. *Opening Speech by Dr Yaacob Ibrahim, Minister for Communications and Information and Minister-In-Charge of Cyber Security*, at the Asean Ministerial Conference on Cybersecurity.URL: https://s3.amazonaws.com/ceipfiles/-pdf/CyberNorms/Multilateral/2nd-AMCC-Chairmans-Statement-cleared.pdf (Last accessed: 31 August 2022).

51. ASEAN, 2018a. *ASEAN Leaders' Statement on Cybersecurity Cooperation*. URL: http://setnas-asean.id/site/uploads/document/document/5b04cdc25d192-asean-leaders-statement-on-cybersecurity-cooperation.pdf (Last accessed: 31 August 2022).

52. ASEAN, 2018b. *ASEAN Member States Agree to Strengthen Cyber Coordination and Capacity-Building Efforts*. URL: https://www.csa.gov.sg/news/press-releases/amcc-2018 (Last accessed: 12 August 2022).

53. ASEAN, 2018c. *Chairman's Statement of The 3rd ASEAN Ministerial Conference On Cybersecurity, Singapore, 19 September 2018*. URL:

https://asean.org/asean2020/wp-content/uploads/2021/01/AMCC-2018-Chairmans-Statement-Finalised.pdf (Last accessed: 31 August 2022).

54. ASEAN, 2020. *ASEAN Cyberthreat Assessment 2020*. Key Insights From The ASEAN Cybercrime Operations Desk. URL: https://www.interpol.int/content/download/-14922/file/ASEAN_CyberThreatAssessment_2020.pdf [Accessed 31 August 2022].

55. ASEAN, 2021. *ASEAN Digital Master plan 2025*. URL:: https://asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf. (Last accessed: 31 August 2022).

56. ASEAN, 2021b. *ASEAN documents on Combating Traysnational Crime and Terrorism*. A Compilation of ASEAN Declarations, Joint Declarations, and Statements on Combating Transnational Crime and Terrorism. URL: https://asean.org/wp-content/uploads/2021/01/ASEAN-Documents-on-Combating-Transnational-Crime-and-Terrorism-1.pdf (Last accessed: 31 August 2022).

57. Asia Society Policy Institute, 2017. *Preserving the Long Peace in Asiaю The Institutional Building Blocks of Long-Term Regional Security*. URL: https://asiasociety.org/files/uploads/191files/LongPeaceAsia_onlinevers.pdf (Last accessed: 12 August 2022).

58. Bagga, R., 2018. *The National Cyber Security Policy Of India 2013: An Analytical Study*. URL: https://ir.nbu.ac.in/bitstream/123456789/2985/1/March_2018_14.pdf (Last accessed: 31 August 2022).

59. Banerjee, C., 2022. India 6th most targeted by Chinese. *The Times of India*. 22 Jun. URL: https://timesofindia.indiatimes.com/india/india-6th-most-targeted-by-chinese-hackers-since-2016/articleshow/76503656.cms (Last accessed: 31 August 2022).

60. Barrinha, A., Renard, T., 2020. *The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace, Council on Foreign Relations*. URL: https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace/ (Last accessed: 12 August 2022).

61. Bartlett, B., 2019. *How Japanese Cybersecurity Policy Changes. Harvard Program on U.S.-Japan Relations.* Occasional Paper Series. URL:

https://programs.wcfia.harvard.edu/files/us-japan/files/19-01_bartlett.pdf (Last accessed: 31 August 2022).

62. Berkowitz, B., 2007. *The New Face of War: How War Will Be Fought in the 21st Century*. New York: Free Press.

63. Berry, V., 2022. *How India aims to protect key infrastructure amid rise in cyber attacks from across the border*. URL: https://www.wionews.com/india-news/how-india-aims-to-protect-key-infrastructure-amid-rise-in-cyber-attacks-from-across-the-border-496789 (Last accessed: 31 August 2022).

64. Bhattacharjee, S., 2022. India's Delayed Cyber Security Policy. *South Asian Voices.* 27 July. URL: https://southasianvoices.org/indias-delayed-cyber-security-policy/ (Last accessed: 11 August 2022).

65. Biden expands US investment ban on Chinese firms. *BBC News*. 3 Jun. URL: https://www.bbc.com/news/business-57334265 [Accessed 31 August 2022].

66. Bischoff, P., 2021. *Which countries have the worst (and best) cybersecurity?* URL:https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/ (Last accessed: 11 August 2022).

67. Borger, J., 1999 Pentagon kept the lid on cyberwar in Kosovo *The Guardian*. Tue 9 Nov. URL: https://www.theguardian.com/world/1999/nov/09/balkans (Last accessed: 31 August 2022).

68. Borghard, E.D. and Schneider, J., 2019. Israel responded to a Hamas cyberattack with an airstrike. That's not such a big deal. Policymakers are debating how best to retaliate against cyberwarfare actions — and how not to. *Washington Post*. 9 May. URL: https://www. washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cybera (Last accessed: 11 August 2022).

69. Bunker, R.J and Moore T.L., 1996. Nonlethal Technology and Fourth Epoch War: A New Paradigm of Politico-Military Force. *Land Warfare Paper*.No. 23. URL: https://scholarship.claremont.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1491&context=cgu_fac_pub (Last accessed: 11 August 2022).

70. Bunker, R.J., 1996. Generations, Waves, and Epochs: Modes of Warfare and the RPMA. *Airpower Journal* 10.1. URL: https://core.ac.uk/download/pdf/70975273.pdf (Last accessed: 31 August 2022).

71. Burgers, T., Farber, D.J., 2021. China's Dangerous Step Toward Cyber Conflict. China is changing the cyber game in East-Asia – and increasing the potential for conflict across the Indo-Pacific. *The Diplomat*. 12 Mar. URL: https://thediplomat.com/2021/03/chinas-dangerous-step-toward-cyber-war/ (Last accessed: 31 August 2022).

72. Callejas, J.F., Afifi, A. and Lozinskiy, N., 2021. *Cybersecurity in the United Nations system organizations.* Report of the Joint Inspection Unit, United Nations. URL: https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf (Last accessed: 31 August 2022).

73. CCDCOE, 2014. *Information Security Discussed at the Dushanbe Summit of the Shanghai Cooperation Organisation*. URL: https://ccdcoe.org/incyderarticles/information-security-discussed-at-the-dushanbe-summit-of-the-shanghai-cooperation-organisation/ (Last accessed: 31 August 2022).

74. CCDCOE, 2018. *Shanghai Cooperation Organisation*. URL: https://ccdcoe.org/organisations/sco/ (Last accessed: 31 August 2022).

75. CCDCOE, 2021. Štrucl, D. *Comparative study on the cyber defence of NATO Member States*. URL: https://www.ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf (Last accessed: 31 August 2022).

76. Cebrowski, A.K., Garstka, J.J., 1998. *Network-Centric Warfare: Its Origin and Future.* URL: http://all.net/books/iw/iwarstuff/www.usni.org/Proceedings/Articles98-/PROcebrowski.htm (Last accessed: 12 August 2022).

77. Chen, S., 2017. Chinese Satellite Relays a Quantum Signal Between Cities. *WIRED* 15 Jun. URL: https://www.wired.com/story/chinese-satellite-relays-a-quantum-signal-between-cities/ (Last accessed: 31 August 2022).

78. Chinese hackers may have stolen government info: Experts. *The Times of India*.. 9 Jun. URL: https://timesofindia.indiatimes.com/city/hyderabad/chinese-hackers-may-

have-stolen-government-info-experts/articleshowprint/52664132.cms (Last accessed: 31 August 2022).

79. Choudhury, A.R., 2021. What the world can learn from ASEAN's cyber cooperation. *GovInsider*. 15 Nov URL: https://govinsider.asia/resilience/what-the-world-can-learn-from-aseans-cyber-cooperation-amit-roy-choudhury/ (Last accessed: 31 August 2022).

80. Cobaleda, A.S., Kouliopoulos, A., Kissack, R., Bradley, M., Sánchez, D.B., 2020. *Mapping of Global Security Threats and the Global Security Architecture*. URL: https://www.globe-project.eu/mapping-of-global-security-threats-and-the-global-security-architecture_9861.pdf (Last accessed: 31 August 2022).

81. Creveld M.V., 1991. *The Transformation of War*. New York : Free Press

82. CSIS Commission on smart power, 2007. *A smarter, more secure America.* eds. R. L. Armitage, J. S. Nye URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/071106_csissmartpowerreport.pdf (Last accessed: 31 August 2022).

83. Cybersecurity Exposure Index, 2020. URL: https://10guards.com/ru/articles/-global-cybersecurity-exposure-index-2020/ (Last accessed: 31 August 2022).

84. Daase, Ch., Christopher, G., Dalnoki-Veress, F., Pomper, M., and Shaw, R., 2019 WMD Capabilities Enabled by Additive Manufacturing. *NDS Report Negotiation Design and Strategy.* URL: https://www.nonproliferation.org/wp-content/uploads/2019/09/NDS_Report_1908_WMD_AM_2019.pdf (Last accessed: 31 August 2022).

85. Data Security Council of India, 2013. Analysis of National Cyber Security Policy (NCSP – 2013). URL: https://www.dsci.in/sites/default/files/NCSP_2013_DSCI_-Analysis_v1.0.pdf (Last accessed: 12 August 2022).

86. David, E., 2021. Sanger and Emily Schmall. China Appears to Warn India: Push Too Hard and the Lights Could Go Out. *The New York Times.* 28 Feb. URL: https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html (Last accessed: 31 August 2022).

87. Demchak, C.C., 2018 Three Futures for a Post-Western Cybered World *Military Cyber Affairs*. Volume 3 Issue 1 Article 6. URL: https://scholarcommons.usf.edu/mca/vol3/iss1/6 (Last accessed: 31 August 2022).

88. Demchak, C.C., Dombrowski, P., 2011. Rise of a Cybered Westphalian Age. *Strategic Studies Quarterly*. Spring. URL: https://www.hsdl.org/?view&did=744113 (Last accessed: 15 August 2022).

89. Demchak, C.C., Dombrowski, P., 2014. Cyber Westphalia Asserting State Prerogatives in Cyberspace Georgetown *Journal of International Affairs*. URL: <https://www.academia.edu/33200124/Cyber_Westphalia_Asserting_State_Prerogatives_in_ Cyberspace (Last accessed: 31 August 2022).

90. Department of Defense, 1999. An Assessment of International Legal Issues in Information Operations. URL: https://fas.org/irp/eprint/io-legal.pdf, P.9-10 (Last accessed: 15 August 2022).

91. Department of Defense, 2012. *Autonomy in Weapon Systems*. Directive. number 3000.09. URL: https://www.hsdl.org/?view&did=726163 [Accessed 31 August 2022].

92. Digital 2021: Global Overview Report, 2021. URL: https://datareportal.com/reports/digital-2021-global-overview-report (Last accessed: 31 August 2022).

93. Digital 2021: India. URL: https://datareportal.com/reports/digital-2021-india?rq=India%202021 (Last accessed: 31 August 2022).

94. Digital 2022: India. [online]. Available at: < https://datareportal.com/reports/digital-2022-india > (Last accessed: 31 August 2022).

95. Digital 2022: Japan. URL: https://datareportal.com/reports/digital-2022-japan (Last accessed: 15 August 2022).

96. Doffman, Z., 2019. *Israel Responds To Cyber Attack With Air Strike On Cyber Attackers In World First Forbes*. 6 May. URL: https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/?sh=13e3d498afb5 [Accessed 31 August 2022].

97. Dreifus, C., Walsh, T., 2019. A.I. Expert, Is Racing to Stop the Killer Robots. *The New York Times* 30 Jul. URL: https://www.nytimes.com/2019/07/30/-

science/autonomous-weapons-artificial-intelligence.html?auth=link-dismiss-google1tap (Last accessed: 31 August 2022).

98. Drones: What are they and how do they work? 2012 *BBC News*. 31 Jan. URL: https://www.bbc.com/news/world-south-asia-10713898 (Last accessed: 31 August 2022).

99. Dunlap, C., 2021. *J.D.International law and cyber ops: Q & A with Mike Schmitt about the status of Tallinn 3.0*. URL: https://sites.duke.edu/lawfire/2021/10/03/-international-law-and-cyber-ops-q-a-with-mike-schmitt-about-the-status-of-tallinn-3-0/ (Last accessed: 22 August 2022).

100. Echevarria, A.J., 2005. *Fourth-generation war and other myths* URL: https://www.files.ethz.ch/isn/22592/Fourth%20Generation%20War%20and%20Other%20Myths.pdf (Last accessed: 31 August 2022).

101. European Commission, 2020. *Changing security paradigm.* URL: https://knowledge4policy.ec.europa.eu/changing-security-paradigm_en (Last accessed: 22 August 2022).

102. Exclusive: Who are 'Mallu Cyber Soldiers' that hacked Pakistan websites, 2022. *International Business Times*. 23 Aug. URL: https://www.ibtimes.co.in/exclusive-who-are-mallu-cyber-soldiers-that-hacked-pakistan-websites-648366 (Last accessed: 31 August 2022).

103. Fazzini, K., 2019. In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides. *CNBC*. 27 Feb. URL: https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html (Last accessed: 31 August 2022).

104. Fedasiuk, R., Weinstein, E., Puglisi, A., 2021. *China's Foreign Technology Wish List*. URL: https://cset.georgetown.edu/publication/chinas-foreign-technology-wish-list/ (Last accessed: 22 August 2022).

105. Fernandez, E., 2019. Soon, People May Be Able To Use 3D Printers To Build Weapons Of Mass Destruction. *Forbes* 17 Sep. URL: https://www.forbes.com/sites/fernandezelizabeth/2019/09/17/soon-people-may-be-able-to-use-3d-printers-to-build-weapons-of-mass-destruction/?sh=12dfb0ee6c92 (Last accessed: 31 August 2022).

106. Floridi, L., 2020. *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*. URL: https://link.springer.com/article/10.1007/s13347-020-00423-6 (Last accessed: 31 August 2022).

107. Fogg, I., 2021. Benchmarking the global 5G experience. *Opensignal*. 03 Feb. URL: https://www.opensignal.com/2021/02/03/benchmarking-the-global-5g-experience (Last accessed: 13 August 2022).

108. Frisby, J.,2020. *Cybersecurity Exposure Index (CEI)* 2020. URL: https://passwordmanagers.co/cybersecurity-exposure-index/#asia-pacific (Last accessed: 31 August 2022).

109. Frolova, O., Kuchmii, O., 2021. Public-private partnership in the sphere of cybersecurity as an important factor of european stability. *Міжнародні та політичні дослідження*. Одеса: Одеський національний університет імені І. І. Мечникова, Вип. 34. С. 194-211.

110. Ghosh, S., 2021. India's National Cybersecurity Strategy Awaiting Approval. *Bank Info Security.* 1 Nov. URL: https://www.bankinfosecurity.in/indias-national-cybersecurity-strategy-awaiting-approval-a-17829 (Last accessed: 31 August 2022).

111. Goldman, E.O., 2021. *Fresh thinking and new approaches are needed on diplomacy's newest frontier.* URL: https://afsa.org/cyber-diplomacy-strategic-competition (Last accessed: 22 August 2022).

112. Gomez, M.A.N. (2016) Arming Cyberspace: The Militarization of a Virtual Domain *Global Security and Intelligence Studies*. Vol. 1: No. 2, Article 5. URL: https://www.ibei.org/arming-cyberspace-the-militarization-of-a-virtual-domain_54871.pdf (Last accessed: 12 August 2022).

113. Groll, E., Seligman, L., 2019. Trump Weighs Cyberattack on Iran. But Pentagon planners caution such a strike could prompt damaging retaliation *Foreign Policy.* 23 Sep. URL: https://foreignpolicy.com/2019/09/23/security-brief-trump-weighs-cyberattack-on-iran/ (Last accessed: 31 August 2022).

114. Hammes, T.X., 2007. War evolves into the fourth generation. *Military Review.* May-June. URL: https://www.hsdl.org/?view&did=482199 (Last accessed: 15 August 2022).

115. Hathaway, 2016 Melissa Hathaway Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri Japan Cyber Readiness At A Glance September 2016. URL: https://www.potomacinstitute.org/images/CRI/CRI_Japan_Profile_PIPS.pdf (Last accessed: 31 August 2022).

116. Government of Japan, 2016. General Framework for Secured IoT Systems. URL: https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf (Last accessed: 18 August 2022).

117. Hein, M., Yurin, V., 2010. Stuxnet - Ein Computerwurm attackiert Netze weltweit – Produziert. *Deutsche Welle.* 04 Oct. URL: https://www.dw.com/ru/stuxnet-ein-computerwurm-attackiert-netze-weltweit/audio-6087814 (Last accessed: 31 August 2022).

118. Hein, M.V, 2011. Wurm-Alarm. *Deutsche Welle.* URL: https://learngerman.dw.com/de/stuxnet-20-bereits-platziert/a-15255673# (Last accessed: 18 August 2022).

119. Hoffman, F.G., 2009. Hybrid Warfare and Challenges. Issue 52, 1st quarter. URL: https://smallwarsjournal.com/documents/jfqhoffman.pdf (Last accessed: 31 August 2022).

120. Holst, A., 2019a. *Smartphone penetration rate by country 2019*. URL: https://www.statista.com/statistics/539395/smartphone-penetration-worldwide-by-country/ (Last accessed: 31 August 2022).

121. Holst, A., 2019b. *Smartphone users by country worldwide 2019*. URL: https://www.statista.com/statistics/748053/worldwide-top-countries-smartphone-users/ (Last accessed: 18 August 2022).

122. Ichihara, M., 2020. Is Japan Immune From China's Media Influence Operations? Efforts to boost pro-China narratives in Japan haven't received much attention – but that doesn't mean they don't exist. *The Diplomat*. 19 Dec. URL: https://thediplomat.com/2020/12/is-japan-immune-from-chinas-media-influence-operations/ (Last accessed: 31 August 2022).

123. India: Opportunity & Role in the 4th Industrial Revolution. *DG'S JOURNAL*. 17 Jan. URL: https://www.ciiblog.in/india-opportunity-role-in-the-4th-industrial-revolution/ (Last accessed: 31 August 2022).

124. Indo-Pacific Defense Forum, 2019. *ASEAN ministers stress cooperation to reduce cyber threats*. URL: https://ipdefenseforum.com/2019/11/asean-ministers-stress-cooperation-to-reduce-cyber-threats/ (Last accessed: 15 August 2022).

125. Information Security Policy Council, 2006. *The First National Strategy on Information Security « Toward the realization of a trustworthy society»*. URL: https://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf (Last accessed: 31 August 2022).

126. Information Security Policy Council, 2009. *The Second National Strategy on Information Security « Aiming for Strong « Individual» and « Society» in IT Age»*. URL: https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf (Last accessed: 31 August 2022).

127. Internet world stats, 2019. *Top 20 countries with the highest number of internet users.* URL: https://www.internetworldstats.com/top20.htm (Last accessed: 18 August 2022).

128. ITU, 2010. *Definitions and terminology relating to building confidence and security in the use of information and communication technologies*. Resolution 181. URL: https://www.itu.int/en/council/Documents/basic-texts/RES-181-E.pdf (Last accessed: 31 August 2022).

129. ITU, 2017. *Global Cybersecurity Index-2017.* URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (Last accessed: 22 August 2022).

130. ITU, 2020. *Global Cybersecurity Index. 2020.* URL: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E/ (Last accessed: 31 August 2022).

131. Jain, M., 2019. *The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment*. URL: https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/ (Last accessed: 31 August 2022).

132. Jain, T., 2015. *Cyber Security Policy Of India 2015 Must Be Formulated.* URL: https://www.linkedin.com/pulse/cyber-security-policy-india-2015-must-formulated-tushar-jain/ (Last accessed: 31 August 2022).

133. Kato, M., 2019. Japan steps up deployment of defense AI and robots. *Nikkei Asia*. 27 Jan. URL: https://asia.nikkei.com/Politics/Japan-steps-up-deployment-of-defense-AI-and-robots (Last accessed: 11 August 2022).

134. Kim, G., Lee, H., Lee, B., Lee, J., Son, W., 2021. *Fourth Industrial Revolution in Japan: Technology to Address Social Challenges.* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3815376) (Last accessed: 31 August 2022).

135. Klimburg, A., 2013. *Cyberpower and National Cyber Security in International Relations.* URL: URL: https://watson.brown.edu/events/2013/alexander-klimburg-cyberpower-and-national-cyber-security-international-relations/2013 (Last accessed: 31 August 2022).

136. Klimburg, A., Tirmaa-Klaar, H., 2011. *Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU.* URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf (Last accessed: 15 August 2022).

137. Koh, D., 2020. The Geopolitics of Cybersecurity. *The Diplomat.* 09 Dec. URL: https://thediplomat.com/2020/12/the-geopolitics-of-cybersecurity/ (Last accessed: 31 August 2022).

138. Kuchmii O., Frolova O., 2018. International humanitarian cooperation within the framework of hybrid threats for the international security system. *Evropský politický a právní diskurz*, Volume 5, Issue 5, Praha: BEROSTAV DRUŽSTVO. P. 6-13.

139. Libicki, M.C., 2009. *Cyberdeterrence and Cyberwar*. URL: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (Last accessed: 31 August 2022).

140. Libicki, M.C., 2012. *Cyberspace Is Not a Warfighting Domain.* URL: https://kb.osu.edu/bitstream/handle/1811/73111/ISJLP_V8N2_321.pdf?sequence=1&isAllowed=y (Last accessed: 31 August 2022).

141. Libicki, M.C., 1995. *What is information warfare.* URL: https://apps.dtic.mil/sti/pdfs/ADA367662.pdf (Last accessed: 11 August 2022).

142. Lind, W.S., 2004. *Understanding Fourth Generation War.* URL: https://original.antiwar.com/lind/2004/01/15/understanding-fourth-generation-war/ (Last accessed: 31 August 2022).

143. Looking Into The Future: Is Digital India The 'Next Big Thing'? 2021. *The Scalers*. URL: https://thescalers.com/looking-into-the-future-is-digital-india-the-next-big-thing/ (Last accessed: 31 August 2022).

144. Lung, N., 2018. *ASEAN leaders issue statement on cybersecurity cooperation*. URL: https://opengovasia.com/asean-leaders-issue-statement-on-cybersecurity-cooperation/ (Last accessed: 31 August 2022).

145. Manantan, M. B. F., 2021. Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Institute of International Affairs*. 10 Nov. URL: https://www.internationalaffairs.org.au/australianoutlook/defining-cyber-diplomacy/ (Last accessed: 11 August 2022).

146. Marcus, J., 2019 Analysis. Saudi oil attacks: Drones and missiles launched from Iran – US *BBC News*. 17 Sep. URL: https://www.bbc.com/news/world-middle-east-49733558 (Last accessed: 31 August 2022).

147. Matsubara, M., 2013. Japan's New Cybersecurity Mission. *The Diplomat*. 02 Aug. URL: https://thediplomat.com/2013/08/japans-new-cybersecurity-mission/ (Last accessed: 18 August 2022).

148. Matsubara, M., Mochinaga, D., 2021. Japan's Cybersecurity Strategy: From the Olympics to the Indo-Pacific. *Asie.Visions.* No. 119, February. URL: https://www.ifri.org/en/publications/notes-de-lifri/asie-visions/japans-cybersecurity-strategy-olympics-indo-pacific (Last accessed: 31 August 2022).

149. McKune, S., 2015. *An Analysis of the International Code of Conduct for Information Security. Will the SCO states' efforts to address «territorial disputes» in cyberspace determine the future of international human rights law?* URL: https://citizenlab.ca/2015/09/international-code-of-conduct/ (Last accessed: 31 August 2022).

150. Ministry of Electronics & Information Technology, Government of India, 2013. *National Cyber Security Policy-2013.* URL: https://meity.gov.in/writereaddata/-files/downloads/National_cyber_security_policy-2013%281%29.pdf (Last accessed: 31 August 2022).

151. Ministry of External Affairs. Government of India, 2021. Dushanbe Declaration on the Twentieth Anniversary of the Shanghai Cooperation Organisation (September 17, 2021). URL: https://mea.gov.in/bilateral_documents.htm?dtl/34275/Dushanbe_Declaration_on_the_-Twentieth_Anniversary_of_the_Shanghai_Cooperation_Organisation (Last accessed: 22 August 2022).

152. Ministry of Foreign Affairs of the People's Republic of China, 2020. *Statement of the Council of Heads of State of the Shanghai Cooperation Organisation on cooperation in the field of ensuring international information security*. URL: https://www.fmprc.gov.cn/rus/wjdt/gb/202011/t20201110_858237.html (Last accessed: 31 August 2022).

153. Ministry of Law And Justice, 2008. *The Information Technology Act (Amendment)*. URL: https://meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf (Last accessed: 11 August 2022).

154. Ministry of Law, Justice and Company Affairs (Legislative Department), 2000. *The Information Technology Act*. URL: https://meity.gov.in/writereaddata/files/itbill2000.pdf (Last accessed: 31 August 2022).

155. Moody R., 2019. *Which countries have the worst (and best) cybersecurity*? URL: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/ (Last accessed: 31 August 2022).

156. Muratbekova, A., 2019. Exploring the Shanghai Cooperation Organisation's Identity Crisis: What is Next? *International Organisations Research Journal*. Vol. 14. No 4. URL: https://www.academia.edu/42833730/Exploring_the_Shanghai_Cooperation_Organisation_s_Identity_Crisis_What_is_Next (Last accessed: 31 August 2022).

157. Mustafa, G., Murtaza, Z., Murtaza, K., 2020 Cyber Warfare Between Pakistan and India: Implications for the Region. *Pakistan Languages and Humanities Review*. Vol. 4, No. 1. URL: https://www.researchgate.net/publication/347409992_Cyber_Warfare

_Between_Pakistan_and_India_Implications_for_the_Region (Last accessed: 31 August 2022).

158. National Cyber Security Strategy, 2022. URL: https://www.drishtiias.com/daily-updates/daily-news-analysis/national-cyber-security-strategy-1 (Last accessed: 11 August 2022).

159. National Defense Strategy of United States of America, 2018. URL: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (Last accessed: 31 August 2022).

160. Nitta, Y., 2014. Review of the Japan Cybersecurity Strategy September 2014. *ISPSW Strategy Series: Focus on Defense and International Security.* URL: https://www.files.ethz.ch/isn/183668/290_Nitta.pdf (Last accessed: 31 August 2022).

161. Nye, J.S., 1990. *Bound to Lead: The Changing Nature of American Power.* New York: Basic Books .

162. Nye, J.S., 2002. *The Paradox of American Power.* New York: Oxford University Press.

163. Nye, J.S., 2004. *Soft Power.* New York: Public Affairs.

164. Nye, J.S., 2008. *The Powers to Lead*. New York: Oxford University Press.

165. Nye, J.S., 2010. Cyber Power. URL: https://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf (Last accessed: 31 August 2022).

166. Nye, J.S., 2011. *The Future of Power.* New York: PublicAffairs.

167. Nye, J.S., Owens, W.A., 1996. America's Information Edge. *Foreign Affairs.* Vol. 75, No. 2. URL: https://www.foreignaffairs.com/articles/united-states/1996-03-01/americas-information-edge (Last accessed: 21 August 2022).

168. OSCE, 2020. Duffy, H., Greene, A. *Note on the Shanghai Convention on combating terrorism, separatism and extremism Warsaw* (21 September 2020). URL: https://www.osce.org/files/f/documents/e/8/467697.pdf (Last accessed: 31 August 2022).

169. Parmar, S.D., 2018 *Cybersecurity in India: An Evolving Concern for National Security* (Central University of Gujarat). URL:

https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf (Last accessed: 31 August 2022).

170. Patil, K., 2022. *Quad and Cybersecurity*. URL: https://idsa.in/idsacomments/quad-and-cybersecurity-kpatil-220622 (Last accessed: 31 August 2022).

171. Patil, S., Bhan, A., 2022. *Cyber Attacks. Pakistan emerges as China's proxy against India*. URL: https://www-orfonline-org.translate.goog/research/pakistan-emerges-as-chinas-proxy-against-india/?_x_tr_sl=en&_x_tr_tl=uk&_x_tr_hl=ru&_x_tr_pto=op, wapp (Last accessed: 21 August 2022).

172. Putra, N.A., 2018. Is ASEAN Doing Enough to Address Cybersecurity Risks? *The Diplomat*. 06 Mar. URL: https://thediplomat.com/2018/03/is-asean-doing-enough-to-address-cybersecurity-risks/ [Accessed 31 August 2022].

173. Quad Cybersecurity Partnership: Joint Principles. URL: https://www.mofa.go.jp/files/100347801.pdf (Last accessed: 31 August 2022).

174. Rajagopalan, R.P., 2022. The Growing Tech Focus of the Quad. *Observer Research Foundation*. 09 Jul. URL: https://www.orfonline.org/research/the-growing-tech-focus-of-the-quad/ (Last accessed: 11 August 2022).

175. Raman, S., Sharma, N., 2019. Cyber Terrorism in India: A Physical Reality Orvirtual Myth. *Indian Journal of Law and Human Behavior*. Volume 5 Number 2 (Special Issue). URL: https://journals.indexcopernicus.com/api/file/viewByFileId/783266.pdf (Last accessed: 31 August 2022).

176. RAND Corporation, 2017. Paoli, G.P., Aldridge, J., Ryan, N., Warnes, R., 2017. *Behind the curtain. The illicit trade of firearms, explosives and ammunition on the dark web.* Published by the RAND Corporation, Santa Monica, Calif., and Cambridge URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2091/RAND_RR2091.pdf> (Last accessed: 18 August 2022).

177. Ratner, E., Kliman, D. Blume, S.V., Rush, D. and others, 2020. *Rising to the China Challenge. Renewing American Competitiveness in the Indo-Pacific*. URL: https://www.cnas.org/publications/reports/rising-to-the-china-challenge (Last accessed: 31 August 2022).

178. Rattray, G.J., 2017. *An Environmental Approach to Understanding Cyberpower*. URL: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-10.pdf?ver=2017-06-16-115053-850 (Last accessed: 15 August 2022).

179. Relia, S., 2021. India's tryst with a New National Cyber Security Policy: Here's what we need. *Financial Express*. 4 August. URL: https://www.financialexpress.com/defence/indias-tryst-with-a-new-national-cyber-security-policy-heres-what-we-need/2304053/ (Last accessed: 31 August 2022).

180. Rijksdienst voor Ondernemend Nederland, 2018. *Cyber Security in India. Opportunities for Dutch companies*. URL: https://www.thehaguesecuritydelta.com/media/com_hsd/report/218/document/Cyber-Security-in-India.pdf (Last accessed: 31 August 2022).

181. Riordan, S., 2019. Cyberdiplomacy: Managing Security and Governance Online. Cfmbridge: Polity Press.

182. Rõigas, H., 2015. *An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?*. URL: https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/ (Last accessed: 21 August 2022).

183. Rose, G., Nestorovska, D., 2005 Towards An ASEAN Counter-Terrorism Treaty. *Singapore Year Book of International Law and Contributors*. URL: http://www.commonlii.org/sg/journals/SGYrBkIntLaw/2005/13.pdf (Last accessed: 31 August 2022).

184. Saran, S., Deo, A., 2020. *« Pax Sinica: Implications for the Indian Dawn»* . URL: https://www.weforum.org/agenda/2020/01/pax-sinica-an-extract/ (Last accessed: 31 August 2022).

185. SCO, 2006. *Statement of Heads of SCO Member States on International Information Security* (Shanghai, 15 June 2006). URL: https://www.iri.edu.ar/publicaciones_iri/anuario/CD%20Anuario%202007/Asia/SCO%20-%20statement%20of%20heads%20of%20SCO%20member%20states%20on%20internat.pdf (Last accessed: 31 August 2022).

186. SCO, 2009. *Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security*. URL: https://ccdcoe.org/uploads/2018/10/SCO-090616-IISAgreement.pdf (Last accessed: 31 August 2022).

187. SCO, 2013. *Bishkek Declaration By the Heads of the Member States of the Shanghai Cooperation Organization* (September 13, 2013). URL: http://eng.sectsco.org/load/199687/ (Last accessed: 12 August 2022).

188. SCO, 2014. *SCO Development Strategy of The Shanghai Cooperation Organization* Until 2025. URL: https://policy.asiapacificenergy.org/sites/default/files/Development%20Strategy%20of%20the%20Shanghai%20Cooperation%20Organization%20until%202025%20%28EN%29.pdf (Last accessed: 31 August 2022).

189. SCO, 2017. *The Astana declarationof the Heads of State of the Shanghai Cooperation Organisation*. URL: http://eng.sectsco.org/load/297146/ (Last accessed: 31 August 2022).

190. SCO, 2018. *Press release on the outcome of the 13th meeting of the SCO National Security Council Secretaries*. URL: http://eng.sectsco.org/news/20180522/431989.html (Last accessed: 31 August 2022).

191. SCO, 2020. *The Moscow Declaration of the Council of Heads of State of the Shanghai Cooperation Organisation.* URL: http://eng.sectsco.org/news/20201110/690356.html (Last accessed: 12 August 2022).

192. Secretary of Defense Esper Tells U.S. Naval War College Students His Focus is Great-Power Competition, 2019. URL: https://usnwc.edu/News-and-Events/News/Secretary-of-Defense-Esper-Tells-US-Naval-War-College-Students-His-Focus-is-Great-Power-Competition?mod=article_inline (Last accessed: 31 August 2022).

193. Sherman, J., 2020. Is the U.S. Winning Its Campaign Against Huawei? *Lawfare*, Wednesday. 12 Aug. URL: https://www.lawfareblog.com/us-winning-its-campaign-against-huawei (Last accessed: 31 August 2022).

194. Siabro Anastasiia, 2021. The influence of scientific and technological development on the transformation of the global security paradigm. «*Evropský politický a právní diskurz» («European political and law discourse»).* 2021. Vol. 8 Iss. 5. P. 6-13.

195. Singapore Government Agency, 2019. *Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019* (02 Oct 2019). URL: https://www.csa.gov.sg/News/Speeches/Asean-Ministerial-Conference-on-Cybersecurity-2019 (Last accessed: 15 August 2022).

196. Singapore Government Agency, 2020. *Opening Speech by Mr S Iswaran, Minister for Communications and Information, Minister-in-Charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2020* (07 Oct 2020). URL: https://www.csa.gov.sg/News/Speeches/asean-ministerial-conference-on-cybersecurity-2020 (Last accessed: 31 August 2022).

197. Singapore Ministry for Communications and Information, 2021a. *Information, at ASEAN Ministerial Conference on Cybersecurity on 6 October 2021.* URL: https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/10/keynote-address-by-mrs-josephine-teo-at-asean-ministerial-conference-on-cybersecurity (Last accessed: 31 August 2022).

198. Singapore Ministry for Communications and Information, 2021b. *Keynote Address by Mrs Josephine Teo, Minister for Communications and Information, at ASEAN Ministerial Conference on Cybersecurity on 6 October 2021.* URL: https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/10/keynote-address-by-mrs-josephine-teo-at-asean-ministerial-conference-on-cybersecurity (Last accessed: 21 August 2022).

199. Singh, S., 2019. *India's National Cyber Security Policy: Gaps And The Way Forward*. URL: https://www.researchgate.net/publication/351686813_INDIA%27S_NATIONAL_CYBER_SECURITY_POLICY_GAPS_AND_THE_WAY_FORWARD (Last accessed: 31 August 2022).

200. Smith, E.A., 2002. *Effects Based Operations Applying Network Centric Warfare in Peace, Crisis, and War.* URL: http://www.dodccrp.org/files/Smith_EBO.pdf (Last accessed: 31 August 2022).

201. Starr, S.H., 2017. *Toward a Preliminary Theory of Cyberpower*. URL:https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/-Cyberpower-I-Chap-03.pdf?ver=2017-06-16-115054-677 (Last accessed: 31 August 2022).

202. Stein, G., 1995. Information Warfare. *Airpower Journal*. URL: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf (Last accessed: 31 August 2022).

203. Subex, 2019. *A cyber-attack on an Indian nuclear plant raises worrying questions.* URL: https://www.subexsecure.com/media_coverage/a-cyber-attack-on-an-indian-nuclear-plant-raises-worrying-questions/ (Last accessed: 31 August 2022).

204. Szafranski, R., 1995. A theory of information warfare. Preparing for 2020. *Airpower Journal.* URL: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-09_Issue-1-Se/1995_Vol9_No1.pdf (Last accessed: 21 August 2022).

205. Talmazan, Y., Arouzi, A., Arkin, D. and Smith, S. Pompeo calls Saudi oil field attack an 'act of war'. *NBC News.* Sept. 18 URL: https://www.nbcnews.com/news/world/pompeo-heads-saudi-arabia-middle-east-tensions-grow-n1055206 (Last accessed: 17 August 2022).

206. The countries of the QUAD four will start cooperating in the cybersphere. *Time News*. 25 Sep. URL: https://time.news/the-countries-of-the-quad-four-will-start-cooperating-in-the-cybersphere-news-news/ (Last accessed: 31 August 2022).

207. The Government of Japan, 2013. *National Security Strategy* (December 17). URL: https://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf (Last accessed: 31 August 2022).

208. The Government of Japan, 2015. *Cybersecurity Strategy* (September 4,). URL: https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf (Last accessed: 31 August 2022).

209. The Government of Japan, 2018. *Cybersecurity Strategy.* URL: https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf (Last accessed: 31 August 2022).

210. The Government of Japan, 2021. *Cybersecurity Strategy*. URL: <https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf (Last accessed: 17 August 2022).

211. The Government of India, 2015. Approach and Key Components of e-Kranti: National e-Governance Plan 2.0. Press Information Bureau. URL: https://pib.gov.in/newsite/printrelease.aspx?relid=117690 (Last accessed: 31 August 2022).

212. The Network Readiness Index, 2020. *Accelerating Digital Transformation in a post-COVID Global Economy*. URL: https://networkreadinessindex.org/wp-content/uploads/2020/11/NRI-2020-V8_28-11-2020.pdf (Last accessed: 31 August 2022).

213. The White House, 2021. Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/ (Last accessed: 31 August 2022).

214. Toffler, A., Toffler, H., 1995. *War and Anti-war*. New York: Warner Books, 1995.

215. Top 14 Cybersecurity Breaches in Japan. URL: https://www.cyberlands.io/topsecuritybreachesjapan (Last accessed: 31 August 2022).

216. Top 10 Military Technology Trends & Innovations for 2022. URL: https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022/ (Last accessed: 31 August 2022).

217. UNIDIR, 2013. *The Cyber Index: International Security Trends and Realities UNIDIR*. URL: https://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (Last accessed: 31 August 2022).

218. Unique Identification Authority of India. *About Unique Identification Authority of India.* URL: https://www.uidai.gov.in/en/about-uidai/unique-identification-authority-of-india.html (Last accessed: 31 August 2022).

219. United Nations, 2020. *UN E-Government Survey-2020*. URL: https://desapublications.un.org/file/781/download (Last accessed: 31 August 2022).

220. Waghre, P. and Mehta Sh., 2019. India's National Cybersecurity Policy Must Acknowledge Modern Realities. India's National Cybersecurity Policy must bolster its global ambitions. *The Diplomat*. 20 December. URL: https://thediplomat.com/2019/12/indias-national-cybersecurity-policy-must-acknowledge-modern-realities/ (Last accessed: 21August 2022).

221. WAQAS. Pakistan-Linked Hackers Conduct Third Cyber-Espionage Campaign Against India. *Hackread*. 24 Mar. URL: https://www.hackread.com/pakistan-hackers-cyber-espionage-campaign-india-army/ (Last accessed: 31 August 2022).

222. WIPO, 2019. *Global innovation index* 2019. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2019.pdf (Last accessed: 31 August 2022).

223. WIPO, 2020. *Global innovation index 2020*. Who Will Finance Innovation? Eds. by Soumitra Dutta, Bruno Lanvin, and Sacha Wunsch-Vincent Editors. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020.pdf (Last accessed: 18 August 2022).

224. WIPO, 2021. *Global innovation index 2021*. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2021.pdf (Last accessed: 31 August 2022).

225. World Economic Forum, 2020. *Global Risks Report*. URL: https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (Last accessed: 31 August 2022).

226. World Economic Forum, 2022. *Centre for the Fourth Industrial Revolution India*. URL: https://www.weforum.org/centre-for-the-fourth-industrial-revolution-india (Last accessed: 31 August 2022).

Додаток А

Список публікацій за темою дисертації

Статті у наукових фахових виданнях України

1. **Сябро А.В.** Сучасний стан розвитку інформаційно-комунікаційних технологій в Україні. *Гілея: науковий вісник.* 2018. Вип. 135 (№8). С. 364-367. URL: http://gileya.org/index.php?ng=library&cont=long&id=161

2. **Сябро А.В.** Пріоритети співробітництва Японії зі США у сфері кібербезпеки. *Гілея: науковий вісник*. 2019. Вип. 150 (№ 11). Ч. 3. С.72-77.

URL: http://gileya.org/index.php?ng=library&cont=long&id=214

3. Рижков М.М., **Сябро А.В.** Позиції держав Азійсько-Тихоокеанського регіону щодо ухвалення резолюцій з питань міжнародної інформаційної безпеки в рамках ООН. *Актуальні проблеми міжнародних відносин.* 2019. Вип. 139. С.13-26.

URL: http://www.library.univ.kiev.ua/ukr/host/viking/db/ftp/univ/apmv/apmv_2019_139.pdf

4. **Сябро А.В.** Особливості національної стратегії кібербезпеки Індії. *Міжнародні відносини. Серія «Політичні науки».* 2019. № 20. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/4136

Статті в іноземних виданнях

5. **Siabro Anastasiia.** The influence of scientific and technological development on the transformation of the global security paradigm. «*Evropský politický a právní diskurz» («European political and law discourse»).* 2021. Vol. 8 Iss. 5. C. 6-13. URL: https://eppd13.cz/wp-content/uploads/2021/2021-8-5/03.pdf

Праці, які додатково відображають наукові результати дисертації

6. **Сябро А.В.** Мілітаризація кіберпростору як чинник актуалізації проблеми інформаційної безпеки у сучасних міжнародних відносинах. *Міжнародна інформація / Міжнародні комунікації: історія, сучасність і перспективи:* матеріали Міжнародної науково-практичної конференції, 6 грудня 2019 року. *Міжнародні відносини. Серія «Політичні науки».* 2019. № 21. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/3873/3533

7. **Сябро А.В.** Проблема запровадження обмежень у сфері інформації і комунікації як чинник забезпечення національної інформаційної безпеки. *Стратегічне позиціонування України в сучасному міжнародному просторі*: матеріали Міжнародної науково-теоретичної конференції, 15 жовтня 2020 року. Київ, 2020. С. 72-73.

URL: http://www.iir.edu.ua/uploads/files/%D0%A2%D0%B5%D0%B7%D0%B8_SPIMUS_2020.pdf

8. **Сябро А.В.** Сутнісні характеристики стратегії інформаційної безпеки Південної Кореї. *Актуальні питання суспільних та гуманітарних наук (Глухівські читання-2020)*: збірник матеріалів X Міжнародної науково-практичної інтернет-конференції, 9-11 грудня 2020 року. Глухів: Глухівський НПУ ім. О. Довженка, 2020. С. 113-115.

URL: http://tpgnpu.ho.ua/images/my_images/doc_pdf/vidavnictvo/glchit_%202020.pdf

9. **Сябро А.В.** Трансформація концепту «м'якої» сили в сучасному інформаційному протиборстві. *Травневі студії 2021: історія, міжнародні відносини, філософія:* збірник матеріалів III Міжнародної наукової конференції студентів та молодих вчених, 23 квітня 2021 року. Вінниця: ДонНУ імені Василя Стуса, 2021. Вип. 6. С. 92-94.

URL: https://jts.donnu.edu.ua/article/view/10896

10. **Сябро А.В.** Інформаційна безпека у стратегіях діяльності міжнародних регіональних організацій (на прикладі АТР). *Шевченківська весна 2021:* матеріали Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених, 29 березня, 2021. Київ, 2021. С. 51-55.

URL: http://www.iir.edu.ua/uploads/files/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D0%A8%D0%92_2021_%D0%B0%D1%81%D0%BF%D1%96%D1%80%D0%B0%D0%BD%D1%82%D0%B8(1).pdf

Додаток Б

Відомості про апробацію результатів дисертації

1. Міжнародна науково-практична конференція «Міжнародна інформація / Міжнародні комунікації: історія, сучасність і перспективи», 6 грудня 2019 року, м. Київ, Україна, наукова доповідь та публікація матеріалів.

2. Міжнародної науково-теоретична конференція «Стратегічне позиціонування України в сучасному міжнародному просторі», 15 жовтня 2020 року, м. Київ, Україна, наукова доповідь та публікація матеріалів.

3. X Міжнародна інтернет-конференція молодих учених і студентів «Глухівські наукові читання - 2020. Актуальні питання суспільних і гуманітарних наук», 9-11 грудня 2020 року, м. Глухів, Україна, наукова доповідь та публікація матеріалів.

4. Міжнародна науково-практична конференція студентів, аспірантів і молодих вчених «Шевченківська весна 2021», 29 березня 2021 року, м. Київ, Україна, наукова доповідь та публікація матеріалів.

5. III Міжнародної наукової конференції студентів і молодих вчених «Травневі студії 2021: історія, міжнародні відносини, філософія», 23 квітня 2021 року, Вінниця, Україна, наукова доповідь та публікація матеріалів.