Міністерство освіти і науки України
Львівський національний університет імені Івана Франка

Кваліфікаційна наукова
праця на правах рукопису

ПОТЕРЕЙКО ОРИСЛАВА ОЛЕГІВНА

УДК 321.01:004.77](043.5)

ДИСЕРТАЦІЯ

ВІРТУАЛІЗАЦІЯ ДЕРЖАВИ: ТЕОРЕТИКО-МЕТОДОЛОГІЧНИЙ АНАЛІЗ

23.00.01 – теорія та історія політичної науки

Подається на здобуття наукового ступеня кандидата політичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ О. О. Потерейко

Науковий керівник: Хома Наталія Михайлівна, доктор політичних наук, доцент

Львів – 2019

АНОТАЦІЯ

Потерейко О. О. Віртуалізація держави: теоретико-методологічний аналіз. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата політичних наук за спеціальністю 23.00.01 «Теорія та історія політичної науки». – Львівський національний університет імені Івана Франка. Львів, 2019.

У дисертації акцентовано, що основні ознаки держави, визначені ще Конвенцією Монтевідео (1933), практично не змінювалися і нині потребують перегляду. Дисертантка аргументує таку необхідність стрімким розвитком інформаційно-комунікаційних технологій, глобалізацією та іншими чинниками новітнього соціально-політичного розвитку. У роботі відзначено: 1) комунікативні технології нівелювали відстані та державні кордони, «стиснули» час та відстані донесення інформації; 2) трансформується ставлення громадян до влади та політики загалом, стрімко видозмінюються шляхи комунікації, посилюються наслідки такої комунікації для держави та громадянина. Відтак інформаційно-комунікативні технології істотно вплинули на державу, модернізуючи її функції та ознаки. Дисертантка аргументує, що аби не втрачати зв’язок із громадянами, сучасна держава нині змушена виступати активним актором інформаційно-комунікаційного простору, поширювати на нього свою юрисдикцію. Відзначено: продовжуючи виконувати більшість традиційних функцій, новітні держави активно творять нові, трансформуючи класичні напрямки своєї діяльності.

У дослідженні відзначено тенденцію, зумовлену розвитком інформаційного простору – медіатизацію політики, в результаті якої держава перетворюється на комплекс символічних репрезентацій у свідомості громадян, змушена змагатися за їхню увагу, відстоювати свій авторитет в інформаційному просторі. З цією метою держава щораз частіше виступає учасником символічних, гібридних та інших медіа-протистоянь.

Відтак дисертанткою обґрунтовується, що перед новітньою державою стоїть завдання напрацювання нових механізмів взаємодії з громадянами, уможливлення швидкості та простоти комунікації в системі «влада – громадянин», розвитку нових компетенцій бюрократії, захисту національного інформаційного простору від тих дій, які посягають на національну державу. Аргументовано, що механізми здійснення державної влади стають дедалі більше узалежнені від комунікаційних процесів, що найперше проявляється у зміні форматів спілкування між громадянами та державними структурами. Підкреслено: громадяни отримують щораз більше можливостей впливати на політичні рішення – зокрема через Інтернет, а відтак новітні держави вимушені набувати повноважень реагування на інформаційні потоки, урахування їх у прийнятті подальших рішень.

Відтак констатовано: технологічний розвиток трансформує поняття «держава», її ознаки, функції. Усвідомивши нові виклики та перспективи розвитку інформаційного суспільства, держави уже прийняли та впроваджують стратегії кібербезпеки. Ці процеси обумовлюють актуальність дослідження віртуалізації держави, розробку теоретико-методологічного підґрунтя вивчення цих процесів. Наголошено: окрім теоретичної актуальності, зумовленої відсутністю досліджень щодо віртуалізації інституту держави в українській політичній науці, аналізувати процеси віртуалізації важливо з огляду на потребу конструювання дієвої стратегії кібербезпеки.

Метою дисертації визначено пошук пізнавальних моделей, аналіз еволюції наукової концептуалізації та евристичних перспектив процесу віртуалізації держави. Для досягнення дослідницької мети були поставлені завдання: дослідити еволюцію політичних ідей про «віртуальне»; виявити особливості становлення та теоретичного осмислення процесів віртуалізації держави; систематизувати головні методологічні підходи до аналізу проблеми віртуалізації держави та з’ясувати найоптимальніші наукові бачення, що об’єктивно засвідчують зміст реалізації віртуалізації держави в умовах глобалізації; дослідити зміну системи ознак сучасної держави та форматів її

співпраці з громадянами; запропонувати авторську теоретико-методологічну концептуалізацію понять «кібердержава», «віртуалізація держави»; проаналізувати на прикладі США, ФРН, Польщі та України процеси віртуалізації інституту держави.

Об'єктом дослідження виступає віртуалізація держави як процес формування нового типу цифрової держави (кібердержави), яка базується на імплементації досягнень інформаційно-комунікаційних технологій у політику. Предметом дослідження є форми політичної рефлексії про віртуалізацію інституту держави, концептуалізація відносин в системі «людина – держава» в умовах поглиблення віртуалізації держави.

Теоретико-методологічний інструментарій дисертації охоплює найперше наукові теоретичні дослідження кінця XX – початку XXI століть. Мова про класиків концепції інформаційного суспільства (З. Бауман, У. Бек, Д. Белл, Е. Тоффлер, М. Кастельс та ін.) праці яких сформували уявлення про особливості сучасної епохи та зумовлені ними загрози для новітньої держави. На основі праць з комунікативістики (М. Маклюен, Є. Морозов та ін.) вивчаються зміни інституту держави та небезпеки для його стабільного функціонування, зумовлені глобалізаційними та новітніми інформаційно-комунікаційними тенденціями. Праці постмодерністів (Ж. Бодрійяр, П. Віріліо, Ж. Деріда, Ж. Дельоз, М. Фуко та ін.) допомогли розкрити ідею символізації ознак держави. Дослідження опирається на низку нормативно-правових актів. Предмет дослідження зумовив звернення до міждисциплінарного підходу, що синтезує дві методології – інституційну та комунікативну. Завдяки інституційному підходу уможливився аналіз перетворень (віртуалізації) політичного інституту держави, основні ознаки якого визначені Конвенцією Монтевідео та потребують перегляду в умовах інформаційно-комунікаційного прогресу. Комунікативний підхід уможливив поєднання теорії глобалізації, постмодерного символічного обміну та дискурс-аналізу з ідеями віртуалізації держави, що відбуваються в умовах розвитку комунікативних технологій та в інформаційному середовищі, а також аналіз інформаційних воєн як один із

виявів віртуалізації держави. Також з метою з'ясування тенденцій віртуалізації держави в дослідженні використано метод контент-аналізу, що уможливив аналіз текстів національних стратегій кібербезпеки. Також у дисертації використано історичний, порівняльний методи, методи синтез та аналіз.

Структура дисертації передбачає чотири розділи, поділені на підрозділи. Перший розділ охоплює аналіз історіографії та визначає методологію дослідження. Другий розділ поділений на чотири підрозділи, що зумовлене логікою дослідження: оскільки Конвенція Монтевідео виділяє чотири основні ознаки класичної держави (постійне населення, визначена територія, уряд та здатність взаємодіяти з іншими державами), то кожен з підрозділів аналізує одну з них, акцентуючи на вияві ознак віртуалізації. Третій розділ аналізує кіберстратегії США, ФРН та Польщі. Четвертий розділ присвячений дослідженню віртуалізації Української держави. Аналіз, найперше, здійснюється на основі вивчення нормативно-правових актів, прийнятих за останні п'ять років.

Наукова новизна одержаних результатів зумовлена сукупністю визначених завдань, засобами їхнього розв'язання. Віртуалізацію держави дисертантка визначає як процес видозміни основних ознак держави (постійне населення, визначена територія, дієздатний уряд і здатність вступати у міжнародні зв'язки з іншими державами) під впливом інформаційно-комунікаційних і глобалізаційних процесів. Виділено основні чинники віртуалізації: а) щодо постійного населення – перенесення до кіберпростору механізмів формування національної ідентичності; б) щодо постійної території – «розмивання» кордонів в процесі боротьби з кіберзлочинністю та глобальними ризиками; поступова втрата громадянами міцного зв'язку з певною територією; в) щодо уряду – поступове перенесення процесу прийняття урядових рішень в інформаційний простір, організація урядом заходів щодо кібербезпеки, залучення громадян до процесу прийняття державних рішень через інформаційний простір; г) щодо здатності держави вступати в міжнародні

відносини – ймовірність часткового делегування суверенітету в інформаційному просторі.

У дисертації на основі аналізу кіберстратегій США, ФРН і Польщі визначено основні тенденції віртуалізації інституту держави: до процесу управління безпекою в кіберпросторі залучаються нові актори (постачальники інформаційно-комунікативних технологій, НУО, наукові установи та ін.); кіберзлочини визначені небезпеками на рівні з іншими злочинами, посилюється електронна ідентифікація користувачів; розробляється ідея свободи в Інтернеті; в кіберпросторі вбачаються як небезпеки, так і можливості; держави декларують намір розвивати у громадян інформаційно-комунікаційну компетентність; держави об’єднуються для протистояння гібридним загрозам та ін. Також дисертанткою проаналізовані процеси віртуалізації Української держави за останні п’ять років шляхом дослідження проблем формування ідентичності громадян, регулювання відносин у кіберпросторі, у сфері кібербезпеки, появі нових органів і компетенцій органів влади в інформаційній сфері, реагуванні на гібридні загрози.

Дисертантка уточнює розуміння сутності віртуальної держави як форми існування національної держави, яка видозмінює свої класичні (за Концепцією Монтевідео) ознаки завдяки взаємодії інституту держави з кіберпростором. У дослідженні розглянуто поняття «інфляції» визначеної території держави (детериторіалізації) як сучасної тенденції, зумовленої змінами способів життя та комунікації, в результаті чого чинник території держави дедалі менше визначає її багатство, силу, впливовість на міжнародній арені. Дисертантка розвиває ідею «суспільства ризику» (У. Бек), що доповнюється авторським аналізом кіберстратегій, розроблених в США, ФРН, Польщі та певною мірою в Україні. Політологічного звучання набули в дослідження понять кіберпростору та кібердержави.

Практичне значення одержаних результатів визначається їх актуальністю, новизною і висновками – загальнотеоретичними та практичними. Теоретична цінність положень дисертації полягає не тільки в їх концептуальному, а й

дискусійно-постановочному характері. Дослідження формує наукові уявлення про сутність віртуалізації держави, особливості зміни традиційних ознак держави. Основні положення та висновки роботи можуть використовуватися в навчальному процесі при викладанні політологічних дисциплін, а також у практичній діяльності громадських активістів, інших суб'єктів політики.

Ключові слова: держава, віртуалізація держави, інформаційне суспільство, детериторіалізація, медіатизація, глобалізація, кіберпростір, кібербезпека.

SUMMARY

Potereiko O. O. Virtualization of the state: theoretical and methodological analysis. – Qualified scientific work on the rights of the manuscript.

Dissertation for a PhD candidate in Political Science, specialty 23.00.01 – Theory and History of Political Science. – Ivan Franko National University of Lviv. Lviv, 2019.

The dissertation emphasises that the basic features of the state, as defined by the Montevideo Convention (The Montevideo Convention on the Rights and Duties of States, 1933), have remained practically unchanged and demand of revision. The researcher argues the need for rapid development of information and communication technologies, globalization and other factors of modern social and political development. In the research work it is noted: 1) communication technologies leveled distances and state borders, "squeezed" time and distances of information transmission; 2) the attitude of citizens to government and politics is transformed, the ways of communication are changing rapidly, furthermore, the consequences of such communication for the state and the citizen are amplified. Therefore, information and communication technologies have significantly influenced the state, modernizing its functions and features. The researcher supposes that the modern state is now forced to play an active role in the information and communication space, to extend its jurisdiction to it in order not to lose connection with citizens. It is noted that the

newest states are actively creating new ones, transforming the classical areas of their activity, at the same time continuing to perform most of the traditional functions.

The tendency is spotted in the research and caused by the development of the information space – the mediation of politics, as a result of which the state becomes a complex of symbolic representations in the consciousness of citizens and is forced to compete for their attention and to assert their authority in the information space. The state is increasingly involved in symbolic, hybrid and other media confrontations for this purpose.

Therefore, the researcher justifies that the new state faces the challenge of developing new mechanisms of interaction with citizens, enabling the speed and simplicity of communication in the system "government – citizen", development new competencies of bureaucracy and the protection of the national information space from those acts which encroach upon the nation state. It is argued that the mechanisms for exercising state power are becoming increasingly dependent on communication processes, which is first manifested in the change of the communication formats between citizens and state structures. It is emphasised that citizens are getting more and more opportunities to influence political decisions, particularly through the Internet, consequently, the newest states have to acquire the power to respond to information flows and take them into account in their future decisions.

So it is stated: technological development transforms the concept of "state", its features and functions. Recognizing the new challenges and prospects for developing the information society, the states have already adopted and now they are implementing cybersecurity strategies. These processes determine the relevance of the study of virtualization of the state and the development of a theoretical and methodological basis for the study of these processes. Apart from the theoretical relevance, which is caused by the lack of research on the virtualization of the state institute in Ukrainian political science, it is important to analyze the processes of virtualization in view of the need to design an effective cybersecurity strategy.

The purpose of the dissertation is the search for cognitive models and analysis of the evolution of scientific conceptualization and heuristic prospects of the state virtualization process. The following tasks were set in order to achieve the research goal: 1) to explore the evolution of political ideas about the "virtual"; 2) to reveal peculiarities of formation and theoretical comprehension of the virtualization processes of the state; 3) to systematize the main methodological approaches to the analysis of the problem of state virtualization and to find out the most optimal scientific visions, which objectively certify the content of realization of the state virtualization in the conditions of globalization; 4) to explore the changing system of features of the modern state and the formats of its cooperation with citizens; 5) to offer the author's theoretical and methodological conceptualization of the concepts of "cyber state", "virtualization of the state"; 6) to analyze, on the example of the USA, Germany, Poland and Ukraine, the processes of virtualization of the state institute.

The object of the study is the virtualization of the state as a process of formation of a new type of digital state (cyber-state), based on the implementation of the achievements of information and communication technologies in politics. The subject of the study is the form of political reflection on the virtualization of the state institution and the conceptualization of relations in the system of "man – state" in the conditions the state virtualization expansion.

First of all, theoretical and methodological basis of the dissertation cover the scientific theoretical researches of the end of XX – beginning of XXI centuries. The classics' works about the concept of the information society (Z. Bauman, U. Beck, D. Bell, A. Toffler, M. Castells, etc.) formed an idea of the peculiarities of the modern era which caused the dangers to the modern state. On the basis of works on communication studies (M. McLuhan, E. Morozov, etc.) we can learn about the changes of the state institute and the dangers for its stable functioning which are caused by globalization and the latest information and communication tendencies. The works of postmodernists (J. Baudrillard, P. Virilio, J. Deridda, G. Deleuze, M. Foucault, etc.) helped to discover the idea of symbolization of the state features. The subject of the research led to an interdisciplinary approach that synthesizes two

methodologies – institutional and communicative. Due to the institutional approach, it was possible to analyze the transformations (virtualization) of the political institute of the state, the main features of which are defined by the Montevideo Convention and require a revision in the conditions of information and communication progress. The communicative approach made it possible to combine the theory of globalization, postmodern symbolic exchange and discourse analysis with the ideas of state virtualization that occur in the conditions of development of communication technologies and in the information environment, as well as the analysis of information wars as one of the manifestations of state virtualization. In the research, a content is used analysis to identify trends in state virtualization that made it possible to analyze the texts of national cyber security strategies. Historical, comparative, synthesis and analysis methods are also applied in the dissertation.

The structure of the dissertation consists of four chapters, which are divided into sections. The first chapter covers the analysis of historiography and defines the methodology of the research. The second chapter is divided into four sections, which is determined by the logic of the research. As the Montevideo Convention identifies four basic features of the classical state (permanent population, defined territory, government, and ability to interact with other states), each section analyzes one of them, focusing on identifying characteristics of virtualization. The third chapter analyzes the cyber strategies of the USA, Germany and Poland. The fourth chapter is devoted to the study of the Ukrainian state virtualization. The analysis, first of all, is based on a study of the legal acts which were adopted in the last five years.

The scientific innovativeness resulted from a set of defined tasks and importance of their solutions. The researcher defines state virtualization as a process of changing the basic features of the state (permanent population, defined territory, a capable government and ability to enter into international relations with other states) under the influence of information and communication and globalization processes.

The main factors of virtualization are distinguished as: a) the permanent population – the transfer of mechanisms of formation of national identity to cyberspace; b) the permanent territory – "blurrin" borders in the fight against

cybercrime and global risks; the gradual loss by citizens of a strong connection to a certain territory; c) the government – the gradual transfer of the government decision into the information space, the government's organization of cybersecurity activities, the involvement of citizens in the adoption process of government decision through the information space; d) the ability of the state to enter into international relations – the probability of partial loss of sovereignty in the information space.

In the dissertation on the basis of the cyber strategies of the USA, Germany and Poland the main tendencies of virtualization of the state institute are defined: 1) new actors (information and communication technology providers, NGOs, scientific institutions, etc.) are involved in the process of security management in cyberspace; 2) cybercrime that is identified by dangers is on par with other crimes, enhancing electronic user identification; 3) the idea of freedom on the Internet is being developed; 4) cyberspace we can see both dangers and opportunities; 5) states declare their intention to develop information and communication competence among citizens; 6) states unite to counter hybrid threats, etc.

The researcher emphasises the understanding of the essence of the virtual state as a form of existence of the nation state, which modifies its classical (according to the Montevideo Convention) features due to the interaction of the state institute with cyberspace. The dissertation includes a concept of "inflation" of a defined state territory (deterritorialization) as a modern tendency which is caused by changes in lifestyles and communication, as a result of which the factor of the territory of the state less and less determines its wealth, power and influence in the international arena. Researcher describes the idea of a "risk society" (U. Beck), which is complemented by the author's analysis of cyber strategies that are developed in the USA, Germany, Poland and Ukraine. The definitions of cyberspace and cyber state were politicized in the research.

The practical significance of the obtained results is determined by their relevance, novelty and conclusions – general theoretical and practical. The theoretical value of the dissertation consists in not only in their conceptual but also in discussion

and staging. The research generates scientific ideas about the essence of virtualization of the state and peculiarities of change of traditional features of it.

Key words: state, virtualization of the state, information society, deterritorialization, mediation, globalization, cyberspace, cybersecurity.

Список публікацій здобувача за темою дисертації

Праці, в яких опубліковані основні наукові результати дисертації

1. Потерейко, О. О. (2016). Теоретико-методологічні засади аналізу віртуалізації держави. *Вісник Львівського національного університету. Серія Філософсько-політологічні студії, 8*, 124–129.

2. Потерейко, О. О. (2016). Теоретико-методологічні підходи аналізу детериторіалізації у контексті віртуалізації держави. *Політикус, 1,* 38–40.

3. Потерейко, О. О. (2019). Населення як ознака віртуальної держави. *Гілея, 142,* 97–100.

4. Потерейко, О. О. (2019). Апарат управління як ознака держави в процесі віртуалізації. *Гілея, 144,* 108–111.

5. Potereiko, O. O. (2019). Government as a significant component of the virtual country. *Global Academics, 1 (2).* Available from: https://www.i-journal.org/upload/2.pdf

Праці, які засвідчують апробацію матеріалів дисертації

1. Потерейко, О. О. (2016). Віртуалізація держави як концептуальна характеристика еволюціонуючої політичної реальності. In Матеріали міжнародної науково-практичної конференції *Нове та традиційне у дослідженнях сучасних представників суспільних наук* (pp. 118-120). Київ: Київська наукова суспільнознавча організація.

2. Потерейко, О. О. (2016). Детериторіалізація як характеристика віртуалізації держави: аналіз теоретичних підходів. In Матеріали VI міжнародної науково-практичної конференції *Розвиток політичної науки:*

європейські практики та національні перспективи (pp. 33-35). Чернівці: Чернівецький національний університет імені Юрія Федьковича.

3. Потерейко, О. О. (2017). Віртуалізація соціально-політичної реальності: основні риси та аспекти. In Тези звітної наукової конференції філософського факультету Львівського національного університету імені Івана Франка (pp. 194-195). Дрогобич: ТзОВ «Трек».

4. Потерейко, О. О. (2017). Процеси віртуалізації держави в сучасному світі: теоретико-методологічний аналіз. In Тези II всеукраїнської науково-практичної конференції *Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів* (pp. 126-129). Одеса: ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського».

5. Потерейко, О. О. (2017). Вихід інформації за межі територіальних кордонів: проблема регулювання кіберпростору. In Матеріали всеукраїнської науково-практичної конференції *Пріоритетні завдання і стратегії розвитку суспільних наук* (pp. 90-93). Запоріжжя: Класичний приватний університет.

6. Потерейко, О. О. (2018). Криптовалюта як результат тенденції віртуалізації новітнього інституту держави. In Матеріали III всеукраїнської науково-практичної конференції *Соціально-політичні проблеми сучасності* (pp. 73-75). Дніпро: Університет імені Альфреда Нобеля.

7. Потерейко, О. О. (2019). Детериторіалізація в системі ознак віртуальної держави. In Матеріали IV всеукраїнської науково-практичної конференції *Соціально-політичні проблеми сучасності* (pp. 10-12). Дніпро: Університет імені Альфреда Нобеля.

З М І С Т

ВСТУП……16

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ВІРТУАЛІЗАЦІЇ ДЕРЖАВИ……24

1.1. Історіографія проблематики віртуалізації держави……...24

1.2. Методологія дослідження віртуалізації держави……...43

Висновки до розділу 1. ……...63

РОЗДІЛ 2. ЗМІНА ОЗНАК ДЕРЖАВИ В ПРОЦЕСІ ВІРТУАЛІЗАЦІЇ……..66

2.1. Трансформація ознаки населення в процесі віртуалізації новітньої держави……...66

2.2. Визначена територія як ознака держави в процесі віртуалізації…….74

2.3. Віртуалізація уряду та системи органів державної влади……86

2.4. Міждержавні відносини крізь призму віртуалізації……..97

Висновки до розділу 2……...106

РОЗДІЛ 3. ВІРТУАЛІЗАЦІЯ ІНСТИТУТУ ДЕРЖАВИ: КЕЙСИ США, ФРН І ПОЛЬЩІ……110

3.1. Постійне населення як об’єкт національних стратегій кібербезпеки……110

3.2. Державна територія як об’єкт національних стратегій кібербезпеки……121

3.3. Відображення механізмів віртуалізації уряду на прикладі кіберстратегій аналізованих держав……..127

3.4. Віртуалізація міжнародних відносин у стратегіях кібербезпеки…...136

Висновки до розділу 3……...145

РОЗДІЛ 4. ВІРТУАЛІЗАЦІЯ УКРАЇНСЬКОЇ ДЕРЖАВИ: ДОСВІД 2014–2019 РОКІВ……..147

4.1. Особливості населення як класичної ознаки держави за умов віртуалізації інституту держави в Україні……147

4.2. Державна територія в умовах віртуалізації інституту держави в Україні……..153

4.3. Віртуалізація на урядовому рівні функціонування інституту держави в Україні……..……..157

4.4. Міждержавні відносини крізь призму віртуалізації України……168

Висновки до розділу 4……..174

ВИСНОВКИ ……176

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……184

ДОДАТКИ 200

В С Т У П

Актуальність теми дослідження. Науковий інтерес до проблематики віртуалізації держави є увиразненням змін, які відбуваються нині під впливом глобалізації, технологічної революції, цифровізації та низки інших чинників. В сутності віртуалізації та віртуальної держави прослідковуються щонайменше два аспекти: 1) технологічний (реальний, матеріальний); 2) онтологічний (суб'єктивний, сконструйований, уявний). Відтак для політичної науки цікавими є процеси, коли за допомогою технологічних новацій відбувається більшою чи меншою мірою заміщення реальної держави, як основи організації та консолідації суспільства, певною уявною моделлю. Постає питання про консолідуючу здатність такої моделі держави. Потребує з'ясування: чи існує (може існувати) та наскільки ефективно здатна функціонувати держава віртуального типу або ж, можливо, це лише сконструйований технологіями та дискурсом конструкт; наскільки зміняться визначальні ознаки держави в умовах сьогодення та в перспективі.

Основні ознаки держави були визначені ще у 1933 році в Конвенції Монтевідео; відтоді вони практично не переглядалися. Проте така необхідність назріла з огляду на стрімкий розвиток технологій, цифровізацію, глобалізацію та інші чинники. Очевидно, що новітня держава набуває нової конфігурації. Зберігаючи свої основні класичні ознаки, інститут держави модернізує їх, пристосовуючи до особливостей сьогодення. Продовжуючи реалізацію низки традиційних функцій, новітні держави активно творять нові; це супроводжується глобалізацією функцій сучасної держави. Комунікативні технології нівелювали відстані та державні кордони, «стиснули» час донесення інформації, надали цьому процесу нових форм. Водночас в останні десятиліття стрімко трансформується ставлення громадян до влади та політики загалом, видозмінюються шляхи комунікації в системі «людина – держава» («держава в смартфоні»), посилюються наслідки комунікативних взаємодій як для держави, так і для громадянина.

Цифровізація стає визначальною для політичного інституту держави, модернізуючи його функції та ознаки. Глобалізація посилила небезпеки функціонування сучасних держав, адже через відкритість кордонів, активізацію міжнародних взаємодій, нині держави втрачають здатність самотужки подолати небезпеки функціонування кіберпростору; через взаємозалежність економік інститут держави більше не може одноосібно передбачити перспективи власного економічного розвитку тощо.

Відзначимо й тенденцію, зумовлену еволюцією інформаційного простору – медіатизацію політики, в результаті якої держава перетворюється на комплекс символічних репрезентацій у свідомості громадян, змушена змагатися за їхню увагу, відстоювати свій авторитет в інформаційному просторі. З цією метою держави дедалі частіше виступають учасниками символічних, гібридних та інших медіа-протистоянь.

З огляду на зазначене, перед новітньою державою стоїть завдання напрацювання нових механізмів взаємодії з громадянами, уможливлення швидкості та простоти комунікації державних органів, розвитку нових компетенцій бюрократії, захисту національного інформаційного простору від посягань на національну державу тощо. Механізми здійснення державної влади стають дедалі більше узалежнені від комунікаційних процесів, що найперше проявляється у зміні форматів спілкування між громадянами та державними структурами. Громадяни отримують щораз більше можливостей впливати на політичні рішення завдяки цифровізації, а відтак сучасні держави набувають навичок реагування на інформаційні потоки, розвитку нових форм взаємодії з громадськістю.

Відтак констатуємо: технологічний прогрес нині стрімко трансформує сутність держави, її ознаки, функції, механізми функціонування, сприйняття цього інституту громадянами. Переваги, а також ймовірні загрози таких процесів, потребують вивчення, що й обумовлює актуальність дослідження комплексу питань віртуалізації держави. Це актуалізоване нещодавно

презентованим в Україні брендом цифрової держави («держави в смартфоні») і наміром впровадження цієї моделі держави найближчими роками.

Зв'язок роботи з науковими програмами, планами, темами. Наукове дослідження є частиною комплексної науково-дослідної теми кафедри теорії та історії політичної науки Львівського національного університету імені Івана Франка «Теорії політики: форми політичної рефлексії» (державний номер реєстрації № 0111U005524).

Мета дисертації науковій концептуалізації та з'ясуванні евристичних перспектив віртуалізації держави.

Для досягнення дослідницької мети поставлено такі **завдання:**

– дослідити еволюцію ідей про «віртуальне»;

– систематизувати головні методологічні підходи до аналізу проблеми віртуалізації держави, на основі чого з'ясувати зміст віртуалізації політичного інституту держави;

– виявити сутнісні характеристики віртуальної держави, особливості процесу віртуалізації цього інституту;

– з'ясувати особливості віртуалізації постійного населення як ознаки держави;

– проаналізувати новітні процеси віртуалізації державної території;

– схарактеризувати процеси віртуалізації системи органів державної влади;

– розкрити особливості віртуалізації міждержавних відносин;

– проаналізувати на прикладі зарубіжних держав (США, ФРН та Польща) спільні та відмінні особливості процесу віртуалізації інституту держави;

– визначити особливості віртуалізації інституту держави в Україні.

Об'єкт дослідження – процеси віртуалізації держави на технологічному та онтологічному рівнях, що конструюють систему принципів та інструментів (детериторіалізація, дискурсивізація, медіатизація та ін.).

Предмет дослідження – форми політичної рефлексії про віртуальну державу, концептуалізацію відносин «людина – держава» в умовах віртуалізації держави.

Методологічна основа дисертації. Теоретико-методологічний інструментарій опирається на низку теоретичних досліджень, найперше, класиків концепції інформаційного суспільства (З. Бауман, У. Бек, Д. Белл, Е. Тоффлер, М. Кастельс та ін.), праці яких сформували уявлення про особливості сучасної епохи та зумовлені ними загрози для новітньої держави. На основі праць з комунікативістики (М. Маклюен, Є. Морозов та ін.) вивчаються зміни інституту держави та небезпеки для його стабільного функціонування, зумовлені глобалізаційними та новітніми інформаційно-комунікаційними тенденціями. Праці постмодерністів (Ж. Бодрійяр, П. Віріліо, Ж. Деріда, Ж. Дельоз, М. Фуко та ін.) допомогли розкрити ідею символізації ознак держави. Серед українських вчених відзначимо науковий доробок В. Кривошеїна, Г. Почепцова, І. Свища, Г. Піскорської, Н. Ротар, О. Солдатенко, Н. Яковенко, Д. Яковлєва та ін. Дослідження звертається до вітчизняних і закордонних нормативно-правових актів (Конвенція Монтевідео, Конвенція про кіберзлочинність, національні стратегії кібербезпеки США, ФРН та Республіки Польщі, низка нормативних актів України).

Предмет дослідження зумовив звернення до міждисциплінарного підходу, що синтезує дві методології – інституційну та комунікативну. Завдяки інституційному підходу уможливлюється аналіз перетворення (віртуалізації) політичного інституту держави, основні ознаки якого визначені Конвенцією Монтевідео та потребують перегляду в умовах інформаційно-комунікаційного прогресу. Комунікативний підхід сприяв поєднанню теорії глобалізації, постмодерного символічного обміну та дискурс-аналізу з ідеями віртуалізації держави.

Цінною для дослідження процесів віртуалізації держави є й конструктивістська парадигма як постнекласична теорія пізнання політичної реальності. Держава та процеси її модернізації в межах цієї парадигми

постають дискурсивними конструктами, породженими і формами сприйняття масової повсякденної свідомості, соціально-політичних почуттів, і політичними технологіями. Відтак новий політичний порядок формується не лише завдяки результатам діяльності інститутів і соціальних груп, а й значною мірою завдяки різним дискурсам, що спрямовують соціально-політичні рефлексії в процесі соціальних інтеракцій.

З метою виявлення тенденцій віртуалізації держави, в дослідженні використано метод контент-аналізу, що уможливив аналіз текстів національних стратегій кібербезпеки. Також дисертація опирається на історичний, порівняльний методи, синтез та аналіз.

Наукова новизна одержаних результатів зумовлена сукупністю визначених завдань, засобами їхнього розв’язання й конкретизована в таких положеннях:

вперше:

– розглянуто віртуалізацію держави на технологічному (як перенесення виконання державою своїх функцій у вимір Інтернету) та символьному (як перетворення сфер діяльності держави через продукування та поширення соціально-політичних символів) рівнях; акцентовано на видозміні основних ознак держави під впливом глобалізаційних, технологічних, інформаційно-комунікаційних змін;

– віртуалізацію держави інтерпретовано як систему принципів, інструментів (детериторіалізація, дискурсивізація, медіатизація та ін.), які поєднують конструктивні та деструктивні наслідки, що проявляється у ставленні до інституту громадянства, мірі лояльності до держави, руйнуванні національної ідентичності, обмеженні суверенітету, глобальній технологічній залежності тощо;

– виділено основні чинники віртуалізації: а) щодо постійного населення – перенесення до кіберпростору механізмів формування національної ідентичності; б) щодо постійної території – «розмивання» кордонів в процесі боротьби з кіберзлочинністю та глобальними ризиками; поступова втрата

громадянами міцного зв’язку з певною територією; в) щодо уряду – поступове перенесення процесу прийняття урядових рішень в інформаційний простір, організація заходів кібербезпеки, залучення громадян до процесу прийняття державних рішень через інформаційний простір; г) щодо здатності держави вступати у міжнародні відносини – часткове делегування суверенітету держави;

– на основі аналізу кіберстратегій США, ФРН і Польщі визначено основні тенденції віртуалізації інституту держави: до процесу управління безпекою в кіберпросторі залучаються нові актори (постачальники інформаційно-комунікативних технологій, НУО, наукові установи та ін.); кіберзлочини визначені небезпеками на рівні з іншими злочинами; посилюється електронна ідентифікація користувачів; визначаються межі свободи в Інтернеті; у кіберпросторі вбачаються як небезпеки, так і можливості; держави декларують намір розвивати у громадян інформаційно-комунікаційну компетентність; держави об’єднуються для протистояння гібридним загрозам;

– проаналізовані процеси віртуалізації Української держави впродовж 2014–2019 років шляхом дослідження проблем формування ідентичності громадян, відносин у кіберпросторі, у сфері кібербезпеки, діяльності нових органів і компетенцій органів влади в інформаційній сфері, реагуванні на гібридні загрози;

уточнено:

– розуміння сутності віртуальної держави як форми існування національної держави, яка видозмінює класичні (за Концепцією Монтевідео) ознаки завдяки взаємовпливам в системі «держава – кіберпростір»;

– поняття «інфляції» визначеної території держави (детериторіалізації) як тенденції, зумовленої змінами способів життя та комунікації, в результаті чого чинник території держави дедалі менше визначає її багатство, силу, впливовість на міжнародній арені;

набули подальшого розвитку:

– ідея «суспільства ризику» (У. Бек), що доповнюється аналізом кіберстратегій США, ФРН, Республіки Польщі та України: відповідальність за

безпеку покладається на державу, але в протидії значним загрозам необхідна кооперація ресурсів держав;

– поняття кіберпростору та кібердержави, яким надано політологічного звучання через визначення їх сферою державної юрисдикції, а в українському випадку – і сферою домінування національного інтересу.

Практичне значення одержаних результатів визначається їх актуальністю, новизною і висновками – загальнотеоретичними та практичними. Теоретична цінність положень дисертації полягає не тільки в їх концептуальному, а й дискусійно-постановочному характері. Дослідження формує наукові уявлення про сутність віртуалізації держави, особливості зміни традиційних ознак держави. Основні положення та висновки роботи можуть використовуватися в навчальному процесі при викладанні політологічних дисциплін, а також у практичній діяльності суб'єктів політики.

Апробація результатів дисертації. Основні положення дисертації апробовані на міжнародних і всеукраїнських наукових конференціях: «Нове та традиційне у дослідженнях сучасних представників суспільних наук» (м. Київ, 5–6 лютого 2016 р.), «Розвиток політичної науки: європейські практики та національні перспективи» (м. Чернівці, 7–8 квітня 2016 р.), звітній конференції філософського факультету Львівського національного університету імені Івана Франка (м. Львів, 10–11 лютого 2017 р.), «Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів» (м. Одеса, 10 лютого 2017 р.), «Пріоритетні завдання і стратегії розвитку суспільних наук» (м. Запоріжжя, 17–18 листопада 2017 р.), «Соціально-політичні проблеми сучасності» (м. Дніпро, 28 березня 2018 р.).

Публікації. За темою дисертації опубліковано 12 наукових публікацій, з яких 4 статті у фахових виданнях із політичних наук в Україні, 1 стаття в іноземному виданні, 7 опублікованих тез доповідей на науково-практичних конференціях.

Структура та обсяг дисертації зумовлені метою та завданнями, визначеними в процесі науково-теоретичної розробки теми. Наукове

дослідження складається зі вступу, чотирьох розділів (14 підрозділів), висновків, списку використаних джерел та літератури (202 найменування). Загальний обсяг дисертації – 201 сторінка, із них основний текст – 168, список використаних джерел і літератури – 18 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ВІРТУАЛІЗАЦІЇ ДЕРЖАВИ

1.1. Історіографія проблематики віртуалізації держави

Проблема віртуального в соціально-політичній реальності віддавна була увиразнена в політичній філософії. У XX столітті вона набула нового звучання, передусім, позбувшись метафізичних та онтологічних меж. З огляду на розвиток технологій, поширення ЗМІ (зокрема нових медіа), збільшення масштабів символічного обміну назріла практична потреба вивчення процесів віртуалізації. В результаті виникнення методологічних можливостей для осмислення цього поняття в усій його складності, науковці накопичили комплекс підходів до аналізу проблеми віртуалізації держави.

Відзначимо науковий доробок французьких постмодерністів (Ж. Бодрійяр, Ж. Дерріда, М. Фуко та ін.), що започаткували переосмислення ролі сучасної держави в житті індивіда та суспільства. Теорія глобалізації (З. Бауман, У. Бек, Д. Белл, М. Кастельс, Е. Тоффлер та ін.) також ґрунтовно пояснює, як під впливом сучасних комунікативних та інфраструктурних перетворень змінюються класичні ознаки держави. Не можна проігнорувати і напрацювання в галузі комунікативних наук (В. Ліппман, М. Маклюен, Г. Почепцов та ін.), завдяки яким до політичної науки була інтегрована низка понять, наприклад, «глобальне село».

Отож, аби проаналізувати історіографію проблематики віртуалізації держави, доцільно застосувати міждисциплінарний підхід, об’єднати знання різних галузей, адже проблема стосується багатьох вимірів віртуалізації держави. Передусім йдеться про напрацювання політичної науки, політичної філософії, політичної соціології, політичної комунікації, семіотики та права. Відзначимо, що проблематика віртуалізації держави найперше опирається на політичну філософію; без звернення до цих основ ми не зможемо повноцінно аналізувати новітні процеси віртуалізації держави.

Аналіз проблеми віртуальності опосередковано зародився ще в Античності, коли Платон запропонував теорію про світ ідей, яка може розглядатися підґрунтям теорії віртуалістики. Зокрема, йдеться про Платонів поділ дійсності на «світ речей» і «світ ідей» (ейдосів). У певному ракурсі цей підхід можна вважати розмежуванням реального та віртуального світів. Царству ідей філософ відводить статус невигаданого світу, а рівно можливого модусу реальності, первинного. У дев'ятій книзі діалогу «Держава» читаємо: «[…] ти маєш на увазі державу, побудову якої ми щойно розглянули, тобто таку, яка існує лише у сфері думок, бо на землі, як мені здається, її ніде немає. – Але на небі, – зауважив я, – можливо, є її взірець, приступний для того, хто хоче побачити його, а дивлячись на нього, впорядкувати самого себе. І немає ніякого значення, чи вже існує десь на землі така держава, чи щойно буде, бо та людина зайнялася б справами лише такої держави, а жодної іншої – ні» [93, с. 279].

Одне з основних тверджень Платона полягає в тому, що видиме не є реальним, а якщо ми щось бачимо, то це зовсім не означає, що воно існує саме так, як ми це сприймаємо. Це пригадування вічного, первинного, істинного образу речі, створеної Богом. «Свого часу Бог, чи тому, що не захотів, чи, може, була якась необхідність, яка вимагала, щоб більше одного ліжка в природі не існувало, саме й зробив лиш одне-єдине ліжко – те, що, власне, і є ліжком як таким. А двох подібних чи більше Бог не створював і не створить ніколи» [93, с. 301], – йдеться в десятій книзі діалогу.

Важливо, що в контексті вчення Платона «світ ідей» як віртуальний не означає, що ідеї існують лише в мізках людей. Він існує в особливому, вищому, недоступному для людей світі, а навколишні речі – лише породження та відбиття цих ідей.

Варто наголосити на ще одній ідеї, яку Платон висловив у діалозі «Держава». Це «міф про печеру», що став метафоричним поясненням його ідеї про двоїстість сприйняття світу (реальність та її «замінники»). У сьомій книзі діалогу мислитель алегорично порівнює людське життя з життям у печері:

«Уяви собі, що люди ніби перебувають у підземному, подібному до печери помешканні, до якого на всю ширину печери веде відкритий для світла вхід. Люди сидять тут ще з дитинства, мають скуті кайданами ноги й шию, тож рушитися з місця вони не можуть і дивляться лише просто себе, бо повернути голову їм не дозволяють кайдани. Згори та здалеку падає на них світло вогню, до якого вони обернені плечами, а між вогнем і кайданниками проходить вгорі дорога, паралельно до якої, уяви собі, вибудуваний невисокий мур, що нагадує перегородку, яку штукарі встановлюють перед глядачами та над якою показують своє мистецтво?» [93, с. 210]. На стіні цієї печери, перед очима ув'язнених, відбиваються тіні тих предметів, які перебувають за її межами, але оскільки люди сидять спиною до виходу, то вони не знають про реальність їхнього існування. За описом Платона, їм здається, що тінь, яку вони бачать, і є самими предметами та є єдино можливою реальністю.

Вся палітра їхніх уявлень про світ обмежується візерунками тіней, грою світла та відлуння, що мають місце за межами печери. «– Дивний же ти малюєш образ і дивних кайданників! – вигукнув він. – Подібних до нас, – сказав я. – Бо, передовсім, невже ти думаєш, що такі люди могли б бачити ще щось – своє чи чуже, окрім тіней, які кидає вогонь на протилежну стіну печери? – Як вони можуть бачити щось інше, коли все життя ніхто з них голови не поверне?» [93, с. 210].

Відтак Платон один з перших почав розвивати ідею онтологічного роздвоєння світу. Недосяжний світ ідеї можна вважати прообразом віртуальної (з іншого виміру) реальності.

Арістотель спробував подолати такий категоричний розрив, помістивши ідею всередину самої речі. Будь-яка ідея, за його переконанням, перебуває не в ефемерному царстві небесних ідей, а в самій речі, виступаючи її формою. При цьому, ейдос речі несе в собі як її поодинокі властивості (що зумовлює її відмінність від інших), так і щось спільне (що дозволяє говорити про її цілісність).

Згодом ідея віртуальності розвивалася теологами Середньовіччя. Наприклад, шотландський мислитель І. Д. Скот, диференціюючи онтологічне трактування Томи Аквінського, ввів поняття actus virtualis (віртуальний акт) як проміжну ланку між актом і потенцією [115, с. 74]. Так, внутрішній віртуальний акт буття переводить його з потенції в акт, не залучаючи нікого зі сфери зовнішнього буття. І. Д. Скот відкинув принцип «усе, що рухається, рухається чимось іншим» і, відповідно, перший доказ буття Бога Томи Аквінського [115, с. 74]. Також мислитель наполягав на тому, що поняття речі містить у собі емпіричні атрибути не формально (якби річ існувала окремо від емпіричних спостережень), а virtualiter, віртуально. Хоча для розуміння властивостей речі нам може бути потрібно заглибитися в наш досвід, продовжує мислитель, сама реальна річ вже містить безліч емпіричних якостей у своїй єдності, а містить їх віртуально – в іншому випадку, всі вони не закріпилися б як якості цієї речі.

І. Д. Скот використовує термін «віртуальний» для подолання розриву між нашим досвідом і наступним рівнем людського розуміння [115, с. 74]. Віртуальний простір, як протилежність природному тілесному простору, містить інформаційний еквівалент речей. Віртуальний простір змушує нас поводитися так, ніби ми маємо справу з тілесною або природною реальністю [169]. Для філософа щось містить віртуально якийсь ефект, якщо воно здатне його здійснювати, так само як і якесь поняття – якщо це поняття виникає в розумі, що його пізнає [115, с. 74].

Використання терміну «віртуальне» представлене й у трактатах Н. Кузанського, але набуває семантики сили, потенції насіння. Так, в праці «Про бачення Бога» (1453), розмірковуючи про першооснову всього сущого, філософ наводить приклад свого споглядання за горіховим деревом: «Потім розумним оком я бачу, що те ж дерево перебувало у своєму насінні не так, як я зараз його споглядаю, а віртуально; я звертаю увагу на дивну силу того насіння, в якому воно уклалося цілком і це дерево, і всі його горіхи, і вся сила горіхового насіння, і в силі насіння всі горіхові дерева» [67, с. 46].

Отже, для Середньовіччя поняття віртуального означало найперше взаємозв'язок між дійсним і уявним, між наміром та дією. Ним позначали причину можливого і дійсного, потенційного та актуального. Ще в Античності простежувалася ідея поділу світу на дійсний та поставлений за межі людського сприйняття, буття та інобуття, що мають в основі онтологічні міркування. Ці ідеї й розвинулися в Середньовіччі, де вже використовувалося безпосередньо поняття «віртуальне», позначаючи ним інформаційний еквівалент про річ та її можливості.

Дж. Берклі вперше сформулював думку, що зовнішня, незалежна реальність, яка перебуває по інший бік людської свідомості, створюється цією свідомістю, як певна послідовність, що визначається як річ. Ефект віртуалізації реальності полягає у співвіднесенні людського досвіду й пізнання з певною матеріалізацією віртуальних процесів, що відбувається в середині нас [35].

Важливим для усвідомлення віртуальності є підхід філософа XVII століття Г. В. Лейбніца. Мислитель першим ужив термін «можливі світи» та розвинув ідею їх створення в працях «Теодіції» (1710) і «Монадології» (1720). Дослідник уважав, що розум Бога є безкінечним та існує поза часом і простором. На його переконання, всі можливі світи – це лише ідеї або уявлення, котрі існують в думках всюдисущого Бога, а світ, в якому ми живемо – це обраний Богом реальний світ, де все перебуває у гармонії. Ідея відповідає Всесвіту, який є її ментальною репрезентацією. Індивід існує у світі, якщо ідея представляє його, як щось, що існує [2; 178]. Філософ стверджував, що ми живемо в найкращому зі світів, втім, наприклад, А. Шопенгауер заперечив: наш світ – найгірший з можливих світів [139].

Ідею подвійності світу розвивав німецький філософ І. Кант, який аналізував можливості та межі людського пізнання світу. Як зазначають українські дослідники О. Дзьобань і Є. Мануйлов, філософія І. Канта ставить у відповідність віртуальному й матеріальному світам ноумени (те, чим річ є сама по собі) і феномени (те, чим річ є для нас) [35]. І. Кант представляє світ у двох вимірах – чуттєвому (феномен) і ноуменальний світ (не піддається чуттєвому

сприйняттю). Життя при цьому розглядається як єдність дійсної (земної, нижчої) та віртуальної (небесної, вищої) реальностей. Моральний світ І. Кант також оголосив віртуальним. Таким чином, можна сказати, що сьогоднішня віртуальна мережа, за визначенням І. Канта, утворює світ віртуальний, оскільки ступінь формування ціннісних установок під її впливом залежить від моральних якостей користувачів [35].

У XX столітті філософ-позитивіст Р. Карнап запропонував свою теорію опису можливих альтернативних світів: «state description of possible alternative worlds». За основну було взято ідею Г. Лейбніца, про те що необхідна правда – це правда в усіх можливих світах. Р. Карнап розглядав поняття можливих світів в контексті істинності висловленого: фактичною, що реалізується у всіх можливих світах, й аналітичною, що існує в якомусь з можливих світів. На думку дослідника, можливі світи утворюються з певної кількості речень, які складаються з «атомарних речень», що пов’язують можливий світ із реальним, та відповідають стану справ реального світу [174].

Ще один новітній дослідник, фінський філософ Я. Гінтікка, розглядає можливий світ як «[…] можливий стан справ або можливий перебіг подій щодо суб’єкта, який перебуває в реальному світі та проєктує своє «Я» в інші ментальні світи» [129].

Загалом у XX столітті осмислення віртуальності вийшло за межі теології та онтології. Зокрема класики символічного інтеракціонізму (Дж. Мід, Ч. Кулі, У. Томас та ін.) зосередили увагу на розумінні віртуальної реальності як суб’єктивно створеного психологічного світу індивіда. Декларативною формулою цього напрямку є теорема Томаса, сформульована в соціологічній науці на початку XX століття: «Якщо люди визначають ситуацію як реальну, то вона реальна за своїми наслідками» [196]. На лекційному курсі в Чиказькому університеті колега У. Томаса Дж. Х. Мід зазначив: «Якщо річ не вважають істинною, то вона не функціонує як істинна в суспільстві» [182].

У теоремі Томаса наголошується не так на суті віртуального, скільки на його наслідках для реального світу та кожної людини. Психологічний аспект

поняття віртуальності означає, що світ конструюється та створюється відповідно до переконань спільноти. Так, джерелом віртуальності представники соціального інтеракціонізму Д. Г. Мід, Ч. Г. Кулі, Г. Блумер та ін. вважають людську психіку та розум.

П. Бергер та Т. Лукман у праці «Соціальне конструювання реальності. Трактат зі соціології знання» (1965) стверджували, що спільнота твориться в результаті наділення конкретних речей єдиним консенсусним значенням, що може бути «зчитане» іншими: «У житті кожного індивіда існує тимчасова послідовність його входження в орбіту соцієтальної діалектики. Відправною точкою цього процесу є інтерналізація: безпосереднє усвідомлення або інтерпретація об’єктивного факту як певного значення, тобто як прояву суб’єктивних процесів, що відбуваються з іншими, завдяки чому цей факт стає суб’єктивно значущим для мене самого» [15, с. 87]. Відтак згадані вчені розділили реальність на об’єктивну та суб’єктивну, що нерозривно взаємопов’язані. За їх твердженнями, інтеграція відбувається на двох рівнях. «По-перше, інституційний порядок у всій своїй цілісності повинен мати сенс для всіх учасників різних інституційних процесів […]. По-друге, все життя індивіда, що послідовно проходить різні стадії інституційного порядку, повинне бути суб’єктивно осмисленим. Інакше кажучи, індивідуальна біографія, з її послідовними інституційно зумовленими стадіями, повинна бути наділена сенсом, що надає суб’єктивну значущість всій цій біографії» [15, с. 62–63].

Суттєвого розвитку ідея віртуалізації набувала в посткласичній філософсько-культурологічній традиції. Саме віртуальний, штучно створений світ низка дослідників розглядає як віртуальну реальність, закінчене втілення стилю та настроїв Постмодерну.

Питання віртуалізації світу, політики та влади простежуються в концепції симуляції або створення гіперреальності, розробленій французьким мислителем Ж. Бодрійяром. У праці «Симулякри і симуляція» (1984) він висуває тезу про «втрату реальності» в постмодерністську еру, на зміну якій приходить

«гіперреальність». У ній знаки більше нічого не означають, а замикаються на самих собі, внаслідок чого перетворюються на симулякр. «Перехід від знаків, які щось приховують, до знаків, які приховують, що нічого немає, позначає рішучий поворот. Перші відсилають до теології істини та таємниці (до якої ще належить ідеологія). Другі відкривають еру симулякрів і симуляції, коли вже не існує Бога, аби розпізнати своїх, і Страшного суду, аби відділити хибне від істинного, реальне від його штучного воскресіння, бо все вже вмерло й воскресло завчасно» [19, с. 13], – пише Ж. Бодрійяр.

За Ж. Бодрійяром, симулякр – це знак, що набуває власного буття, творить свою реальність, і, по суті, перетворюється на віртуальний об’єкт. Виходячи з цього, виводиться визначення віртуальної реальності як організованого простору симулякрів: особливого світу кодів і заміщень, що суб’єктивно сприймається набагато реальніше, ніж сама реальність.

Ж. Бодрійяр стверджує, що процес віртуальності не тільки поглинув реальність, а й створив передумови для того, щоб реальність назавжди втратила можливість проявити себе: «Йдеться про субституцію, заміну реального знаками реального, тобто про операцію з попередження будь-якого реального процесу за допомогою його оперативної копії, метастабільного сигнального механізму, програмованого та бездоганного, що презентує всі знаки реального й оминає всі його несподівані повороти» [19, с. 7]. На противагу об’єктивно-наявній реальності, яка виражає цілісність, стабільність і завершеність, віртуальна реальність є джерелом відмінності та різноманіття, а тому більшою мірою наділена можливістю інноваційно-творчої, генеруючої, перетворюючої сили. Потреба у створенні ідеального, віртуального середовища завжди була притаманна людині й суспільству, втілювалася в тих чи інших соціально допустимих формах: театр, міф, релігія і т. д.

Аналіз віртуалізації держави простежується в працях Ж. Дельоза, Ж.-Ф. Ліотара, А. Турена, які аналізують віртуальне суспільство з позицій постмодерних підходів до вивчення політики. Вони наголошують, що віртуальному суспільству властиві такі ознаки: децентралізація, опора на

безпосередній досвід, відмова від претензій на єдине. Постмодерністська філософія руйнує класичні стереотипи сприйняття, перетворюючи реальний світ на віртуальний симулякр. У зв'язку з цим виникає спокуса створення «утопічно-деміургічних проєктів», що мають в основі розмитість межі між дійсним і віртуальним світами. Так, віртуальність набуває статусу не підконтрольної реальності структури, а, радше, навпаки, домінанти, яка здатна підкорювати реальність.

Важливими для осягнення сутності віртуальності є праці іншого французького постмодерніста – М. Фуко. Він детально проаналізував поняття дискурсу й дискурсивності як таких, що здатні через дисципліну творити суспільний порядок, не застосовуючи жодного насильства. У основоположній праці з дискурсивної теорії «Археологія знання» (1969) дослідник зазначає: «Дискурс – це тонка контактна поверхня, яка зближує мову і реальність, змішує лексику і досвід; я хотів показати на точних прикладах, що, аналізуючи дискурси, ми бачимо, як розпускаються тісні поєднання слів і речей і вивільняються сукупності правил, що обумовлюють дискурсивну практику. Ці правила визначають не німе існування реальності і не канонічне використання словників, а порядок об'єктів» [126]. Так, дискурс можна вважати віртуальним продуктом комунікативної практики, що вибирає одну з можливих реальностей, залежно від закономірностей свого творення.

Крім того, постмодерністи заклали важливе філософське підґрунтя для дослідження детериторіалізації. Йдеться передусім про Ж. Дельоза і Ф. Гваттарі [32; 33]. З позицій хронополітики вивчають мінливість території французький постмодерніст П. Віріліо [22; 23; 198] та вітчизняні політологи М. Андрущенко [5] та О. Якубін [145].

Аналізуючи віртуалізацію держави та інших політичних інститутів, доцільно звернутися до напрацювань комунікативної теорії. Інтенсивний розвиток комп'ютерних технологій в XX столітті, поява глобальної мережі Інтернет дали змогу застосувати поняття «віртуальна реальність» до нової інформаційно-технологічної сфери. Зокрема йдеться про розвиток

комунікативних технологій, так званий перехід від світу засобів масової інформації (ЗМІ) до світу засобів масової комунікації (ЗМК).

Старт систематичних досліджень, присвячених взаємодії політики зі ЗМК, відбувся ще на початку 1920-х років. Значний внесок у розробку теорії масової комунікації внесли Е. Бернейс [16], Г. Лассуелл [68], П. Лазарсфельд [177], В. Ліппман [70].

Для розвитку комунікативних досліджень важливою є праця В. Ліппмана «Громадська думка» (1929) [70], епіграфом до якої є уривок з Платонової «Держави», а саме міф про печеру. Так античне уявлення про світ ідей та світ речей перейшло до XX століття, і тут вже використовуються для опису не світу ідей та речей, а світу, що існує поза медіа, та світу, що існує в медіа. Як наочний приклад залежності людських уявлень від медіа, автор описує ситуацію життя на острові французів та англійців, які були з'єднані зі зовнішнім світом лише новинами, що приходили разом із пароплавом раз на два місяці. Коли в вересні 1914 року мешканці острова дочекалися пароплава, дізналися, що вже шість тижнів воюють, а їхні сусіди стали їхніми ворогами [70, с. 27]. Так стає очевидно: новини, інформація творить наше уявлення про реальність, що розташована за межами сприйняття конкретної людини. Тут важливо зважати на такі моменти, як викривлення інформації, цензура, маніпуляція, розсіювання уваги, стереотипне сприйняття. Саме від правильного сприйняття інформації залежить, якою буде реальність.

У межах комунікативних наук «віртуальним» називають той «псевдосвіт», який постає перед людиною на екрані монітора під час комп'ютерної гри або при «подорожі» мережею Інтернет. Цей термін також використовують в прив'язці до сфери цифрових, мультимедійних технологій і засобів електронної комунікації, що дають змогу штучно створювати віртуальну чи доповнену реальність.

В процесі вивчення взаємозв'язку, що існує між медіа і політикою, постає проблема медіатизації сфери політики загалом, яку досліджували Ф. Кротц [175], Н. Кулдрі [155], С. Х'ярвард [170], В. Шульц [181] та ін. У межах цієї

галузі дослідження виокремлюється також вивчення порядку денного, основними представниками цього напряму є К. і Дж. Ленг [176], М. Мак-Комбс.

Окремо потребує згадки класик комунікативістики – канадський учений М. Маклюен [74; 75]. Науковець аналізував, наскільки спосіб комунікації визначає зміст спілкування. Це вилилося в формулі «медіа – це повідомлення». Науковець доводив, що всякі технології виконують функцію доповнення та компенсації здатностей людського організму: «Якщо колесо – продовження ноги, то комп'ютер – продовження нашої нервової системи, яке існує завдяки зворотному зв'язку або «струму» [75, с. 63]. В результаті такого взаємозв'язку технології та мислення взаємозумовлені.

М. Маклюен зауважує, що алфавіт (письмо), уможливило вихід людини за межі групи і мислити себе самодостатньою одиницею. Врешті, завдяки такому виходу за межі групи, слово відірвалося від обставин мовлення, йому вдалося надати універсального значення, що не змінюється навіть на значних відстанях.

Але, з іншого боку, цей алфавіт обмежив людське мислення. М. Маклюен цитує В. фон Гумбольдта: «Людина поводиться зі своїми об'єктами здебільшого (або, можна сказати, виключно, оскільки її почуття і дії залежать від сприйняття) так, як вони їй дані в мові. У міру того як людина намагається висловити своє буття за допомогою мови, вона сама потрапляє в мовну пастку: будь-яка мова поміщає народ, якій вона належить, в магічне коло, і з нього не можна вибратися, хіба що вступивши в інше» [74, с. 46].

Завдяки алфавіту абстрактне, чуттєве мислення набуло раціональності та логічності. Внутрішній світ людини став таким, який можна висловити та зрозуміти, але й прив'язався до спільноти, що говорить тією ж мовою. Натомість комунікація, письмо, що відривається від своїх безпосередніх носіїв, впорядковує мислення всіх представників певної спільноти. І це перетворює світ на «глобальне село», де спілкування стає легким, доступним і зрозумілим для людей з різних куточків планети.

Зміни в тенденції сприймати та аналізувати інформацію М. Маклюен описує так: «Зараз, коли ми живемо в електричному середовищі та всередині закодованої інформації не тільки візуально, а й в сенсорному режимі, цілком природно, що у нас з'явилося нове сприйняття, яке руйнує монополію і пріоритет видимого світу, змушує цей давній світ виглядати таким же химерним, як середньовічний герб на дверях хімічної лабораторії» [75, с. 12]. Натомість у результаті поширення електричної комунікації весь світ перетворюється, на думку М. Маклюена, у «глобальне село», де тривалість доставляння повідомлення практично миттєва.

М. Маклюен звертається також до розробленого Т. де Шарденом та В. Вернадським концепту ноосфери. «Для людей писемної культури з їх критичним складом розуму гарячковість Т. де Шардена настільки ж малозрозуміла, як і його некритичний ентузіазм щодо космічної мембрани, яка замкнулася навколо земної кулі завдяки розширенню наших різних почуттів за допомогою електрики. Ця екстерналізація наших почуттів створює те, що Т. де Шарден називає «ноосферою», технологічним мозком світу. Замість того, щоб перетворитися в колосальну Александрійську бібліотеку, світ став комп'ютером, електронним мозком; це описували в науковій фантастиці. І в міру того, як наші почуття виходять назовні, Великий Брат проникає всередину» [74, с. 47].

Відтак внесок комунікативної науки у дослідження проблеми віртуалізації держави полягає в виведенні на міждисциплінарне поле досліджень понять комунікативної стратегії, ноосфери та порядку денного, медійних маніпуляцій та медіатехнологій, які впливають на спосіб взаємодії, мислення спільноти. Саме в межах комунікативних наук гостро постала необхідність стежити за чистотою ноосфери, як і біосфери, адже недбалість у цій сфері загрожує некерованими політичними маніпуляціями.

Зміни, які переживає світ у результаті розвитку технологій та перетворення індустріального світу на постіндустріальний, широко висвітлені в працях теоретиків інформаційного суспільства. Класики концепції

інформаційного суспільства (Е. Тоффлер [118], Д. Белл [14], М. Кастельс [56]) пояснили ті трансформації сучасного світу, які відбуваються під впливом еволюції інформаційних технологій, комунікативних мереж. Всі вони вважали сучасний світ (від середини XX століття) наступним етапом розвитку людства.

На початку 1970-х років американський соціолог Д. Белл розвиває ідею постіндустріального суспільства, що стала теоретичною моделлю економічного розвитку капіталістичних країн. У книзі «Прийдешнє постіндустріальне суспільство» (1973) науковець прогнозував можливі шляхи розвитку світу. На позначення цього майбутнього стану він використав ідею постіндустріального суспільства. «Постіндустріальне суспільство засноване на послугах. Тому воно – гра між людьми. Головне значення має вже не м'язова сила і не енергія, а інформація. Основною дійовою особою стає професіонал, тому що його освіта і досвід дають йому змогу відповідати всім вимогам постіндустріального суспільства. Якщо індустріальне суспільство визначається через кількість товарів, що визначає рівень життя, то постіндустріальне суспільство визначається якістю життя, що вимірюється послугами та різними зручностями – охороною здоров'я, освітою, відпочинком і культурою, – які стають бажаними та доступними кожному» [14, с. 172].

Ідея постіндустріального суспільства Д. Белла описує зміни передусім в економічній сфері, якій властиві: перехід від товарно-виробничої економіки до економіки послуг; домінування професійно-технічного класу; первинність теоретичного знання як джерела нововведень і політичних формулювань; орієнтація на майбутнє; створення нових «інтелектуальних технологій» тощо. При цьому Д. Белл зазначає, що індустріальне суспільство творить узгоджені дії машини та людини для виробництва продуктів. Вирішальним для організації рішень і спрямування змін стає теоретичне знання, що дає змогу розробити розумну технологію, завдяки якій вдасться робити точні передбачення.

Американський учений Е. Тоффлер у праці «Третя хвиля» (1980) обґрунтував концепцію «трьох хвиль», тобто трьох ключових етапів в історії планети, які зумовлені певними змінами у способі життя всього людства. До

настання Першої хвилі більшість людей жили усередині невеликих груп, що часто мігрували. Вони займалися збиральництвом, рибальством, полюванням або скотарством. Приблизно 10 тисяч років тому почалася сільськогосподарська революція, яка поступово поширилася планетою та цілком змінила спосіб життя (осілість, землеробство, створення традиційної сім'ї тощо). З кінця XVII століття в Європі відбувається індустріальна революція, що зумовило початок Другої хвилі планетарних змін (індустріалізація). Після закінчення Другої світової війни почалася Третя хвиля (постіндустріальна). Е. Тоффлер писав: «Я впевнений, що сьогодні ми стоїмо на порозі нової ери синтезу. У всіх галузях знань – від точних наук до соціології, психології та економіки, особливо економіки – ми, ймовірно, побачимо повернення до великомасштабного мислення, до узагальнювальної теорії, до складання частин знову в єдине ціле. Бо стає зрозумілим, що наше прагнення розглядати висмикнуті з контексту кількісні деталі при все точнішому дослідженні все дрібніших проблем призводить до того, що ми дізнаємося все більше про все менше» [118]. Необхідність цього синтезу, на відміну від аналізу, зумовлена, на думку вченого, зростанням потоків інформації, перед якими людина беззахисна. «Оскільки це середовище насичене змінами, то на нашу роботу, сім'ї, церкви, школи, політичні інститути впливає Третя хвиля інформації, але і море самої інформації теж змінюється… Зараз Третя хвиля радикально змінює все це. У міру прискорення змін в суспільстві змінюємося і ми. Нас наздоганяє нова інформація, і ми змушені постійно переглядати картотеку образів. Старі образи, які стосуються минулого життя, повинні замінюватися новими, інакше наші дії не відповідатимуть новій реальності, ми станемо більш некомпетентними» [118]. Інформація – основне багатство, основна небезпека та основна зброя для тих, хто живе в часи Третьої хвилі або постіндустріального суспільства.

Ідею інформаційного проникнення в усіх сфери життя продовжує розвивати американський учений М. Кастельс. Він також обґрунтовує думку про три революції в технологіях. До інформаційних технологій М. Кастельс

зараховує всі технології мікроелектроніки, створення обчислювальної техніки (машин і програмного забезпечення), телекомунікації/мовленні та оптико-електронної промисловості, генну інженерію тощо. У 1990-х роках біологія, електроніка та інформатика зближуються і взаємодіють у площині застосування, відкриття нових матеріалів, і в своєму концептуальному підході – навколо інформаційного ядра [56]. Науковець вважає, що навколо цього ядра інформаційних технологій в останні два десятиліття XX століття зосередилося «сузір'я» великих технологічних проривів в області нових матеріалів, джерел енергії, медицини, тощо. Сучасну зміну парадигми М. Кастельс вважає зсувом від технології, заснованих на дешевій енергії, до технологій, заснованих на дешевих потоках інформації, які уможливили успіхи в мікроелектроніці та телекомунікаційній технології. Науковець, аналізуючи нові види комунікації, зокрема розвиток Інтернету, виділяє «реальну віртуальність», як нову систему, що відбиває дійсність через віртуальні образи та власні закони. Через втрату довіри до традиційних медіа, саме віртуальні образи стають важелем політичного впливу, а також інструментом поширення влади політиків.

Японський учений Й. Масуда у працях «Комп'ютологія» (1966) та «Інформаційне суспільство як постіндустріальне суспільство» (1981) [180] відводив особливе місце інформаційним мережам в побудові інформаційного суспільства та визначенні напрямів його розвитку. Для вченого інформаційне суспільство – це інформатизація (комп'ютеризація) економічної та соціальної сфер діяльності держави. Більш того, він наголосив на особливій ролі інформації, технології і знань як ключових категорій в процесі переходу до постіндустріального суспільства. На думку Й. Масуди, прихована міць соціального перетворення – це кардинальне зростання кількості та якості інформації [28, с. 39].

Г. Рузавін [106] наголошує, що підхід до тлумачення віртуальності сформувався під впливом розвитку комп'ютерних та інформаційних технологій. Сучасні технічні засоби створюють умови для максимального «занурення» в віртуальну реальність, коли суб'єкт не в змозі розрізняти об'єкти

дійсного та віртуального світу. Хоча навколишній світ пізнається суб'єктом безпосередньо через його відчуттях, однак вони (відчуття) на цьому рівні не можуть бути помітними.

Відтак бачимо, що постіндустріальне суспільство проголосило інформацію та комунікацію основними ресурсами, забезпечивши необхідні та достатні умови для створення штучної, технічно-опосередкованої віртуальної реальності. Потенційні переваги інформаційних технологій, які стимулюють конкуренцію, сприяють розширенню виробництва, створюють і підтримують економічне зростання та зайнятість, мають значні перспективи.

Існування світового інформаційного суспільства констатовано на міжнародному нормативно-правовому рівні в «Окінавській хартії глобального інформаційного суспільства» (2000). У ній задекларовано, що інформаційно-комунікаційні технології є одним з найважливіших чинників, що впливають на формування суспільства XXI століття [89]. Ключовим напрямом розбудови інформаційного суспільства визначено: розробку інформаційних мереж, що забезпечують швидкий, надійний, безпечний і економічний доступ за допомогою конкурентних ринкових умов; розвиток людських ресурсів, здатних відповідати вимогам століття щодо інформації; за допомогою освіти і навчання задовольняти висхідний попит на фахівців в області інформаційних технологій в економіці; активне використання новітніх технологій у державному секторі і сприяння наданню в режимі реального часу адміністративних послуг, необхідних для підвищення рівня доступності влади для всіх громадян [89].

2003 року в Женеві, під час проведення першої зустрічі з питань інформаційного суспільства прийнято Декларацію принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті». Цей акт містить основні напрями для подальшого розвитку глобального інформаційного суспільства. Заявлено «[…] прагнення і рішучість побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати інформацію та знання, мати до них доступ, користуватися та обмінюватися ними, з тим, щоб

дати окремим особам, громадам і народам можливості повною мірою реалізувати свій потенціал, сприяючи своєму сталому розвитку і підвищуючи якість свого життя» [31]. Фактично згаданими вище двома документами право на інформацію прирівняно до інших фундаментальних прав і свобод людини.

Отже, згадані праці теоретиків інформаційного суспільства та нормативно-правові акти є важливою основою дослідження процесу віртуалізації держави, оскільки вони визначили роль технологічного розвитку в контексті суспільних перетворень. У них прослідкована взаємозалежність між технологіями, зокрема й інформаційними, та політикою, суспільним і приватним життям. Власне під впливом нескінченних потоків інформації нині й виникає віртуальна реальність.

До перших теоретичних спроб осмислення феномена віртуальної реальності з точки зору інформаційно-технічної спрямованості належить концепція М. Хайма. У праці «Метафізика віртуальної реальності» (1993) автор визначає віртуальність через поняття кіберпростору – ментальної карти інформаційних ландшафтів в пам’яті комп’ютера, що поєднана з програмним забезпеченням. Кіберпростір М. Хайм відносить до способів антропологізації інформації, необхідних для того, щоб людина могла у звичний спосіб оперувати даними як речами в реальності, але на віртуальному рівні, що дає можливість подолати наявну обмеженість реальності [60].

В теорії віртуального суспільства А. Бюля, представленій у його праці «Віртуальне суспільство. Економіка, політика і культура під знаком кіберпростору» (1997) [152], обґрунтовується, що з розвитком технологій віртуальної реальності комп’ютери перетворилися з обчислювальних машин на універсальні машини з виробництва «дзеркальних світів» – реальностей, в яких діють віртуальні аналоги.

Політичного забарвлення ідея віртуальності набуває з розвитком теорії глобалізації. З. Бауман описав зміни, яких зазнав сучасний світ на межі тисячоліть. Ці зміни, з одного боку, означають кінець тоталітаризму, з іншого – початок індивідуалізму. В праці «Плинні часи» (2000) автор аналізує, як на

початку XXI століття змінюється концепт свободи, ідентичності, приватного життя тощо. «Головними джерелами прибутку – особливо великого прибутку і завтрашнього капіталу – все більше стають ідеї, а не матеріальні об'єкти. Ідеї створюються тільки один раз і потім продовжують приносити багатство залежно від кількості споживачів, а не від числа людей, найнятих і зайнятих в процесі копіювання прототипу» [10, с. 163].

Ці думки доповнюють позиції У. Бека, висловлені в працях «Що таке глобалізація» (1997), «Космополітичне бачення» (2006), «Суспільство ризику» (2009). На його думку, глобалізація зумовлена, передусім, ризиками, з якими стикається сучасний світ – і ці ризики не залежать від кордонів національних держав; їх не під силу подолати жодній з держав поодинці. «Разом з промисловим виробництвом відбувається процес універсалізації загроз, незалежно від того, де ці загрози виникають: харчові ланцюги пов'язують практично всіх на Землі; вони не визнають кордонів. Вміст кислот в повітрі руйнує не тільки скульптури і витвори мистецтва, він вже давно знівелював сучасні митні бар'єри. Озера в Канаді теж містять кислоту, на північних краях Скандинавії теж вмирають ліси» [12]. На думку вченого, ця тенденція глобалізації породжує низку проблем.

Глобалізація, стрімкий технологічний процес, який супроводжується детериторіалізацією, зумовив універсальний характер постійного застосування новітніх інформаційних технологій у повсякденному житті. Зокрема у розвідках П. Віріліо («Втрачений вимір» (1991), «Машина бачення» (1994), «Чиста війна» (1997), «Стратегія обману» (2000)) наголошено, що сучасні інформаційно-комунікативні технології створили ефект «стиснення» світового простору-часу, основним політичним наслідком якого є зниження ролі простору та підвищення впливу чинника часу в політиці. Учений прогнозує песимістичну перспективу для всього людства: на місці реального міста, з чітким простором, з'являється місто віртуальне, метаполіс, позбавлений своєї території та готовий стати «юрисдикцією відверто тоталітарної чи навіть глобальної метрополітики» [145, с. 133].

Відзначимо, що процес детериторіалізації проаналізований у великій кількості наукових праць, зокрема А. Аппадураї [148], З. Баумана [10], Р. О'Бріна, Ф. Джеймсона, С. Елдена, К. Омае, М. Уотерса, Дж. Шольте та ін.

Досліджуючи внесок українських вчених у розробку ідеї віртуалізації держави, виділимо праці Г. Почепцова. Саме він один з перших в Україні почав досліджувати інформаційні протистояння, здійснюючи дослідження на межі політичної науки та комунікативної теорії. У праці «Революція.com. Основи протестної інженерії» (2005) [98] дослідник аналізує поняття віртуальної революції. «Віртуальні об'єкти людство активно використовує з метою стабілізації соціальної системи» [98, с. 357], – зазначає Г. Почепцов, акцентуючи на впливі віри та переконань на політичне життя.

Отже, ми простежуємо розвиток ідеї віртуальності та віртуалізації держави від Античності, коли Платон запропонував поділ реальності на світ речей та світ ідей. В Середньовіччі ідею віртуального розглядали в контексті метафізики та онтології, коли віртуальне виступало на позначення всіх можливих ознак і впливів певного об'єкта. Ідею віртуальності можна прослідкувати і в теорії можливих світів Г. Лейбніца. У XX столітті ідею віртуальності доповнили напрацювання таких теорії: соціального інтеракціонізму, що визначав реальність результатом людських переконань щодо того, що становить собою ця реальність; соціального конструкціонізму, за яким суспільне життя поділяється на суб'єктивне (особистісне) та об'єктивне (інституційне), що корелюють одне одного; постмодернізму, представники якого напрацювали ідею про симулякри (Ж. Бодрійяр), дискурс (М. Фуко) тощо.

Не менш важливими для дослідження проблеми віртуалізації держави стали здобутки теоретиків інформаційного суспільства (Д. Белла, Е. Тоффлера, М. Кастельса), адже вони артикулювали технологізацію сучасного життя як чинник якісних перетворень у всіх сферах, а також на відмінності сучасного способу життя від попередніх етапів розвитку спільноти.

Представники комунікативних наук доповнюють ідею віртуалізації поняттями медіатизації політики, медіавпливів, взаємозалежності ЗМІ та їхнього змісту (М. Маклюен). Розвиток теорій комунікацій, як і розвиток аналітичної філософії, постмодерних течій, символічного інтеракціонізму, семіотики та конструктивізму відіграли важливе значення у формуванні уявлень про віртуалізацію держави.

Завдяки розвитку теорії глобалізації стали очевидними процеси «розмивання» суверенітету, стирання кордонів, збільшення взаємозалежності світу, універсалізації проблеми та правил поведінки тощо. З. Бауман та У. Бек описали небезпеки та перспективи розвитку глобалізованого суспільства, в якому держава втрачає монополію на формування ідентичності.

1.2. Методологія дослідження віртуалізації держави

Однією з найцінніших для дослідження процесів віртуалізації держави, на нашу думку, є конструктивістська парадигма як постнекласична теорія пізнання політичної реальності. Соціальний конструктивізм відбиває культурну ситуацію (пост)сучасності, що характеризується розпадом ідеологічних і соціальних основ світогляду та життя людини.

Якщо звернутися до підходів, запропонованих представником радикального конструктивізму П. Ватцлавіком, то учений наголошував на плюралізмі реальностей, існуванні безлічі різних версій реальності, всі з яких є результатом комунікації. «Особливістю конструктивістського бачення реальності П. Ватцлавіком є поділ картини світу на реальність першого та другого порядку, які конструюються суб’єктом. „Перша реальність” пов’язана з фізичними, об’єктивними властивостями предметів і правильним сенсорним сприйняттям, здоровим глуздом, науковою верифікацією. „Друга реальність” – це смисловий і ціннісний атрибут цих предметів, що є результатом комунікаційних процесів, де в принципі не може бути ніяких об’єктивних, науково верифікованих істин. Іншими словами – перша реальність є світом

«голих фізичних фактів», друга – світом смислів і цінностей; «світи» відрізняються різною мірою їх усвідомленості» [120, с. 332].

Для розуміння особливостей віртуалізації держави значущі підходи представників соціального конструктивізму П. Бергера та Т. Лукмана. На їх переконання, об’єктивна реальність може бути легко «переведена» в суб’єктивну реальність, і навпаки. Мова стає головним засобом відбиття і поширення цього неперервного процесу переводу в обох напрямках. Відтак, якщо опиратися на теорію соціального конструювання П. Бергера та Т. Лукмана [15], віртуалізація держави є: 1) продуктом комунікації та спільної діяльності людей; соціально сконструйована реальність є динамічним процесом, знаходиться у постійному розвитку через інтерпретацію її індивідами та відтворюється у нових знаннях.

Держава та процеси її модернізації в межах конструктивістської парадигми постають дискурсивними конструктами, породженими і формами сприйняття масової повсякденної свідомості, соціально-політичних почуттів, і політичними технологіями. Відтак новий політичний порядок формується не лише завдяки результатам діяльності інститутів і соціальних груп, а й значною мірою завдяки різним дискурсам, що спрямовують соціально-політичні рефлексії в процесі соціальних інтеракцій.

Дослідження теоретико-методологічних основ віртуалізації держави зумовлює необхідність визначити основні поняття дисертації, зокрема поняття віртуального, віртуальної держави та віртуалізації держави.

Сучасна ідея віртуальності асоціюється з поняттям віртуальної реальності, що зумовлене поширенням комп’ютерних ігор та Інтернет-технологій. Ще в 1960-ті роки фахівці в галузі кібернетики почали розробляти систему, що інтегрує в єдиному інформаційному просторі зображення, звук і рух, назвавши її «штучною реальністю». «Батько» терміна віртуальна реальність – американський учений Дж. Ланьє – на початку 1980-х років заснував фірму, що випускала побутові комп’ютери з шоломом і рукавичкою, які давали змогу учасникові комп’ютерної гри зануритися в штучну реальність.

З початку 1990-х років терміном «віртуальна реальність» позначають специфічне середовище, створене за допомогою технічних засобів, найчастіше комп'ютера. Проте поняття віртуального не потрібно зводити лише до комп'ютеризації, воно має значно тривалішу історію та ширший спектр значень.

Слово «віртуальний» походить від латинського virtus – римляни вживали його для позначення таких рис воїна: мужність, хоробрість, рішучість. Нині ж англійське «virtus» означає доброчесність, чесноту [24]. Натомість латинське слово «virtualis» використовували для позначення «потенційний», «можливий», англійське «virtual» – фактичний, не номінальний, дійсний; французьке «virtuel» – можливий, потенційний. Так, навіть у дефініціях немає однозначності та простежується відмінність між словами «virtus» та «virtual». Тож поняття «віртуалізація» похідне від «віртуальний», яке, у свою чергу, означає з одного боку, фактичний, дійсний, а з іншого – можливий, гаданий, потенційний.

На переконання В. Афанасьєвої, категорії «віртуальність», «віртуальний» потрапили до суспільствознавчої лексики з механіки та фізики [7]. На уявленнях про віртуальні переміщення ґрунтується один з варіаційних принципів механіки – принцип можливих переміщень, що встановлює загальну умову рівноваги механічної системи [7]. Значення і користь принципу віртуальних переміщень для вирішення завдань механіки обґрунтував швейцарський математик І. Бернуллі; він і ужив слово «virtuel». Введене ще Г. Галілеєм поняття «virtus movens» буквально означало «здатність переміщувати». Зокрема в класичній механіці «віртуальний» – це аналог «можливого», низка можливостей, одна з яких за певних умов обов'язково перетворюється на реальність. Будь-яке реальне переміщення є реалізацією, втіленням одного з безлічі віртуальних [7].

Такий підхід до визначення віртуального простежується і в філософській традиції, зокрема онтологічних дискусіях, де реальний світ є лише одним з можливих. Отже, концепт віртуального не має єдиного трактування. Так, Г.

Рузавін тлумачить поняття «віртуальне» з позицій філософської науки як «те, що покладене в надчуттєву сутність і здатне реалізуватися; нематеріальний різновид буття об'єктивних сутностей або суб'єктивних образів» [106, с. 108–109]. За Г. Рузавіним, певний підхід до віртуальності сформувався під впливом розвитку комп'ютерних та інформаційних технологій. Сучасні технічні засоби створюють умови для максимального «занурення» у віртуальну реальність, коли суб'єкт не в змозі розрізняти об'єкти дійсного й віртуального світу. Віртуальна реальність характеризує стан свідомості, тому вона різниться від реальності об'єктивного світу.

А. Бюль віртуалізацією називає «процес заміщення за допомогою комп'ютерів реального простору як місця відтворення суспільства – простором віртуальним» [Цит за: 53, с. 9]. В. Сілаєва визначає віртуалізацію як «перехід основних видів діяльності в віртуальний простір мережі Інтернет» [111, с. 9], а О. Юхвід – «як властивість комп'ютерної реальності, що підтверджує володіння нею віртуальністю» [142]. На думку І. Свища, головний зміст віртуалізації вбачається в перенесенні наявних елементів культури, а також подальшого культурного виробництва, у цифрову форму з їх подальшим існуванням у сфері віртуальної реальності [107].

Так, вчені наголошують на технологічній (комп'ютерній) віртуалізації – тій, що стає можливою завдяки технологічним здобуткам XX–XIX століть. Проте існує й інша форма віртуальності – нетехнічна, а радше онтологічна. Віртуальність в онтологічному аспекті позиціюється як певний потенційний стан буття. Використовуючи такий підхід, віртуальність потрібно вивчати не лише як активний початок, а також як потенційну схильність до появи певних подій і станів, що можуть реалізуватися за відповідних умов.

За визначенням М. Носова, віртуальна реальність має низку властивостей неіманентного характеру, тобто вона не залежить ні від фізичної, ні від соціальної природи. Окрім того, у процесі віртуалізації набуваються нові властивості, котрі є наслідком застосування інформаційно-комунікаційних

технологій, що приховують у собі суб'єктність розробників програмного продукту [88, с. 96].

Відповідно, віртуальною реальністю можна вважати реальність можливу; умови, за яких вона проявляється, створені штучно – віртуальність замінює даність, підміняє реальність іншою, віртуальною, реальністю [111, с. 12].

Соціальні засади віртуалізації полягають у тому, що на ґрунті отриманих соціальних основ відбуваються перетворення у всіх сферах соціальної діяльності, зокрема й політичної. Головні зміни стосуються державної сфери, а саме формування нового типу держави під впливом інформаційно-комунікаційних технологій.

Вчення про віртуальні світи інституціоналізовані в межах науки віртуалістики. З її позицій всі інші світогляди (філософські, наукові та ін.) пов'язані виключно з константною реальністю. Отже, віртуалістика містить у собі константний світогляд як окремий випадок. Віртуальна модель може охоплювати необмежену кількість різних рівнів реальностей і одного й того самого типу, і різного типу, що дає змогу розробляти методи віртуального управління всередині однотипних реальностей і між різними ймовірними типами реальностей.

У «Маніфесті віртуалістики» (2001) [88] Н. Носов констатує: «Світ – віртуальний». «Віртуалістика вважає, що породжене наділене таким же статусом реальності й істинності, як і те, що породжує; що тимчасовість існування не робить подію менш істотною, ніж «начало», що її породило. Світ в цілому, як і будь-яка його частина, зображається таким, в якому події породжуються, діють, самі породжують інші події, вмирають або проникають в інші події і под. – і все це реально існує. Світ виходить багатошаровим, складним, непостійним, в якому весь час породжуються і вмирають його частини і навіть цілі прошарки. І все це істинно, оскільки існує; кожна частина існує на власних підставах. І немає обмежень ні «вгору», ні «вниз», ні «вшир», ні «вглиб» [88]. Н. Носов виділив ознаки віртуальної реальності: «Віртуальна реальність, незалежно від її «природи» (фізична, психологічна, соціальна,

біологічна, технічна та ін.), має такі властивості: зумовленість, актуальність, автономність, інтерактивність» [88].

Зумовленість означає, що віртуальна реальність твориться активністю всякої іншої реальності, зовнішньої щодо неї. Віртуальна реальність існує «тут і тепер», тільки поки активна реальність, що її породжує. Автономність передбачає, що в віртуальній реальності свої час, простір і закони існування (в кожної віртуальної реальності своя «природа»). Інтерактивність віртуальної реальності варто розуміти так, що вона може взаємодіяти з усіма іншими реальностями, зокрема і з тією, що її породжує, як онтологічно незалежна від них [88].

Такий підхід, щоправда, закріплює за віртуальною реальністю другорядну роль, залежну, яка зумовлена іншою, домінантною і зовнішньою реальністю. Натомість існує підхід, за яким віртуальна реальність розглядається радше як дискурс: змінивши віртуальність, реальність змінюється відповідно. Є й інші підходи, які акцентують на перевазі віртуальності над реальністю (йдеться про ідеологів кібердержави).

Можна констатувати: ідея віртуальної реальності в політичну науку проникла з інших наук, зокрема технічних. Вона позначає можливість існування інших, альтернативних, варіантів дійсності – чи то у свідомості громадян, чи то в інформаційному просторі, чи в умовах, спеціально створених технологічними засобами.

З огляду на такий підхід, віртуалізацію можна розглядати на кількох рівнях – і як комп’ютерну, і як некомп’ютерну (символічну). Остання полягає у тому, що на ґрунті соціальної комунікації відбуваються перетворення в усіх сферах соціальної діяльності, зокрема й політичної. Ця віртуальність може породжуватися в індивідуальній чи колективній психіці, ідеологіями та іншими формами продукування та поширення символів. Власне вона є предметом вивчення політичної науки. Натомість технологічна (комп’ютерна) віртуалістика розглядає трансформацію суспільства як перенесення основних видів діяльності у простір мережі Інтернет (цифрова держава, «держава у

смартфоні»). Серед численних причин поширення ідеї віртуалізації держави, вкажемо на перетворення більшості ЗМК на цифрові.

Ідея віртуалізації держави пов’язана з теорією медіатизації. Медіатизація розглядається, з одного боку, як процес впливу медіа на суспільство і на соціальні інститути, з іншого, – як сукупність технологій і ресурсів, пов’язаних з інформаційно-технологічним розвитком суспільства (нові медіа, мобільні телефони, оптико-волоконні мережі та ін.) [28, с. 3].

В межах медіатизації суспільства відбувається медіатизація політики – своєрідний процес інтеграції політичного простору та медійної сфери, в результаті чого відбувається взаємна трансформація політичного дискурсу та медіа-дискурсу. Медіа виступають тими фільтрами, які сортують інформацію, транслюючи образи реальності за умови недоступності об’єктів, з якими суспільство не має справи в повсякденні. Медіа створюють простір, де зміст політики розкривається через компоненти політичної символізації (символи, образи, знаки, презентації тощо), паралельно вибудовуючи образно-смислову віртуальну проєкцію політики [28, с. 3].

У комунікативістиці відсутнє єдине визначення поняття «медіатизація». Сформувалися два основні підходи до трактування цього поняття, запропоновані А. Геппом: інституційний та соціально-конструктивістський. За інституційним підходом (Дж. Маццолені, В. Шульц, С. Х’ярвард), медіатизація – це процес, в якому соціальні інститути (не пов’язані з медіа) повинні адаптуватися до медійної логіки. В рамках інституційного підходу: по-перше, наголошується на автономії ЗМІ щодо політики; по-друге, констатується зростання впливу медійної логіки на політичну сферу, а саме необхідність політичних акторів адаптуватися до внутрішніх настанов функціонування мас-медіа сегмента [28, с. 25–26]. У цьому контексті медіалогіка розглядається як організаційне, технологічне та естетичне функціонування, зокрема і способи, якими ЗМІ розподіляють матеріальні та символічні ресурси та роботу через формальні та неформальні правила [155].

Представники соціально-конструктивістського підходу (Н. Коулдрі, Ф. Кротц, А. Гепп) визначають медіатизацію як процес, в якому обмін інформацією та інформаційно-комунікаційними технологіями впливають на комунікативні структури суспільства. Н. Коулдрі розглядає медіатизацію як нову форму соціалізації суспільства через поширення інформаційно-комунікативних технологій та інформації. У. Ліппман одним із перших виявив процес медіатизації, а саме розрив між медійної картиною, яка транслюється ЗМІ, і безпосередньою реальністю, яка формується на основі власного досвіду людини [155].

Важливо наголосити на відмінності понять «медіація» та «медіатизація». Медіація позначає радше нейтральну взаємодію медіа з соціально-політичними áкторами. Натомість медіатизація – це спеціальне підлаштування певних сфер логіці медіа [154].

Медіатизація як така не є безпосереднім об’єктом дослідження, проте розуміння її частиною процесу віртуалізації держави необхідне для виконання завдань дисертації. Отож, медіатизація позначає тісне переплетення сфер політики та медіа, де медіа виконують радше панівну роль, підкоряючи політику своїм правилам функціонування. Медіа перебирають все більше політичних функцій передусім легітимізації, формування ідентичності, створення порядку денного тощо. Ці зміни мають не лише функціональні наслідки, а й структурні, адже певні частини політичної системи повинні змінюватися з огляду на існування медіа.

Зв’язок віртуальності та медіа помічає і Г. Почепцов: «Інтернет створив нові можливості для віртуального впливу. Можливо, кожен тип віртуальності, зв’язаний з домінуванням того чи іншого каналу, давав свої варіанти соціальних, політичних чи воєнних наслідків. Книга формує свою віртуальність, кіно – свою, телебачення – свою. Довоєнний розвиток кіноіндустрії сформував тоталітарне суспільство, оскільки і німецьке, і радянське кіно реально були частиною політики, а не мистецтва. Телебачення створило ефект Сі-ен-ен, і під впливом телебачення доводилося завершувати

або суттєво коректувати дії військових (В'єтнам, Сомалі). Сьогодні час Інтернету, що породив різноманітні мережеві структури. Варто повторити за М. Маклюеном, злегка змінивши його думку, що канал – це «не тільки передача, а й інший тип мислення» [98, с. 357].

Медіалогіку можна прослідкувати і на поширенні так званої віртуальної революції, коли ЗМІ стають основним чинником масових протестів в межах новітніх держав у різних регіонах планети. Свідченням зсуву до символічної революції Г. Почепцов вважає успішність оксамитових революцій в кінці XX століття – на початку XXI століття. Так, Г. Почепцов розглядає віртуальну революцію як набір певних віртуальних дестабілізаторів. Серед них: жертва (як індивідуальна, так і колективна); масовість і видовищність протесту (зазвичай народний неспокій пропонує стерти старі правила і можливість створення нових); обов'язкова участь молоді; залученість міжнародного інформаційного потоку для зворотної циркуляції в країну і створення відповідного міжнародного тиску; наявність глядача, адже без контролю всі ці дії не мають сенсу, а в глядача починає руйнуватися наявна модель світу, що, ймовірно, і становить собою мету таких дій; певна часова залежність, оскільки звикання до ситуації знімає її «гарячий» характер, щоб не виникла ідеологія спротиву [98, с. 360–361]. У цьому контексті віртуалізація виступає результатом поширення символів, що циркулюють в медіа.

Віртуальність пов'язана з поняттям дискурсивності. Дискурсивність, за М. Фуко, творить дисципліну, тобто гарантує дотримання певного порядку за умов добровільного підкорення, тобто без участі всякого насильства. «Якщо система виконання покарання в найсуворіших її формах вже не звернена на тіло, тоді за що ж вона чіпляється? Відповідь теоретиків проста, майже очевидна. Якщо не тіло, то душа. Спокута, яка колись мучила тіло, має бути замінена покаранням, що діє на глибині, – на серце, думки, волю, здібності. Маблі сформулював цей принцип раз і назавжди: „Покарання, скажемо так, повинно вражати радше душу, ніж тіло"» [127].

Проте, на думку З. Баумана, такий підхід вичерпав себе з появою та набуттям великих масштабів глобалізаційних процесів. Учений зауважує, що М. Фуко використовував проєкт паноптикуму Й. Бентама як метафору сучасної влади. У паноптикумі мешканці були прикуті до свого місця, позбавлені можливості рухатися, замкнені за товстими стінами та прив'язані до своїх ліжок або робочих місць. На думку З. Баумана, секрет влади господарів полягав у владі над часом. Це була основна стратегія здійснення їх влади. Паноптикум був моделлю взаємних зобов'язань і конфронтації між двома сторонами відносин влади. Але паноптикум має недоліки. «Це дорога стратегія: завоювання простору і прихильність до нього, а також утримання людей, за якими спостерігають, вимагають великих затрат [10, с. 16–17].

Але зараз влада може переміщатися зі швидкістю електронного сигналу; час, необхідний для переміщення її основних складників, зменшився до миті. Практично влада стала дійсно екстериторіальною; вона не сповільнюється в результаті просторового опору. «Більше немає значення, де перебуває людина, що віддає команди, – відмінність між «поруч» і «далеко» анульована [10, с. 16–17]. Так, на думку З. Баумана, можна позбутися незручних і дратівливих аспектів техніки влади.

В паноптикумі було важливо, щоб відповідальні люди завжди були «на місці», поблизу, на контрольно-диспетчерському пункті. У постпаноптичних відносинах владі необхідно, щоб люди, які використовують управлінські важелі, могли в будь-який момент опинитися за межами досяжності – бути цілком недоступними. Ідея паноптикуму та його критика все ж стверджують одне: в державі навчилися контролювати «душу» спільноти передусім завдяки дискурсивним стратегіям, що поширюються з допомогою медіа.

Отже, ідея віртуалізації означає, що в умовах поширення медіа, технологій, поглиблення процесів глобалізації та світової пов'язаності, а також за умов дискурсивного впливу, який здійснюють суб'єкти влади, певну реальність можна мислити як одну з можливих і як таку, яку можна змінити, вплинувши на свідомість людей чи то з допомогою медіа, чи то іншими

дискурсивними методами. При цьому, глобалізацію варто розглядати як процес розмивання кордонів та поглиблення взаємозалежності між країнами з огляду на розвиток демократії, економічний поступ та світові загрози.

Окрім того, процес медіатизації може означати включення певного явища до інформаційного простору. За визначенням ЮНЕСКО, інформація – це «універсальна субстанція, що пронизує усі сфери людської діяльності, слугує провідником знань і думок, інструментом спілкування, взаєморозуміння та співробітництва, утвердження стереотипів мислення, поведінки» [143]. Д. Робертсон називає інформацію «сучасною цивілізацією», адже «інформаційні ресурси визначають цивілізацію більше, ніж фізичні чинники» [191].

Інформаційний простір дає змогу «зробити суспільним надбанням […] системе знань окремих осіб і колективів. Це ставить перед суспільством фундаментальну культурологічну задачу – інтеграцію знань, що дозволяє використовувати в практичній діяльності весь досвід людства, а не протиставляти одне одному фрагменти знань, що накопичені в різних культурах» [140].

На думку О. Сєрьогіна, в інформаційній сфері присутня інтелектуальна складова, що стає не тільки домінантою трудової діяльності, але і якісно перетворює простір вільного часу, розширюючи діапазон інтересів і можливостей самореалізації людини та соціуму як у реальному світі, так і в його віртуальному вимірі. Віртуальний світ – це своєрідне відбиття та вияв законів об’єктивної дійсності, а «віртуальна культура» далеко не завжди є антагоністом національній культурі, стаючи іноді її «заломленням» [110, с. 63].

На думку А. Манойла, інформаційний простір – це сукупність суб’єктів інформаційної взаємодії чи впливу; інформації, призначеної для використання суб’єктами інформаційної сфери; інформаційної інфраструктури, що забезпечує можливість обміну між суб’єктами; суспільних відносин, котрі формуються як наслідок утворення, передачі, розповсюдження та зберігання інформації, обміну інформацією всередині суспільства [77, с. 73]. А Л. Біловус зазначає: в центрі інформаційного простору стоїть суб’єкт, який створює, накопичує,

передає, зберігає інформацію – всі, хто використовують можливості сучасних інформаційних технологій. Інформаційний простір позбувся усіх обмежень, властивих фізичному простору (державні кордони, океани, велика відстань тощо) [18, с. 189]. Проте, на думку вченої, цей простір має й певні обмеження, пов'язані з державною чи військовою таємницею, правом на недоторканність приватного життя, – так звані конвенціональні межі [18, с. 189]. Сьогодні інформаційний простір держави – один із пріоритетів сучасної держави [114].

Крім поширення медіа та проникнення їх у всі сфери політичного життя (медіатизації) та зміни правил переміщення в площині планети (перехід до постпаноптичної системи), відбувається інший процес – встановлення та порушення загальних для всіх правил, які в публічному дискурсі називають «світовим порядком» або, відповідно, «світовим безладом».

«Порядок», за З. Бауманом, означає монотонність, регулярність, повторюваність і передбачуваність. «Ми називаємо щось впорядкованим, якщо ймовірність деяких подій значно перевищує ймовірність їх альтернативних варіантів, при цьому малоймовірні події взагалі не розглядаються або опускаються. Крім того, порядок означає, що якась персоніфікована або Вища Істота впливає на цю ймовірність, може маніпулювати нею та забезпечувати перевагу певним подіям, виводячи їх з розряду випадкових» [10, с. 62–63], – зазначає З. Бауман у праці «Плинні часи» (2000).

Віртуалізація (як комп'ютерна, так і символічна) видозмінює інститут держави. Одним з небагатьох міжнародних документів, який визначає ознаки держави, є Конвенція Монтевідео (Конвенція про права та обов'язки держави) [184], підписана 1933 року. У документі визначається, що держава повинна володіти такими ознаками: а) постійне населення; б) визначена територія; в) уряд; г) здатність вступати в відносини з іншими державами [184]. Ці чотири ознаки ми візьмемо за основу для нашого дослідження і будемо розглядати віртуалізацію держави як інституту, наділеного постійним населенням, визначеною територією, урядом та здатністю вступати у відносини з іншими державами. Водночас не можна упустити те, що Конвенція Монтевідео не

визначає серед основних ознак держави такі, як суверенітет і громадянство. Ми не можемо ігнорувати їх фундаментальне значення в системі ознак держави. Відтак, у нашому аналізі ми звертатимемося й до цих фундаменальних ознак держави, позаяк процеси віртуалізації істотно модифікують і їх.

Зауважимо, що віртуальними також називають держави, які не відповідають всім ознакам міжнародного правосуб'єкта [20; 125]. Такими називають невизнані держави або ті, що існують лише в кіберпросторі. Поява таких акторів є результатом розвитку Інтернету та інших інформаційно-комунікаційних технологій. Віртуальна держава у цьому розумінні – це загальна назва для будь-яких утворень, які заявляють про свою державність, але не є державами по суті і лише імітують певні їхні риси [125]. Кібердержави офіційно не визнаються світовою спільнотою і не сприймаються серйозно країнами, на території яких створені [20].

Прикладом віртуальної держави є Князівство Сіландія, розташоване в нейтральних водах Північного моря неподалік Великої Британії на платформі Форт-Роуз, спорудженій в роки Другої світової війни для захисту від німецьких бомбардувальників. Після закінчення військових дій Форт-Роуз практично не постраждав. 1966 року майор британської армії у відставці П. Р. Бейтс вибрав платформу для своєї незалежної радіостанції «Britain's Better Music Station», а 1967 року оголосив про створення суверенної держави Сіландія і проголосив себе князем Роєм I [20]. Через кілька років уряд Сіландії прийняв Основний закон князівства, розробив такі державні атрибути, як прапор, герб і гімн.

Інший приклад віртуальної держави – Інтернет-держава Віртландія [201], заснована 14.08.2008 року. Вона демонструє, як віртуальна держава може бути цілком позбавлена власної території. Держава Віртландія існує лише в межах інформаційного простору. «Оскільки традиційне самопроголошення держави зазвичай формується шляхом відділення від іншої держави, то територіальне питання завжди є головною причиною суперечки між ними. Віртландський суверенітет не ґрунтується на сепаратизмі. Віртландія не претендує на будь-яку територію, що належить іншій державі. Віртландія – це країна, що виходить за

межі наявних державних кордонів, не порушуючи та не обмежуючи суверенітету жодної держави» [201], зазначено на офіційному сайті Віртландії (http://www.wirtland.com/).

Це лише два приклади держав, які з огляду на невідповідність умовам Конвенції Монтевідео, можна вважати віртуальними або кібердержавами. При цьому зазначимо, що віртуальними також деякі вчені називають ті держави, які не здобули міжнародного визнання, як синонім до «невизнаних держав» [109], хоч і факт визнання не є обов'язковою ознакою для створення держави, бо не перечислений серед чотирьох обов'язкових ознак держави. Громадянином більшості віртуальних держав можна стати в режимі онлайн: всякий охочий має можливість отримати громадянство кібердержави, зареєструвавшись на офіційному сайті.

Основна мета дисертації не полягає в аналізі процесу становлення віртуальних держав, а також не в описі всіх можливих форм технологічних заміщень державних функцій. Наша мета – продемонструвати, як за умов глобалізації, медіатизації, детериторіалізації новітні держави змінюють принципи й механізми свого функціонування. Наведені вище приклади квазідержав – це лише крайній вияв трансформації інституту держави, адже сучасні держави ще неможливо мислити в контексті відсутності території на карті, невизнання міжнародною спільнотою тощо. Ми не будемо аналізувати механізми втрати чи обмеження правосуб'єктності. Процеси віртуалізації, що стали предметом нашого дослідження, позначають тенденцію до перетворення держав як повноцінних суб'єктів міжнародного права, що відбуваються в умовах глобалізації, детериторіалізації, медіатизації, символізації політики: йдеться про розмивання державного суверенітету та визначеної території, вибірковість громадянства, переосмислення поняття легітимного насильства тощо.

Важливим у цьому контексті є зокрема підхід В. Штепа, що стверджує: від звичайної держави віртуальна різниться тим, що центр її влади та суспільного життя, як і джерело суверенітету, перебувають у віртуальному

просторі, отже – ніде [141, с. 74]. Інші дослідники пропонують використовувати термін «віртуальна держава» (virtual state) для акцентування на технологічних перетвореннях усієї інфраструктури усіх гілок влади. Ці перетворення відбуваються внаслідок запровадження економіки знань, використання ІКТ у системі державного управління. Відтак Інтернет стає каналом для соціально-політичної взаємодії держави та суспільства.

Політолог Н. Хома вважає за доцільне розмежувати віртуальну (цифрову) державу (центр влади держави та суспільного життя, а також джерело суверенітету перебувають у віртуальному просторі, у так званій «хмарі»; саме у цьому полягає особливість держави) і кібердержаву – тип е-держави (її еволюційна форма), котра дає змогу будь-кому з дієздатних осіб стати е-резидентом цієї держави (для доступу до низки базових послуг е-держави через ID-карту, що допомагає здійснювати дистанційні операції з використанням електронного підпису) [131, с. 65].

Прибічником розвитку кібердержави виступив Дж. П. Барлоу. 1996 року вчений став автором «Декларації незалежності кіберпростору», в якій стверджував: кіберпростір – явище природне, і суспільство сприяє його розвитку власними колективними діями. Згадана Декларація з’явилась як певний виклик державам, що вже існують. У ній автор постулює створення нового (альтернативного державному) простору, який має творитися на засадах рівності. «Ми створюємо світ, в якому всі можуть діяти без привілеїв чи упереджень, породжених расовими відмінностями, економічною владою, військовою силою або місцем народження. Ми створюємо світ, де будь-хто і всюди може виражати свої переконання, незалежно від того, наскільки він незвичайний, без страху, що його заставлять мовчати або вдаватися до конформізму. Ваші правові концепції власності, вираження, індивідуальності, переміщення неможливо застосувати до нас. Вони базуються на матеріальності, але тут немає матеріальності» [149].

У Декларації Дж. Барлоу впевнено звертається до урядів держав, що жоден з них не має впливу на кіберпростір: «Ви стверджуєте, що у нас є

проблеми, які ви повинні вирішити. Ви цим виправдовуєтеся, щоб вдертися в наші володіння. Багатьох з цих проблем просто не існує. Реальні конфлікти, правопорушення ми будемо виявляти власними силами. Ми формуємо наш власний Суспільний договір. Таке управління виникне за умовами нашого світу, не вашого. Наш світ інший. Кіберпростір складається з трансакцій, зв'язків і безпосередніх думок, вбудованих стоячою хвилею в павутину наших комунікацій. Це наш світ, який усюди і ніде, але він не там, де живуть тілесні істоти. Наші індивідуальності не тілесні, так що, на відміну від вас, ми не можемо добиватися порядку через фізичний примус» [149], – йдеться в Декларації.

Отже, розуміння ідеї кібердержави – різноманітне, її можна трактувати як всяку державу, що певною мірою існує в інформаційному просторі, так й альтернативу сучасному світопорядку, навіть ідеологічну незгоду з функціонуванням класичної держави.

На державному рівні, розробляючи нормативно-правові акти, законодавці все ж керуються тим підходом, що кіберпростір повинен перейти під контроль держави, а не протиставлятися їй. За Законом України «Про основні засади забезпечення кібербезпеки України» кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [50]. Але, на думку українського дослідника О. Дубова, на 2013 рік жодного концептуального розуміння поняття «кібер» в Україні ще не було сформульовано [39].

У дослідженні «Кібермогутність і національна безпека» звернено увагу на те, що зміст концепту «кібер» може бути визначений багатьма способами. Один зі співавторів дослідження, Д. Куел, присвятив окремий розділ роботи саме визначенню термінології та навів щонайменше 28 визначень кіберпростору. У результаті він запропонував визначити поняття як «операційний домен,

обмежений використанням електроніки та електромагнітним спектром для створення, збереження, зміни, обміну та використання інформації у взаємопов'язаних та інтернетизованих інформаційних системах та пов'язаній з ними інфраструктурі» [39, с. 71; 162, с. 4].

Сьогодні ці два конструкти – держава і кіберпростір – тісно переплетені. Створення кіберпростору можна вважати наслідком інформаційної революції, а в результаті медіатизації та глобалізації він не вільний від традиційної політики. Взаємопроникнення держави та кіберпростору виявляються в процесах створення електронного уряду (electronic government, e-Government, e-gov, digital government, online government) і криптоанархії (cryptoanarchy).

Зазначимо, що термін «електронний уряд» з'явився наприкінці 1990-х років, але історію комп'ютеризації в державних організаціях можна простежити з початку комп'ютерної історії, принаймні, з 1970-х років, в текстах, де аналізують використання інформаційних технологій на урядовому рівні [158].

Аби захистити державу в умовах її злиття з кіберпростором, у законодавстві розробили ідею критичної інфраструктури. Поняття «критична інфраструктура» визначене в українському законодавстві як сукупність об'єктів інфраструктури держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку та оборону, природне середовище, призвести до значних фінансових збитків та людських жертв [96]. При цьому об'єкти критичної інфраструктури позначають сукупність підприємств та установ (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що стратегічно важливі для функціонування економіки і безпеки держави, суспільства та особи [96]. Тобто виведення з ладу або руйнування цих об'єктів може мати вплив на національну безпеку та оборону, довкілля, зумовити значні матеріальні та фінансові збитки, людські жертви [185, с. 2].

В разі занесення підприємства до переліку об’єктів критичної інфраструктури (який формують органи виконавчої влади), відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», його власники або керівники відповідальні за забезпечення кіберзахисту комунікаційних систем і захист технологічної інформації [92].

Так, визначивши поняття віртуального (процес усвідомлення певного явища чи факту як одного з можливих варіантів, який породжує та є продуктом іншого, зовнішнього щодо нього явища, і становить собою лише одну з альтернатив, які зароджуються в дискурсі) та держави (інституту, наділеного чотирма ознаками – постійним населенням, визначеною територією, урядом та здатністю взаємодіяти з іншими державами), потрібно з’ясувати сутність віртуалізації держави.

З огляду на вище викладене, процесом віртуалізації держави варто вважати перенесення всіх основних ознак та функцій держави до інформаційного простору (кіберпростору) і тій чи іншій мірі, в результаті чого національна держава, що вважалася нормою впродовж XX століття, є однією з можливих форм цього інституту, проте не єдиною. Ці перетворення відбуваються з огляду на процеси включення держави до кіберпростору, в якому існують свої правила, відмінні від тих, що застосовуються до класичних міждержавних взаємодій. Передусім відмінність цих правил зумовлена відсутністю кордонів у кіберпросторі, швидкістю переміщення інформаційних даних і загальною доступністю інформації, а також її вразливістю до маніпуляцій і злочинних дій.

Держава, що має постійне населення, що проживає на визначеній території, і є джерелом легітимності влади державних органів, котрі представляють державу на міжнародній арені, нині зазнає модифікацій. Вони зумовлені передусім технологічними перетвореннями сучасного світу, що змушують державу поширювати свою юрисдикцію не лише на реально визначену територію, а й на інформаційний простір, де вона ще мусить відстояти право на своє існування. Процес віртуалізації держави позначає як

можливості, так і небезпеки зникнення її в тій формі, в якій заведено мислити державу (часто національну державу) в сучасній науці. А, відповідно, віртуалізація – це і процес боротьби держави за своє виживання.

Визначити процес віртуалізації держави можна з огляду на різні модифікації основних чотирьох ознак, визначених Конвенцією Монтевідео. Так, держава може бути інститутом, не наділеним постійним населенням, тобто без тих, хто проживають на її території тривалий час і мають національну ідентичність.

Методологію нашого дослідження становить синтез двох підходів: інституційного і комунікативного. Завдяки інституційному підходові аналізуватимуться перетворення держави як інституту на рівні її основних ознак, визначених Конвенцією Монтевідео. Комунікативний підхід дасть змогу поєднати теорію глобалізації, постмодерного символічного обміну та домінування дискурсу, що є під час поширення державної юрисдикції на кіберпростір, а також аналізувати інформаційні війни як новітню форму взаємин між державами в умовах інформаційного суспільства.

В межах інституційного підходу аналізуватимуться стратегії кібербезпеки США (2018), ФРН (2016), Польщі (2017) та України (2016). Країни були обрані об’єктами дослідження, бо кожна з них відіграє провідну роль у глобальному (США), регіональному (ФРН у межах ЄС) та субрегіональному (Польща на теренах Центрально-Східної Європи) масштабах. Крім того, всі вони впродовж 2016–2018 років напрацювали національні стратегії кібербезпеки. Дослідження документів, їх порівняння та зіставлення з основними принципами віртуалізації держави дасть змогу зрозуміти, в якій з ознак держави відбуваються найсуттєвіші зміни під впливом технологій та інформаційної революції – у сфері взаємодії з громадянами, територією, перетворення урядових механізмів дії чи у відносинах з іноземними гравцями.

Зазвичай кібербезпека стосується заходів і дій, спрямованих на захист кіберпростору в цивільній і військовій сферах від загроз, які можуть завдати шкоди взаємозалежним мережам та інформаційній інфраструктурі або є

пов’язаними з ними. Кібербезпека спрямована на збереження доступності та цілісності мереж та інфраструктури, а також конфіденційності інформації, яка міститься в них [103]. Українське законодавство визначає кібербезпеку як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі [50].

Важливу функцію забезпечення кібербезпеки виконують провайдери, постачальники сервісів. Вони отримують технічну можливість керувати інформацією та транзитом потоку даних (інтернет-трафіку) через мережі [90].

У другому розділі ми проаналізуємо виміри віртуалізації на чотирьох рівнях державних ознак – постійне населення, визначена територія, наявність уряду та здатність взаємодіяти на міжнародній арені. У третьому розділі ми проаналізуємо наявність ознак віртуалізації держави в стратегіях кібербезпеки США, ФРН та Польщі. У четвертому розділі дисертації аналізуватиметься Стратегія кібербезпеки України, введена в дію 16.03.2016 р. У дослідженні ми розглянемо положення цієї Стратегії, а також інших нормативно-правових актів, що стосуються забезпечення кібербезпеки в Україні та були прийняті у 2014–2019 роках.

Дослідження основних напрямів діяльності держави в кіберпросторі дасть змогу здійснити компаративний аналіз рівня віртуалізації, який буде зорієнтований на порівняння української практики в цифровому просторі та діяльністю її міжнародних партнерів. Дослідження актуальне з огляду й на те, що Україна перебуває в конфлікті з Російською Федерацією, яку 2018 року офіційно визнала агресором [51]. А перебування й в інформаційному протистоянні дає підстави та матеріал для дослідження перетворень у сфері кібербезпеки в Україні.

З допомогою кількісного контент-аналізу буде підраховано кількість використання конкретних лексичних одиниць у текстах досліджуваних

стратегій кібербезпеки. Для прикладу, одиницею дослідження буде слово «національний» («national», що присутнє в усіх англійських та німецькомовному варіанті документів). Порівняння кількісних даних дасть змогу дійти об'єктивних висновків про тенденції в процесі віртуалізації держави. Так інституційний підхід дасть змогу розглядати державу як сукупність правил, дотримання яких уможливлює її функціонування. Це правила і всередині встановлених кордонів, і на міжнародній арені, і в інформаційній сфері.

Висновки до розділу 1.

1. Доведено, що еволюція ідеї віртуальності та віртуалізації держави простежується від Античності, коли Платон запропонував поділ реальності на світ речей та світ ідей. Відтоді, зокрема у Середньовіччі, ідею віртуального розглядали в контексті метафізики та онтології: віртуальне виступало позначенням усеможливих ознак і впливів певного об'єкта. Подальша еволюція ідеї віртуальності прослідкована в теорії можливих світів (Г. Лейбніц).

У XX столітті ідею віртуальності доповнили напрацювання: 1) теорії соціального інтеракціонізму, який визначив реальність результатом людських переконань щодо того, чим є ця реальність; 2) соціального конструктивізму, за яким суспільне життя поділяється на суб'єктивне (особистісне) й об'єктивне (інституційне), що корелюють одне одного; 3) постмодернізму, представники якого напрацювали концепції симулякрів (Ж. Бодрійяр), дискурсу (М. Фуко); це уможливило перенесення дискусії щодо результатів функціонування текстів у площину дискусій про віртуальність. Підґрунтям дослідження віртуалізації держави визначено й праці теоретиків інформаційного суспільства (Д. Белл, Е. Тоффлер та ін.), представників комунікативних наук (М. Маклюен, Н. Луман, В. Ліппман та ін.), теорії глобалізації (З. Бауман, У. Бек та ін.).

Віртуалізація розглядається на технологічному (комп'ютерному) та символічному рівнях: а) комп'ютерна віртуалізація розглядає трансформацію держави як перенесення основних видів діяльності у вимір Інтернету (цифрова

держава, «держава у смартфоні»); б) символічна віртуалізація полягає у перетворенні всіх сфер діяльності держави через різноманітні форми продукування та поширення соціально-політичних символів.

2. Викладено розуміння віртуальної держави як сучасного політичного інституту. Віртуалізація держави відбувається як на технологічному, так і на онтологічному рівнях. Нині не можна констатувати заміщення за допомогою технологій реального інституту держави, як основи організації та консолідації суспільства, певною уявною моделлю. Інститут держави нині зазнає значних перетворень під впливом технологічних перетворень, але це, найперше, змінює механізми виконання нею своїх функцій, але не підриває консолідуючу здатність цього політичного інституту. Віртуальна держава таким чином нині постає як форма держави, яка модернізується під впливом технологій та публічного дискурсу.

Нинішні процеси віртуалізації держави можна інтерпретувати систему принципів та інструментів (детериторіалізація, дискурсивізація, медіатизація та ін.), які мають як конструктивні, так і деструктивні наслідки, що проявляється у ставленні до інституту громадянства, мірі лояльності до держави, руйнуванні національної ідентичності, обмеженні суверенітету, глобальній технологічній залежності тощо. Існуючі дослідження найчастіше відбивають тенденції до інтерпретації віртуалізації держави як: 1) перехід від національної моделі держави до іншої (віртуалізованої); 2) процес адаптації та боротьби за виживання в інформаційному суспільстві; альтернативна форма держави.

3. Попри те, що політичній науці віртуальними або кібердержавами зазвичай називають ті, які не відповідають усім ознакам міжнародного правосуб’єкта (невизнані держави, держави, що існують лише в Інтернеті тощо), під віртуалізацією держави розуміємо, найперше, перетворення механізмів функціонування держави, перенесення виконання державою своєї функцій частково чи уповні в кіберпростір як середовище ризиків і можливостей, утворене в результаті функціонування електронно-комунікаційних систем.

Відзначено, що нині держава поступово видозмінює чотири основні ознаки, закріплені Конвенцією Монтевідео: постійне населення, визначена територія, уряд, здатність вступати у відносини з іншими державами. Названі класичні характеристики держави більшою чи меншою мірою екстраполюються до інформаційного простору (кіберпростору), в результаті чого класичний інститут держави модифікується. Функціонуючи в умовах сучасного кіберпростору, який динамічно розвивається, сучасні держави отримують як нові можливості, так і опиняються перед новими викликами.

Відтак віртуалізація інституту держави постає як багатоаспектний процес з наявними перевагами та ризиками, в результаті якого під впливом інформаційно-комунікаційного прогресу видозмінюються характеристики новітнього інституту держави. Це процес, зумовлений переходом діяльності органів держави у віртуальний простір Інтернету, яка виводить реалізацію функцій держави та можливості впливу на населення на новий рівень.

4. Аргументовано, що простежити механізми державної боротьби з викликами та за власний авторитет в інформаційному просторі можна через аналіз стратегій кібербезпеки. Для цього було обрано кіберстратегії США, ФРН, Польщі та України. Вивчення цих документів, їхнє порівняння дозволить визначити, в якій з чотирьох ознак держави відбуваються найсуттєвіші зміни під впливом технологій та інформаційної революції – у сфері взаємодії з громадянами, території держави, перетворення урядових механізмів чи у відносинах з іноземними áкторами. Згадані стратегії було обрано для аналізу, бо кібербезпека є тією сферою, в якій можна простежити механізми віртуалізації держави, проаналізувавши понятійно-категоріальний апарат документів, першочергові завдання, сформульовані в них, а також механізми їхнього досягнення.

РОЗДІЛ 2. ЗМІНА ОЗНАК ДЕРЖАВИ В ПРОЦЕСІ ВІРТУАЛІЗАЦІЇ

2.1. Трансформація ознаки населення в процесі віртуалізації новітньої держави

Постійне населення – перша серед ознак держави, виділених у Конвенції Монтевідео. Аби проаналізувати, як ця ознака змінюється в процесі віртуалізації держави, необхідно поглянути, як ідею національної держави протиставляють ідеї космополітичної, і як за умов медіатизації та глобалізації суспільства космополітична ідея набирає політичної сили. Таке ідеологічне зміщення може відігравати вагому роль у творенні національної політики. Крім того, важливо зрозуміти, в який спосіб держава зобов’язується надавати громадянам технологічну освіту та регулювати потік інформації в кіберпросторі.

Постійним населенням заведено вважати те, що впродовж тривалого часу проживає на території певного населеного пункту, незалежно від його наявності на момент реєстрації [97]. На прикладі українського законодавства покажемо особливості правового регулювання цього питання. Закон України «Про громадянство» визначає безперервне проживання на території України проживанням в Україні особи, якщо її разовий приватний виїзд за кордон не перевищував 90 днів, а в сумі за рік – 180 днів. Не є порушенням вимоги про безперервне проживання виїзд особи за кордон у службове відрядження, на навчання, у відпустку, на лікування за рекомендацією відповідного медичного закладу або зміна особою місця проживання на території України [41]. Власне у формі громадянства проявляється зв’язок між державою та постійним населенням [41]. Так, з одного боку, саме держава своїм апаратом повинна гарантувати громадянам дотримання та здійснення всіх їхніх прав, а громадяни повинні підкорятися правилам, встановленим системою національного права. З іншого боку, громадяни безпосередньо впливають на формування органів державної влади та здатні брати участь у формування політичних цілей і

цінностей – через вибори, громадянське суспільство, демонстрації, громадською думкою тощо.

Народ (як сукупність громадян держави) зберігає за собою статус джерела влади та легітимності в суспільстві, навіть якщо на практиці не завжди передбачені можливості реального відкликання влади чи усунення неналежного правлінця від влади. Визначаючи народом сукупність громадян, його можна вважати аналогом поняття «політична нація». На відміну від етнічного розуміння нації, політична не передбачає спеціальних повноважень представникам певної етнічної групи, проте навіть за умов рівності всіх громадян елементи етнічного націоналізму зберігаються навіть у найбільш демократичних країнах (наприклад, їх можна вбачати у встановленій офіційної державної мови). Врешті формування національної свідомості громадянства – це та підстава, що зумовлює розуміння сучасної держави як національної, де певна група зберігає за собою право диктувати правила поведінки іншим.

Національна держава як продукт історичного розвитку виникла лише в XIX столітті, й її основою варто вважати ідею нації як такої, що має право на самовизначення, адже після розпаду колоніальних режимів право на самовизначення нації знайшло своє юридичне закріплення на найвищому рівні – в Декларації ООН «Про надання незалежності колоніальним країнам і народам» [29]. Тож націоналізм (у тій чи іншій формі) іманентно присутній у державі того типу, яку сьогодні можна назвати класичною, адже всі держави сприймаються як такі, що виникли в результаті народного самовизначення.

Якщо нація сформувала національну державу, то національна держава взяла на себе обов’язок формувати, плекати та розвивати національну ідентичність. Національною ідентичністю вважаємо уявлення, які приписує собі індивід, розуміючи свою приналежність до спільноти, об’єднаної спільними культурними ознаками. Чи не основною ознакою цієї ідентичності є усвідомлення себе та певної спільноти людей як «Своїх», що повинні жити у світі, який заселяють «Чужі».

За логікою національної держави, її громадяни – унікальні, особливі та специфічні, покликали до існування цю державу, яка повинна захищати їх від «Інших», від втрати «своєї ідентичності». З. Бауман вказує, що ідея етнічної приналежності постулює щось на кшталт «шлюби укладаються на небесах і ніякі людські дії не можуть їх розірвати» [10, с. 117]. Але наприкінці XX століття ідентичність перестає трактуватися тільки як така, що твориться групою, – її творення опиняється руках самої людини, що отримує все більше доступу до інформації та вибору власних пріоритетів.

Зі слів М. Маклюена, сьогодні електроніка та автоматика змушують нас пристосовуватися до умов глобалізації, ніби весь світ став рідним домом [74, с. 16]. Цю тезу можна підтвердити даними про кількість користувачів мережею Інтернет, де громадяни всякої держави можуть вступати у взаємодію один з одним попри кордони. За даними аналітичних розвідок компаній «We Are Social» і «Hootsuite», загальна кількість користувачів Інтернету 2018 року становила 53 % населення планети, тобто понад 4 млрд осіб [159]. З них кількість тих, що використовують смартфон, становить 68 %. І цей відсоток росте з року в рік. А соціальними медіа користується понад 42 % населення планети (2017 року їхня частка становила 37 %). Це дає підстави стверджувати про постійне зростання кількості учасників віртуальних взаємодій.

Навіть більше, відсутність доступу до інформаційних технологій новітнє міжнародне право вважає неприпустимим. Так, в Женевських принципах 2003 року йдеться: «Ми усвідомлюємо, що інформаційні комунікативні технології слід розглядати як інструмент, а не як самоціль. За сприятливих умов ці технології здатні стати потужним інструментом підвищення продуктивності, економічного зростання, створення нових робочих місць і розширення можливостей працевлаштування, а також підвищення якості життя для всіх. Вони також можуть сприяти веденню діалогу між народами, країнами та цивілізаціями. Ми також повністю усвідомлюємо, що сьогодні переваги революції в області інформаційних технологій нерівномірно розподілені між розвиненими країнами та тими, що розвиваються, а також всередині країн. Ми

сповнені рішучості перетворити цей розрив в цифрових технологіях в цифрові можливості для всіх, перш за все для тих, кому загрожує відставання і подальша маргіналізація» [31]. У цьому контексті важливо згадати, що 6 липня 2012 р. Рада ООН з прав людини визнала, що право на доступ до Інтернету повинно бути захищеним; було прийнято резолюцію в якій зазначила, що ті ж права, що гарантуються для людини в офлайні, повинні захищатися і в онлайн-середовищі [171]. Так, право на доступ до Інтернету можна визначити як забезпечене державою право людини на доступ до всесвітньої глобальної мережі Інтернет з метою реалізації основоположних прав людини [85]. Отже, цифрову нерівність між країнами, що становить нерівність у доступі до інформаційних технологій, прирівнюють до нерівності в економічній, соціальній, культурній, освітній сферах, які поглиблюються в результаті нерівного доступу до комп'ютерних технологій.

Так, національна держава більше не може стверджувати, що продукована нею ідентичність буде достатньою підставою для об'єднання людей, котрі проживають на її території. Причиною та ймовірною площиною для об'єднання та творення ідентичності, виступає, передусім, інформаційний простір або кіберпростір. Діяльність в Інтернеті передбачає комунікацію в межах спільнот, необмежених державними кордонами. І сам факт існування Інтернету створює специфічні умови комунікації, недоступні в часи до його появи, і ще донедавна поставлені за межі державної юрисдикції. Тож держава опинилася перед вимогою змінювати свої канали комунікації та пристосовуватися до технологічних нововведень. «З огляду на мінливість і непостійність усіх або більшості форм ідентичності, саме здатність «робити покупки» в супермаркеті ідентичностей, ступінь дійсної або передбачуваної споживчої свободи вибирати свою ідентичність й утримувати її скільки треба, стає найлегшим шляхом здійснити свої фантазії про ідентичність. Маючи цю здатність, людина здатна створювати та знищувати ідентичність, коли завгодно. Або їй так здається» [10, с. 91], – зазначає З. Бауман.

Учений вважає, що у такий спосіб сучасність перейшла через період «автентичної» індивідуальністю в період «іронічної» індивідуальності та далі – в сучасну культуру, яку можна назвати «асоціативною індивідуальністю» – постійною втратою зв'язку між внутрішньою душею і зовнішньою формою соціальних відносин. Відтак ідентичність зазнає постійних «вагань» [10, с. 91].

З. Бауман цитує А. Турена, який уважав: сучасний стан суспільства сигналізує про «кінець визначення людини як соціальної істоти, обмеженої її місцем в суспільстві, що обумовлює її поведінку або дії», і тому захист соціальними особистостями своєї «культурної та психологічної специфіки» не може здійснюватися без «розуміння того, що принцип їх комбінації можна знайти всередині людини, а не в соціальних установах або універсальних принципах» [10, с. 192]. А Е. Хобсбом зауважує: ніколи слово «спільнота» не використовувалося більш нерозбірливо і беззмістовно, ніж в десятиліття, коли в реальному житті стало складно знайти спільноти в соціологічному сенсі. «Люди шукають групи, до яких можуть належати, безумовно і назавжди, у світі, де все рухається і переміщається, в якому ніщо не є надійним» [Цит. за: 10, с. 184].

З огляду на розмитість поняття соціальної спільноти, на яку вказує З. Бауман, людина опиняється у ситуації, коли її соціальне становище більше не може диктувати їй спосіб мислення та поведінки. Кожен громадянин опиняється перед необхідністю обирати свою ідентичність самотужки, і тут все залежить лише від його амбіцій та уяви: «Як тільки руйнується спільнота, придумують ідентичність» [10, с. 184]. У вченого виникають підстави стверджувати, що в різкому контрасті до патріотичної або націоналістичної віри, найперспективнішим видом єдності є той, що досягається щодня заново, шляхом протиборства, суперечки, переговорів і угод про цінності, переваги обраного способу життя та ідентичності безлічі різних членів спільноти. Таке розуміння зводить до максимуму розуміння людської ідентичності як продукту комунікації та мінімізує можливість державного впливу на цей процес.

Залишатися громадянином держави фізично, але перестати бути носієм національної ідентичності – форма прояву віртуалізації держави.

Спілкування, що не знає меж і мовних бар'єрів – ідея «глобального села», втілена на практиці, творить специфічний вид ідентичності та світогляду, який не узгоджується з національною ідентичністю. Завдяки Інтернету в людському спілкуванні зберігається та втілюється логіка тісного або малого світу, описана наприкінці 1960-х років американським психологом С. Мілґремом [183]. Її називають теорією малого світу або теорією шести рукостискань. Запропонована вченим гіпотеза полягала в тому, що кожна людина опосередковано знайома зі всяким іншим жителем планети через недовгий ланцюжок спільних знайомих. У середньому цей ланцюжок складається з шістьох осіб. С. Мілґрем опирався на дані експерименту, який полягав у такому: в одному місті роздали 300 конвертів, які треба було передати певній людині, що жила в іншому місті. Конверти можна було передавати тільки через своїх знайомих і родичів. Зробивши підрахунки, С. Мілґрем визначив, що в середньому кожний конверт пройшов через шість осіб. З появою соціальних мереж ця теорія тільки підтвердилась. Так, 2018 року відстань між людьми у соціальній мережі Facebook скоротили до 4,57 особи [151].

Логічним наслідком такої взаємовпов'язаності є породження того світогляду, який У. Бек назвав космополітичним. «Більше немає сенсу сперечатися про практичність патріотизму чи про неймовірність ідеї космополітизму. Адже світ став космополітичним з огляду на загрози, які над ним нависли – екологічна, загроза тероризму, навіть війна в Іраку, що першою продемонструвала, наскільки війна здатна зачепити весь світ через мас-медіа» [150]. При цьому космополітизм не означає цілковиту відмову від усвідомлення себе носієм певної культури. На думку У. Бека, космополітична ідентичність – єдиний правильний орієнтир розвитку національної держави. Аби досягнути такого рівня свідомості не лише громадянам, а й державам необхідно вдаватися до певних практик, які б виробили у «світових громадян» терпимість і відкритість до того, що в національній державі вважається «чужим». Б.

Шержинський та Дж. Уррі виділили такі практики космополітизму: 1) багатостороння, масштабна мобільність, в якій люди можуть подорожувати тілесно, уявно та віртуально; 2) здатність користуватись багатьма місцями та середовищами за раз; 3) цікавість до різних місць, людей та культур; здатність локалізувати ці місця і культури історично, географічно та антропологічно; 4) здатність відбивати власне суспільство і культуру в площині історичних та географічних знань, мати вміння до рефлексії та естетичного судження між різними локаціями та суспільствами; 5) семіотичні навички інтерпретувати картинки численних «Інших», бачити, що вони відтворюють тощо; 6) відкритість до інших людей та культур, бажання та здатність цінувати певні елементи мови, культури «Інших» [Цит. за: 150].

Так, космополітична свідомість потребує виховання через можливості (постійну мобільність) та через освіту (дізнаватися про «Інших», розуміти їхню культуру та їхній зв’язок з власною культурою).

«Ніхто і ніколи не вивчав, яка міра інформації необхідна, щоб поставити під сумнів образ індивіда або суспільства. У наш час, у всякому разі, обсяг інновацій набагато перевершує все, що було створено нового у всіх культурах минулого в усьому світі. Ми відчайдушніше, ніж наші предки, прагнемо знаходити та збирати шматки зруйнованого образу [75, с. 143], – констатує М. Маклюен, даючи зрозуміти, що ідентичність за умов медіатизації та віртуалізації потребує першочергового формулювання, адже пов’язав із психологічним бажанням людини зрозуміти, ким вона є.

Отже, резюмуємо результати нашого аналізу змін, що відбуваються у відносинах громадянина і держави в процесах віртуалізації, медіатизації та глобалізації. Прив’язаний до національної держави як представник народу (нації), сучасний громадянин часто не ідентифікує себе з державою, в якій проживає, в результаті споглядання загальнопланетарних медіа та користування соціальними мережами, мережею Інтернет загалом. Залишатися громадянином держави фізично, але перестати бути носієм національної ідентичності – форма прояву віртуалізації держави. В результаті цього замість

національної ідентичності та національного світогляду в людини може розвиватися усвідомлення себе як представника людства, що живе в умовах постійних ризиків та в середовищі культурного різноманіття; вона може стати носієм космополітичної свідомості.

Відтак віртуалізація постійного населення як однієї з чотирьох основних ознак держави, виділених в Конвенції Монтевідео, полягає у:

– відході від ідеї етнічної нації як такої, що наділена панівними правами визначати владу на території певної держави;

– формування ідентичностей громадян держави переходить в інформаційний простір, який не завжди контролює держава; з огляду на те, що кількість користувачів Інтернету постійно зростає, процес медіатизації спільноти можна вважати глобальним процесом;

– творення космополітичного світогляду в результаті уніфікації комунікативних платформ, запровадження освітніх ініціатив та усвідомлення глобальних загроз, що нависають над всіма державами та здолати які можна лише спільно;

– загострення різних форм націоналізму як засіб протистояти процесові «розмивання» кордонів. Цей націоналізм набуває вигляду ностальгії за безпечним минулим, сформованим образом власної ідентичності, страхом перед зникненням знайомого світу, в якому кожен може стати жертвою невідомих «Чужих». Аби уникнути цих уявних небезпек (за визначенням Б. Андерсена), спільнота набуває ознак закритості.

Очевидно, що процес віртуалізації громадянства супроводжується певними суперечливими тенденціями. З одного боку, відбувається поширення інформаційних та комунікативних технологій, перетворення їх на доступні. З іншого боку, тенденції закриватися від процесів глобалізації і заклики будувати «стіни» між державами знаходять щораз більше прихильників.

Крайньою формою віртуального громадянства стало б офіційне створення інституту світового громадянина, чия ідентичність сповідує принципи космополітизму. Такий громадянин освічений та лояльний, постійно

переміщається (наприклад, прихильний до фрілансу), може знайти спільну мову з представниками різних держав та усвідомлює себе частиною світового процесу. При цьому, «віртуалізований громадянин» повинен зберігати зв'язок з власною культурою, але не обов'язково з територією свого походження. Тенденцію перетворення простору на віртуальний буде проаналізовано у наступному підрозділі.

2.2. Визначена територія як ознака держави в процесі віртуалізації

Предметом дослідження другого підрозділу є поняття визначеної території як однієї з основних ознак держави, а також її трансформація в умовах глобалізації та медіатизації, зокрема й політичної сфери. За Конвенцією Монтевідео територія держави повинна бути визначеною. Всі відхилення від вимоги визначеності державної території дають підстави вважати її наділеною ознаками віртуальності.

Територія держави – це територіальна ділянка, на якій поширюється державна влада, що передбачає функціонування узгодженої адміністративно-правової системи. На цій території також проживає населення держави, що наділяє державний лад легітимністю, дозволяючи йому здійснювати легітимне насильство. Фактично встановлену територію визначають наявністю та фіксованістю державного кордону. Саме державний кордон, визнаний іншими державами, дає підставу говорити про існування визначеної території певної держави. Державні кордони формують простір соціальної взаємодії громадян певної держави.

Важливо, що визначена територія – це не лише певна ділянка суші та моря. Це простір взаємодії та комунікації, де гарантоване правильне «прочитання» текстів, що продукуються політиками. За А. Лефевром, соціальний простір можна мислити лише як особливий різновид «діалектично пов'язаної тріади», що охоплює три моменти: просторову практику (як сприймається простір?); репрезентацію простору (що розуміється під простором?); простір репрезентації (як проживається простір?) [69].

Ідея території пов’язана з ідеєю суверенітету, який визначається так: верховенство, самостійність, повнота та неподільність влади в межах її території; незалежність і рівноправність у зовнішніх зносинах [30]. Тобто, кордони держави існують не лише для позначення меж соціальної взаємодії, а й меж повноважень уряду певної країни, межі суверенітету та легітимності влади.

Врешті, поняття визначеної території пов’язане і з вимогою до держави бути наділеною постійним населенням. Територія створює простір спільноти, над яким «витає» національна ідентичність, що протистоїть «Іншим»: «Передбачається, що однорідність етнічної суті, гетерономна: це не продукт, створений людиною. І не дивно, що етнічна приналежність більше, ніж всякий інший вид постульованої ідентичності, виходить на перший план, коли починають говорити про наступ страшного, поліфонічного простору, де «ніхто не знає, як з ким говорити». Так держава прагне зайняти «безпечну нішу», в якій «кожен схожий на всякого іншого», тож мало що потрібно обговорювати і розмови ці легкі [10, с. 117], – зазначає З. Бауман. Це дає підстави пов’язувати ідею територіальної визначеності та національної ідентичності.

Отже, поняття визначеної території у класичній концепції держави пов’язане зі всіма іншими ознаками держави. Передусім з вимогою мати постійних громадян, адже вони повинні проживати на цій території; завдяки цим громадянам на певну територію поширюється суверенітет держави, її легітимна влада зберігає за собою право диктувати обов’язкові для всіх правила поведінки. За межами визначеної державної території це повноваження зникає; Вступати у відносини з іншими державами держава може лише на підставі неоспорюваності своєї території з територією інших держав, відсутність територіальних претензій – це запорука мирних міждержавних стосунків.

Проте сьогодні існують певні тенденції в процесі визначення територіальних меж держави, що потрібно враховувати в процесі дослідження віртуалізації держави. Передусім, йдеться про стрімкий технологічний розвиток і процеси глобалізації, що зумовлюють «розмивання» кордонів. Ймовірність дуже швидко долати значні відстані відбивається в перегляді відносин між

часом і простором. «Сучасність починається, коли простір і час відокремлені від життєвої практики та один від одного, і тому їх можна розуміти як різні та взаємно незалежні категорії, коли вони вже не є, як це було впродовж довгих століть, тісно пов'язаними між собою і тому стають ледь помітними аспектами життєвого досвіду» [10, с. 20], – зазначає З. Бауман у праці «Плинні часи». Розірванні відносин між часом і простором здаються для нього чи не основною ознакою сьогодення. «[...] В сучасності час здобуває історію, як тільки швидкість руху через простір (на відміну від незмінного, по суті, простору) […] стає питанням спритності, уяви та винахідливості людини [...] Як тільки відстань, пройдена за одиницю часу, стала залежати від технології, від штучних транспортних засобів, всі правила обмеження швидкості руху, що дійшли до наших днів, успадковані з минулого, могли бути, в принципі, порушені. Лише небо (або, як це з'ясовувалося пізніше, швидкість світла) перетворилося на межу, і сучасність стала одним безперервним, непохитним і швидким прискоренням зусилля, спрямованим на досягнення цієї межі» [10, с. 20].

Зміна тривалості переміщення з точки А в точку Б, а точніше її радикальне скорочення, дають підстави говорити про домінування часу над відстанню, а відтак і територією. Ці поняття, концепти залишаються дуже пов'язаними у свідомості людей, адже безпосередньо стосуються практики – пересування та переміщення, передусім інформації. «Слова «далеко» і «довго», як і «поруч» і «швидко», використовуються для позначення майже одного і того ж: скільки зусиль потрібно людині, щоб подолати певну відстань, – стосується це ходьби, оранки чи збору врожаю. Якщо людей попросити пояснити, що вони мають на увазі під поняттями «простір і час», вони могли б сказати, що «простір» – це те, що ви можете пройти за певний час, тоді як «час» – це те, що вам потрібно, щоб подолати простір» [10, с. 122–123], – зазначає З. Бауман.

На думку цитованого вище мислителя, сучасність почалася зі звільнення людини з-під влади простору та часу. Звільнення з-під влади простору для громадян означає мобільність – можливість подорожувати, не зважаючи на кордони та великі відстані. «Завдяки недавньому винаходу залізниці,

автомобіля, літака фізичний вплив кожної людини, колись обмежений кількома кілометрами, тепер розширився на сотні миль. Більш того, завдяки дивовижній біологічній події – відкриттю електромагнітних хвиль – кожен індивід відтепер (активно й пасивно) водночас перебуває на всіх морях і континентах – він перебуває у всіх точках Землі» [74, с. 47], – цитує М. Маклюен Т. де Шардена.

Проте розуміння простору лише як певної території – неоднозначне. Британська вчена Д. Мессі зазначає, що у 1970-х роках підхід до розгляду простору як соціального конструкту став класичним: простір трактують як результат соціальних, економічних та, власне, політичних процесів, натомість його розгляд як виключно території відходить на задній план [Цит. за: 160]. У 1980-х роках, за Д. Мессі, уже не лише простір розглядали як соціальний конструкт, а й сам соціум трактувався як просторово сконструйований.

У найзагальнішому значенні політичний простір визначають через такі властивості: 1) універсальність, здатність впливати на всі сфери життя, елементи суспільства, відносини, події; 2) включеність – можливість безмежного проникнення в усі сфери життя; 3) атрибутивність – здатність поєднуватися з неполітичними суспільними явищами, відносинами та сферами [59].

Якщо в геополітичному просторі кордони нині ще наявні, то в інформаційному просторі, де й формуються ідентичності громадян, таких кордонів немає [143]. У більшості сучасних розвідок інформаційний простір інтерпретується дуже схематично – як складова частина простору культури, і, водночас, як особлива галузь фізичного простору, яка може виокремлюватися за заданими ознаками (наприклад, за носіями інформації) [140].

У ситуації, коли на рівні з географічною, фізичною територією, обмеженою кордонами, виступає уявна, віртуальна, комунікативна площина, обмежена приладами підключення до інформаційного простору, варто згадати концепцію М. Фуко, який стверджує: «Простір є фундаментальним у будь-якій формі суспільного життя; простір є фундаментальним у будь-якому порядку здійснення влади» [161]. Він запроваджує поняття «гетеротопія»,

протиставляючи його утопії. На відміну від утопій, котрі не мають реального місця, але все ж мають місце в просторі уяви, набувають вираження в просторі мови, вписані в дискурс, гетеротопії пов'язані із принциповою неможливістю віднаходження спільного простору. Як акцентує О. Беззубова, «у пізніших роздумах М. Фуко важливого значення набуває поєднання питання мови, мислення та простору, що, зокрема, знайшло вираження в понятті дисциплінарних просторів» [11; 79, с. 115], на які поширюється юрисдикція певних органів влади.

Отже, проаналізувавши зміну відносин між часом і простором, зумовлену поширенням інформаційних технологій, важливо зазначити, що поняття території починає конкурувати з поняттям простору, що не обмежується суто географічними координатами, а твориться зокрема межами взаємодії членів спільноти, простором домінування владного дискурсу.

Такий підхід можна підтвердити тенденцією людей вдаватися до так званого «кочівнового способу життя». На думку З. Баумана, донедавна його вважали ознакою варварських і слаборозвинених суспільств. «Кочівники визначалися як первісні люди, і від Г. Гроція проводилася паралель між кочівниками та «первісним» і «диким» (тобто грубим, неприборканим, неокультуреним, нецивілізованим): «створення законів, культурний прогрес і розвиток цивілізації тісно пов'язані з еволюцією та вдосконаленням відносин між людиною і землею в часі та просторі» [10, с. 201]. Тобто, в науці домінував погляд, що прогрес неминуче пов'язаний з відмовою від кочівнового способу життя на користь осілого. З. Бауман цитує Ф. Ратцеля, що вказав свою аксіому: боротьба за існування означала боротьбу за простір [10, с. 201]. Натомість сучасність, на думку З. Баумана, – це реванш кочівного способу життя над принципом територіальності та осілості, адже осілою більшістю керує кочівнова й екстериторіальна еліта, що не прив'язана до жодної території. Їхня можливість подорожувати та згортання контрольно-пропускних пунктів стало «метаметою» політики, а також воєн, вважає З. Бауман. Окрім того, зараз

виконання людьми оплачуваної роботи дедалі менше прив'язане до конкретної локації робочого місця (фріланс).

Важливо, що поняттям кочівнового способу життя можна позначати не лише переміщення різними територіями, а й різними культурними просторами. Для того, щоб побувати в іншій країні чи ознайомитися з її культурою, достатньо мережі Інтернет. Втрата зв'язку між працівником та робочим місцем означає вільне переміщення в будь-який час. Так, ідея кочівного способу життя цілком узгоджується з можливістю «набувати космополітичної ідентичності». Адже обидві ці звички стають можливим завдяки інформаційному простору та в ньому. І сприяють цьому два чинники. Передусім, це спосіб життя громадян, що втрачають зв'язок з територією, прив'язуючись до простору (зокрема інформаційного), в якому вони творять свою ідентичність. Крім того, держава більше не прагне володіти якомога більшою кількістю територій, оскільки вони перестали вимірювати багатство.

Перша тенденція означає «виснаження» культурного ідеалу, що породжує ідею нішевості, відведеної для кожної спільноти. Але «власна ніша» переважно означає територіальне відділення, право на окремий «захищений простір», який потребує захисту і який вартує захисту саме тому, що він окремий, тобто оточений охоронюваними кордонами, через які пропускають тільки людей «тієї ж» ідентичності та забороняють доступ «Іншим». За таким підходом ідея територіальності та наявності кордонів між різними державами породжує та живить ідею націоналізму.

Щодо зміни ідеї багатства та його зв'язку з фактом володіння значною територією З. Бауман вказує, що «тяжка сучасність» була ерою територіальних завоювань, адже в землі зберігалися основні ресурси. Тоді багатство і могутність залежали від розміру і якості земельних ресурсів, були повільними, неповороткими та незручними для переміщення. Але, на думку філософа, за умов сучасного розвитку більше не важливо, хто «великий», а хто «менший». Натомість важливо, хто «швидкий», а хто «повільний». «Правлять ті, чия швидкість вища, ніж швидкість противника. Коли швидкість означає

домінування, «освоєння, використання і заселення території», то стає перешкодою, а не перевагою [10, с. 201]. На його думку, прийняття під свою юрисдикцію і, більш того, анексія чиєїсь землі означають капіталомісткі, важкі та невигідні турботи про управління та забезпечення громадського порядку, відповідальність, зобов'язання – і перш за все накладають значні обмеження на свободу переміщення в майбутньому.

Крім втрати зв'язку території та культури, а також багатства, є ще один чинник, який здатен нівелювати важливість території для держави – це універсалізація загроз. «Не можна сказати, що наше століття обійшлося без історичних катастроф: дві світові війни, Аушвіц, Нагасакі, потім Ґаррісбурґ і Бхопал, тепер Чорнобиль. Це змушує до обережності у виборі лексики та до загостреного сприйняття особливостей історичного розвитку. Всі страждання, біди та насильства, котрі люди завдавали один одному, падали досі на «Інших» – євреїв, чорношкірих, жінок, мігрантів, дисидентів, комуністів і под. З однієї сторони, існували загородження, табори, міські квартали, військові блоки, з іншого – власні чотири стіни – реальні або символічні кордони, за якими могли сховатися ті, кого, здавалося б, не торкнулася біда» [12], – вважає У. Бек. На його думку, тепер від загроз неможливо прикритися ідеєю «Своїх» та «Інших»; перед ймовірністю загроз усі держави однакові та жодна з них не може впоратися з цими небезпеками самотужки.

Нині такими «Іншими» найперше є мігранти, найперше з нестабільних країн Близького Сходу. Загальноєвропейська міграційна криза, яка стартувала у 2015 році, спричинила загострену реакцію окремих країн Європи на проблему біженців (мова передусім про Угорщину). Всупереч описаній У. Беком тенденції, дотепер проти «Інших» будують стіни, а найперше ультраправі політики та організації підживлюють ксенофобію.

Отже, з огляду на провадження новітнього «кочівнового способу життя», затратність та економічну нерентабельність завоювання та утримання нових територій, а також через позатериторіальність загроз кінця XX століття –

початку XXI століття, можна говорити про зміну ставлення до визначеної території як безперечної ознаки держави.

У процесі віртуалізації території як ознаки держави виділимо такі тенденції:

– поняття території починає конкурувати з поняттям простору, що не обмежується суто географічними координатами, а твориться зокрема межами взаємодії членів спільноти, простором домінування владного дискурсу;

– зміна відносин між простором і часом, що виникає в результаті технологічного поступу та мобільності населення; так громадяни отримують можливість переміщення швидко та на великі відстані;

– домінування поняття простору над територією; тобто, важливі не виключно державні кордони, а й межі соціальної взаємодії, що розгортається зокрема в кіберпросторі;

– територія як земля певною мірою зменшує свою цінність, оскільки обтяжує та сповільнює процес прийняття рішень;

– уніфікація загроз перетворює всю планету на єдиний простір, не розділений кордонами;

– нові тенденції породжують спротив певних держав, які надають перевагу стратегіям «закритості».

Ці тенденції дають підстави говорити про те, що відбувається процес детериторіалізації, коли фізична територія стає не настільки важливою, як інший простір – віртуальний, інформаційний. У праці «Глобалізація» М. Уотерса цей процес розглядається як сукупність тенденцій, що призводять до детериторіалізації соціального, яка зумовлюється експансією символічних обмінів. Фундаментом теорії глобалізації, за М. Уотерсом, є концепція відносин між соціальною організацією та територіальністю, які в кожний історичний момент детермінуються одним із трьох типів обміну: матеріальним (економічним), політичним, символічним:

– матеріальні обміни мають тенденцію до локалізації соціальних відносин: виробництво товарів передбачає концентрацію в одному місці

робочої сили, капіталу, сировини; взаємодію в режимі «віч-на-віч» під час управління процесом праці та надання послуг;

– політичні обміни мають тенденцію до інтернаціоналізації – територіальної експансії соціальних відносин: здійснення влади передбачає контроль за населенням, що мешкає на даній території, і надання гарантій суверенності цього контролю, які одержуються внаслідок взаємодії з інституціями влади за межами даної території;

– символічні обміни мають тенденцію до вивільнення соціальних відносин від просторової референції: процес утворення та трансляції інтелектуальних і естетичних символів може відносно легко переміщуватись, здійснюватися між територіально віддаленими індивідами/групами [199, с. 7].

Серед трьох описаних способів взаємодії, на думку М. Уотерса, зараз домінує символічний.

Для А. Аппадураї детериторіалізація – це втрата прив’язки соціальних процесів до фізичного простору. У теоретичній моделі А. Аппадураї первинна дихотомія «локальне/глобальне» заміщується за суттю дихотомією «територіальне/детериторіалізоване», а глобальність і локальність виступають як дві складові глобалізації [148, с. 4]. У свою чергу П. Віріліо також трактує детериторіалізацію як форму глобалізації. Він стверджує, що прискорення комунікації призвело до заміни географічного простору часом і зазначає, – «проблема кінця століття – детериторіалізація» [22]. У праці «Машина бачення» П. Віріліо можна прослідкувати деструктуризацію можливостей як вияв детериторіалізації. Дослідник аналізує зміни, згадуючи роздуми М. Мерло-Понті: «Усе, що я бачу, в принципі досяжне для мене (принаймні, для мого погляду), присутнє на карті “я можу”». Цією фразою М. Мерло-Понті точно описує те, що знищується телетопологією. Насправді суть того, що я бачу вже не є для мене досяжною, не потрапляє з необхідністю на карту “я можу”, моїх можливостей» [23, с. 95]. При цьому топологія описує невідповідність того, що ми бачимо, і того, з цим можемо взаємодіяти, оскільки те, що ми бачимо, демонструє машина, телевізор. Простір, що спочатку був прозорий, а

потім розділений прозорим склом (за П. Віріліо), тепер діє за принципами непрямої прозорості екрану. Завдяки цьому можлива так звана телеприсутність, що не є ні присутністю, ні відсутністю, це просто форма віртуального буття. Тобто, П. Віріліо надає перевагу визначати детериторіалізацію як абстрактний наслідок поширення комунікативних процесів і технологій, тим, що існує у свідомості та знищується у зв'язку із впровадженням непізнаної новизни.

Т. Бєльська розглядає детериторіалізацію як прояв глобалізації [17, с. 99]. На її думку, глобалізація призводить до «реконфігурації» географічного простору, тож прийняття рішень відбувається на значній відстані від тих, кого вони стосуються. Географічна відстань стає менш важливою, аніж донедавна. Локальне може трансформуватись у глобальне та навпаки; виходячи за межі місцевого; цінності, символи, традиції отримують глобальне розповсюдження.

Отже, зміна відносин територіальності на відносини детериторіальності, спричинені мобільністю населення, технологічним поступом, швидкістю передавання інформації, має кілька вимірів: соціальні, культурні, символічні. Межі між цими видами детериторіалізації можна провести хіба умовно.

Ж. Бодрійяр зазначав, що «відтепер територія більше ані передує карті, ані живе довше за неї, а карта передує території» [19, с. 108]. Так, панування інформаційних технологій і мас-медіа як засобів комунікацій призводить до настільки прискореного поширення інформації та створюваних образів, що відбувається «детериторіалізація культури» та створення нових форм соціальної ідентичності, чітко не пов'язаних із визначених місцем [19, с. 108]. Можна прослідкувати кореляцію між втратою зв'язку з територією та процесами формування ідентичності, коли національна ідентичність стає однією з альтернатив. Адже, за Ж. Бодрійяром, відбувається циркуляція знаків і образів, що стає дедалі швидшою. Ці знаки не просто формують світ, а й самі стають об'єктивною реальністю. Світ симуляцій, як стверджує мислитель, дає нам можливість потрапити у світ знаків, які не позначають нічого реального; більш того, довести саму реальність та її істинність тепер практично неможливо. Адже людина, поставлена за межі простору, де відбуваються події,

про які повідомляють у медіа, до яких відсилають знаки, котрі доводиться кожному споживати, і вона не може перевірити їхню істинність. Ці твердження Ж. Бодрійяр висловлює в есеях «Чи справді була війна в Затоці» і «Війни в Затоці не було». Симуляції війни, як стверджує вчений, лише циркулювали в інформаційному просторі, а відтак і у свідомості людей, не важливо, де ті проживали, але ніхто не міг перевірити їхню правдивість.

Такі судження перегукуються з концепцією Е. Тоффлера, обґрунтованою в праці «Футурошок» (1970). Так, бувши очевидцем того, як звичний світ зазнає перетворень, науковець описує світ, де все, що мало значення раніше (стосунки, сім'я, знання), більше не має звичного досі значення. Суспільство модерну було «оформлено» потужною структурою соціальних і державних інститутів, які вже зі середини XX століття трансформуються. Розрив звичних соціальних взаємодій і усталених традицій призводить до «деінституціалізації» суспільства. На думку Е. Тоффлера, настає політична криза; багато інститутів зникають (можливо, це мав на увазі Ж. Бодрійяр, кажучи про «смерть» соціального), деякі втрачають довіру громадян.

Отже, інформаційні трансформації стають панівними чинниками в розвитку сучасного суспільства, яким керують мас-медіа з новою структурою, стратифікацією, динамічною циркуляцією переданих повідомлень. Мас-медіа зумовлюють віртуалізацію об'єктивної реальності, загалом перетворюючись на засіб осягнення світу, а іноді навіть і заміщаючи саму реальність.

Виділимо два підходи до розуміння детериторіалізації:

1) виникнення детериторіалізації на підставі глобалізації та розвитку новітніх інформаційних технологій. Віртуалізація територій відбувається під впливом електронних комунікативних засобів. Віртуальні території не мають географічно-територіальної прив'язки, виникають у зв'язку з детериторіалізацією світового простору, тобто виходу політичних процесів за межі географічних територій у сферу віртуальних комунікацій;

2) детериторіалізація відбувається у свідомості людей, що призводить до деструктуризації можливостей навіть за достатності ресурсів. Це можна

описати так: насправді суть того, що я бачу, вже не є для мене досяжною, не потрапляє з необхідністю на карту «я можу».

Загалом детериторіалізація за своєю природою є процесом, який зумовлює втрату прив'язки соціальних процесів до фізичного простору, а в результаті та з усвідомленням людьми, що його заселяють. Між соціальною організацією та фізичним простором існують процеси обміну, які у свою чергу слід поділяти на матеріальні, політичні та символічні, серед них зараз домінують останні.

Фразою «проблема кінця століття – детериторіалізація» П. Віріліо акцентує, що прискорення комунікації поступово призводить до заміни географічного простору часом або інформаційним простором. Причиною цієї заміни є втрата зв'язку між матеріальним і нематеріальним, тобто соціальним.

У такому контексті процес і факт детериторіалізації можна визначити як ознаку процесу віртуалізації держави – її занурення в інформаційний простір, запровадження дедалі більшої кількості механізмів формування символічного середовища поза фізичним простором розташування держави. Підставами виникнення детериторіалізації є, найперше, глобалізація та розвиток новітніх інформаційних технологій під впливом електронних комунікативних засобів, а також системні перетворення у свідомості людей.

Отже, сучасна «інфляція» визначеної території як ознаки держави зумовлена кілька моментами. По-перше, йдеться про зміну способу життя або принаймні про можливість значної кількості населення змінити спосіб життя з осілого на новітній «кочівний». Мобільність і здатність швидко долати значні відстані призводять до ігнорування чинника територіальності у формування ідентичностей. По-друге, важливо, що територія все менше асоціюється з багатством, силою, могутністю. Вона означає додаткові витрати, обтяжлива для всякого уряду в питаннях утримання та здобуття легітимності від населення, що її заселяє. Сьогодні могутність розташована радше в інформаційній потужності, якою більшою чи меншою мірою наділена кожна сучасна держава.

Крім втрати зв'язку території та культури, а також багатства, є ще один чинник, який здатен нівелювати важливість території для держави – це універсалізація загроз. Вони становлять небезпеку для всіх держав, незалежно від їхніх державних кордонів. Крім того, жодна держава не може впоратися з цими небезпеками самотужки, тож мусить брати участь в глобальних процесах знаходження порозуміння та протидії колективним викликам.

Чи не найважливішим чинником віртуалізації державної території стає медіатизація. Так, інформаційний простір як сфера домінування знання стає майданчиком розгортання процесів віртуалізації держави, а також пошуку альтернативних до її сучасної форм.

Отже, названі аспекти є основою детериторіалізації. Вона полягає у зміні статусу території як неодмінної ознаки держави. Не йдеться про нівелювання фізичного простору, проте визнається становлення інформаційного простору як повноцінного середовища функціонування новітньої держави. Простежуються два підходи до визначення поняття детериторіалізації. Перший акцентує на формуванні віртуальних територій, що не мають географічно-територіальної прив'язки. Другий підхід звертає увагу на перетворення свідомості людей. У процесі вивчення віртуалізації державної території вдалося виділити такі тенденції: поняття території починає конкурувати з поняттям простору, що твориться межами взаємодії членів спільноти; громадяни мають можливість переміщуватися швидко та на великі відстані; територія як земля втрачає свою буквальну цінність, оскільки обтяжує та сповільнює процес прийняття рішень; уніфікація загроз перетворює всю планету на єдиний простір, який вже значно менше враховує чинник кордонів; нові тенденції породжують спротив певних держав, які надають перевагу стратегіям «закритості».

2.3. Віртуалізація уряду та системи органів державної влади

Наявність дієздатного уряду – третя ознака держави, визначена Конвенцією Монтевідео. Уряд встановлює правила та гарантує їх дотримання на території, що вважається державною. Уряд має характеризуватися

легітимністю, а джерелом легітимності виступає постійне населення держави. Фактично, йдеться про суверенітет у тій частині поняття, що передбачає здійснення влади на своїй території. На думку Х. Арендт [6], саме легітимність робить владу владою та відрізняє її від насильства, сили, примусу тощо. «Інститути країни черпають свою владу в підтримці народу; така підтримка ніщо інше, як продовження тієї згоди, що зробила можливим існування законів. В умовах репрезентативного правління народ припускає, що повинен правити тими, хто править ним. Усі політичні інститути є проявом влади, її матеріалізацію; як тільки животворна сила народної підтримки їх покине – і вони кам'яніють і занепадають» [6, с. 319], – зазначає Х. Арендт у праці «Про насильство».

Монополія на владу – одна з основних ознак органів державної влади, на яку звертали увагу Ж. Боден, Т. Гоббс, та була описана М. Вебером в есе «Політика як покликання і професія» [200]. М. Вебер стверджує, що «держава – це всяка спільнота людей, що успішно претендує на монополію легітимного застосування фізичної сили в межах даної території» [200].

Визначаючи наявність уряду, наділеного легітимною владою, ознакою держави, проаналізуємо, які тенденції змінюють класичне уявлення про процес урядування. Перше, на що варто звернути увагу, це процес так званого «ослаблення держави». За усталеними підходами, державні інститути повинні застосовувати насильство, захищаючи своїх громадян і з їхнього дозволу. Проте в умовах глобалізації очевидною для певних учених стає тенденція до ослаблення держави, причиною і наслідком чого можна вважати той факт, що ознак політичної суб'єктності набувають бюрократи, партії та навіть поодинокі громадяни. При цьому така тенденція не свідчить про настання кризи в суспільстві, радше, навпаки, йдеться про її розвиток, вважає зокрема У. Бек. «Так, здавна і з різних сторін критикували втрату значення парламенту як центру раціонального формування волі. Рішення, які за конституцією, належать до парламентської компетенції та компетенції окремого депутата, як стверджують, все більше і більше приймаються, по-перше, керівництвом

фракцій (і ширше – партійним апаратом), а по-друге, державною бюрократією. Ця втрата парламентської функції часто тлумачиться як неминучий наслідок дедалі більшого ускладнення відносин в сучасних індустріальних суспільствах. Критичні спостерігачі кажуть про закладене в самому принципі представництва прогресуюче відокремлення апарату державної влади від волі громадян» [12], – зазначає У. Бек у праці «Суспільство ризику. На шляху до іншого модерну» (1986).

Але, продовжуючи свою думку, У. Бек зазначає, що не неспроможність, а успішність політики призвела до втрати державою інтервенційної влади та до «розмивання» місця політики. «Можна навіть сказати: що успішніша в цьому столітті була боротьба за політичні права; що успішніше ці права реалізовувалися і наповнювалися життям, то наполегливіше піддавався сумніву примат політичної системи та тим фіктивнішим водночас ставало проголошуване зосередження рішень в верхах політико-парламентської системи» [12], – пише У. Бек. Тож, на його думку, сама демократизація зумовлює те, що політика ніби сама позбавляє себе влади та місця. Адже як тільки демократія здобуває трохи більше можливостей та перемог, це породжує щораз нові масштаби і прагнення, які за умов розширення демократії змушують настрій громадян змінитися. Вони стають незадоволеними «застоєм» та «авторитарним характером» встановлених відносин. В такому сенсі «успішна» політика в демократії може зумовити втрату інститутами політичної системи своєї ваги.

Так, причиною «ослаблення» держави У. Бек вважає перемоги демократії, слідування правам людини. Це зумовлено і технологічним розвитком, оскільки розвиток медіа та соціальних мереж робить політику публічною, а контроль за інформаційними потоками – дуже складним для організації. Разом з тим відзначимо: перемога демократії та доступ до інформаційно-комунікативних технологій може також вести і до недемократичних тенденцій в державі, наприклад, перемоги на виборах популістів та диктаторів, що перетворюють державу на сильну та закриту. Цей процес є зворотною стороною глобалізації.

Також поспішно буде стверджувати, що технології та доступ до інформації перетворюють світ на глобальну демократію. На думку білоруського вченого Є. Морозова, сучасні диктатури також навчилися виживати, відмовившись від цензури, за умов функціонування соціальних мереж. Такі режими розглядаємо як неоавторитарні. Згаданий учений аналізує так звану «дилему диктатора»: концепцію, за якою диктатори нібито не зможуть брати участь в глобалізації, поки вони не відкриють свої мережі натовпам закордонних радників і інвестиційних банкірів, які витопчуть їхні країни в пошуках вигоди [84].

1985 році Дж. Шульц, тогочасний Державний секретар США, одним із перших заявив, що «тоталітарні суспільства опинилися перед дилемою: вони або відкидають ці технології (і пропускають нову промислову революцію), або дозволяють їх (що призведе до ліквідації тоталітарного контролю). Дж. Бхагваті, економіст Колумбійського університету, висловив суть «дилеми диктатора» так: «Комп'ютер є несумісний з компартією» [Цит. за: 84]. Однак Є. Морозов навів приклад дослідження німецьких учених Х. Л. Керна і Є. Хайнмюллера, які намагалися зрозуміти, як рівень задоволення своїм життям серед громадян Німецької Демократичної Республіки та їхня підтримка режиму корелювалася з доступністю до каналів західного мовлення. Х. Л. Керн і Є. Хайнмюллер з'ясували: східнонімецька молодь, що мала змогу дивитися передачі західного телебачення, загалом була більш задоволена життям і режимом, ніж ті, в кого такого доступу не було. Молоді люди, що жили в так званій «Долині невігласів», де доступ до медіа був обмежений, були більшою мірою політизовані, критично налаштовані до режиму і схильні звертатися за візами. За словами Керна і Хайнмюллера, несподівано для марксистів капіталістичне телебачення, схоже, виконувало в комуністичній Східній Німеччині (НДР) ту ж роль, яку Маркс приписав релігії в капіталістичному суспільстві, оголосивши її «опіумом народу» [84].

З огляду на ці аргументи, складно стверджувати, що розвиток технологій неодмінно означає демократизацію суспільства, хоч і демократизація

супроводжується розвитком комунікативних мереж. Недемократичні режими також навчилися з них користати (прикладом можуть слугувати Сінгапур), проте залишається суттєвим той факт, що ігнорувати кіберпростір держави з різним типом політичного режиму більше не можуть.

З. Бауман «виснаження влади» проглядає передусім у тому, що держава втратила здатність примушувати людей працювати; вона більше не може визначати, що треба зробити та хто повинен це зробити. У відповідь на це вона маскує центри прийняття своїх рішень, і громадяни повинні діяти на власний розсуд. «Наші переживання подібні на відчуття авіапасажирів, які високо в небі виявили, що каюта пілота порожня» [10, с. 144], – пише З. Бауман.

Учений акцентує на ще одній тенденції сучасної політики – приховуванні тих, хто насправді приймає рішення, цитуючи Г. Дебора: «Центр управління тепер прихований: ним ніколи не займають відомі лідери або чітка ідеологія» [10, с. 144]. Відтак у науковий дискурс із публіцистичного інтегрувалося поняття «ляльководи», яке засвідчує зростання неформальної деструктивної інституціоналізації сучасної політики, рішення в якій дедалі частіше приймаються латентно.

Розмивання центрів прийняття рішення зумовлено економічними законами вигідності (утилітарності). З. Бауман пояснює: уряд, присвятивши себе зростанню добробуту своїх виборців, не має іншого вибору, окрім благати та лестити, щоб заманити капітали на свою територію, і, коли йому це вдається, переконати будувати тут багатоповерхові офіси, а не залишатися в орендованих на одну ніч готельних номерах. І це можна зробити або спробувати зробити, «створюючи кращі умови для вільного підприємництва», що означає пристосування політичної гри до правил «вільного підприємництва» [10, с. 162–163]. Так, на думку вченого, уряди змушують себе утримуватися від всяких дій, які можуть створити враження, що територія, політично керована урядом, не схвалює традицій, очікування і підприємства, що глобально мислять і глобально діють, або схвалює їх меншою мірою, ніж сусідні країни.

На практиці все це означає низькі податки, меншу кількість або відсутність правил і, перш за все, «гнучкий ринок робочої сили». Вимога до держав створювати «інвестиційно привабливе середовище» диктує залежність уряду від капіталу, який, на відміну від першого, вже цілком втратив прив'язку до території. «Як це не парадоксально, уряди можуть сподіватися утримати капітал на місці, тільки усуваючи всі обґрунтовані сумніви в тому, що він може вільно переміщатися – негайно або без попередження» [10, с. 163], – зазначає З. Бауман.

Крім вільного переміщення капіталу та розвитку демократії, серед причин послаблення держави вкажемо на технологічні зміни, що, з одного боку, полегшують та уможливлюють доступ громадян до процесу прийняття рішень, а, з іншого, самі стають об'єктом політики, потребуючи схвалення. «Напрям розвитку та результати технологічної зміни обговорюють, їх потрібно легітимізувати. Тим самим виробнича і науково-технічна діяльність отримує новий політичний і моральний виміри, які раніше здавалися чужими її природі» [10], – зауважує У. Бек.

Збільшення чисельності суб'єктів та об'єктів політики, перехід до інформаційної сфери – все це призводить до того, що складні державні структури не встигають реагувати на зміни, що відбуваються все швидше з огляду на «легкість» переміщення. Вони ще не повною мірою перейшли в інформаційний простір, де їм потрібно протистояти законам кіберпростору, а також іншим «лідерам думок», які вже встигли відстояти своє право нав'язувати свою думку в цьому ж кіберпросторі. Така ситуація суттєво відрізняється від властивої XX століттю. На думку З. Баумана, «важкий», фордистський капіталізм був світом законодавців, розробників режиму і контролерів, світом чоловіків і жінок, орієнтованих на оточення, які переслідували цілі, визначені іншими людьми. «Це був світ авторитетів: лідерів, які знають все краще за інших, і вчителів, які вказують вам, як краще робити те, що ви робите. Легкий, дружній до споживача капіталізм не скасовує закони авторитетів і не робить їх надмірними. Він просто надає життя і

забезпечує співіснування авторитетів в такій кількості, що ні один з них не в змозі залишатися авторитетом тривалий час, не кажучи вже про володіння права на «винятковість» [10, с. 71]. Так, віртуалізація держави, зумовлена появою значної кількості авторитетів, а «численні авторитети» – це суперечливий термін. Зі слів З. Баумана, коли авторитетів багато, вони починають знищувати один одного, і єдиним ефективним лідером в цій галузі залишається той, хто буде вибирати між ними. Тобто, саме виборець відповідає за те, що можливий авторитет стає реальним. Авторитети більше не командують, а шукають прихильність виборця.

В інформаційному просторі за умов поширення електронних медіа, розпорошення ідеї авторитету та носія влади з'являється простір для розвитку дискурсу влади, навіть якщо йдеться про владу тимчасових авторитетів, коли насильство над тілом змінює влада над душею (за термінологією М. Фуко), проте це вже відбувається за межами державного контролю. В кіберавторитетів зазвичай відсутні можливості застосувати фізичне насильство до того, хто ігнорує встановлені ним правила. […] Більше немає ніяких великих лідерів, які сказали б вам, що робити, і звільнили б вас від відповідальності за наслідки ваших дій» [10, с. 37], – зауважує З. Бауман.

Так, серед основних причин послаблення держави в сучасний період можна вважати постійне розширення обсягу прав людини, урядову залежність від позатериторіального капіталу та технологічний розвиток, що і стає об'єктом, і інструментом політичного регулювання. Попри те, що недемократичні режими також навчилися пристосовуватися до певних інформаційних викликів, ці перетворення відкривають шлях для формування електронної демократії та медіадемократії.

Електронна демократія виступає такою формою суспільних відносин, за якої громадяни та організації залучаються до державотворення, державного управління, місцевого самоуправління шляхом широкого застосування інформаційно-комунікаційних технологій [163]. Проте для того, щоб це залучення мало наслідком розвиток спільноти згідно з космополітичними

цінностями, громадяни держави повинні бути обізнані, медіаграмотні та активні. Власне це бере до уваги й ідея медіадемократії.

Медіадемократія – це поняття, а також рух, спрямований на створення плюралізму в медіа [192]. Медіадемократія передбачає, що «здоров'я» демократичної політичної системи залежить від ефективної, точної та повної передачі соціальної, політичної та культурної інформації в суспільстві; що ЗМІ є каналами цієї інформації та діють в інтересах суспільства; що ЗМІ дедалі частіше нездатні та незацікавлені виконувати цю роль через посилення концентрації власності та комерційного тиску. Це підриває демократію, оскільки громадяни не мають можливості навчитися дебатувати з питань державної політики [192].

Розробники ідеї медіадемократії роблять акцент на тому, що медіа та громадяни повинні діяти спільно, контролюючи уряд та надаючи йому інформацію про настрої публіки. Прихильники медіадемократії виступають на підтримку незалежних та альтернативних ЗМІ, щоб уникнути їх тиску власників. Відтак через громадянську журналістику та суспільне мовлення люди можуть виробляти та поширювати інформацію та думки, які маргіналізуються в основних ЗМІ [192].

Отже, концепція медіадемократії та електронної демократії повинні доповнювати одна одну в той спосіб, що одна гарантує можливість доступу до процесу прийняття рішення, інша слідкує за тим, щоб громадяни приймали рішення обдумано та на підставі об'єктивних даних. Крім того, чи не основною передумовою функціонування е-демократії є створення та налагодження роботи електронного уряду.

Електронний уряд передбачає автоматизацію або комп'ютеризацію всіх прийнятих паперових процедур, які зумовлюють нові стилі керівництва, способи обговорення та прийняття стратегічних рішень, способи ведення справ та донесення думок громадян та громад, а також нові способи організації та донесення інформації [94]. Існує багато визначень електронного уряду: від використання ІТ для вільного руху інформації з метою подолання фізичних

кордонів традиційного паперу до використання технології для підвищення доступності та постачання державних послуг для громадян, ділових партнерів і співробітників [94]. Тобто, електронний уряд – це загальна концепція, що стосується ефективного використання урядом інформаційних технологій і сучасних комунікацій через різні інформаційні служби [147].

Більшість урядів у світі уже застосовують механізми електронного урядування для створення чіткого бачення цілей уряду; щоб громадяни могли взаємодіяти з державою швидше; для надання суспільних послуг та перетворення їх на більш ефективні; а також для того, щоб забезпечити цілісний обіг інформації між державними установами [156].

При цьому Організація економічного співробітництва та розвитку (ОЕСР) більшою мірою зачіпає питання управління, і меншою мірою – питання технологій («E-government is more about government than about «e») [94]. Це означає, що уряди повинні використовувати механізми та можливості інформаційного суспільства для того, щоб робота органів державного управління максимально відповідала потребам громадян [94], а ця вимога втілює уряд сучасної держави в інформаційному просторі.

При цьому електронний уряд – не просто використання Інтернету в роботі органів влади. Прозорість структур державного управління, яка є метою концепції e-government, не досягається лише підключенням до мережі Інтернет або створенням інформаційного web-сайту. Он-лайн доступ є обов’язковим елементом електронного уряду, проте це вимагає ще й суттєвішої перебудови традиційних форм функціонування уряду. Він вимагає прозорості управління, можливості здійснювати моніторинг, контроль над виконавчою владою, прийнятими рішеннями тощо [94]. Взагалі електронний уряд традиційно розглядають основою для національних стратегій, спрямованих на досягнення досконалості на основі використання Інтернет-технологій [164].

Електронний уряд формує ідеологію відкритої влади. Одним з аргументів може бути американський документ про електронне врядування від 2002 року, який визначає електронне урядування «використанням урядом Інтернет-

додатків та інших інформаційних технологій, у поєднанні з процесами, що впроваджують ці технології, для посилення доступу до урядової інформації та до послуг для громадськості, для інших установ та інших урядових одиниць; або покращення діяльність уряду, яка повинна передбачати ефективність, результативність, якість послуг і трансформацію» [164].

Принципи електронного уряду та електронного врядування – це радше відповіді на виклики XXI століття, у якому розвиваються процеси медіатизації та глобалізації, розпорошення авторитетів. Але, крім ознаки, про яку вже було вказано вище (доступ до урядової інформації з боку громадян, на підставі якої формується громадська думка та твориться легітимність), електронний уряд надає владі іншу перевагу. В результаті дотримання принципів електронного уряду, тобто, занурюючись в інформаційний простір, держава зберігає здатність спостерігати та контролювати громадян в цьому просторі, що донедавна був поставлений за межі її юрисдикції. Так держава може не «закривати очі» на процеси становлення нових авторитетів і «купування» (послуговуючись термінологією З. Баумана) ідентичностей. Саме електронний уряд стає необхідним в умовах «розмивання» кордонів та знищення відстаней, адже, потрапивши до віртуальності, держава може й не втрачати контроль з тими її громадянами, що проживають за межами її визначеної території.

Аналізуючи процеси запровадження електронного уряду, потрібно розуміти подвійну суть цього процесу: він вигідний громадянам, що не втрачають свого керівництва «з поля зору», і він вигідний уряду, що в результаті процесів віртуалізації своїх органів влади зберігає змогу контролювати своїх громадян.

На основі такого визначення можна дійти висновку, що віртуалізація держави означає домінування сфери публічного над політичним і тими сторонами політики, які заведено вважати таємним. Адже потрапивши у простір рефлексій (щодо творення ідентичностей, державної політики, економічних залежностей), політики вже не можуть ігнорувати тенденції, присутні в громадській думці. Поміщаючи в кіберпростір свою владу, політики

повинні постійно відстоювати своє право на владу, адже саме тут домінування кожного суб'єкта постійно піддається сумніву і перебуває за крок від того, щоб його замінив інший, вправніший авторитет.

Відзначимо, що технологічний розвиток як причина та наслідок віртуалізації держави полягає у двоякому процесі. З одного боку, ці технології стають об'єктом державного регулювання та легітимації, з іншого боку, власне технології стають новим інструментом здійснення політики – як з боку громадян (у вигляді електронного голосування, моніторингу за прийнятими рішеннями тощо), так і з боку самого уряду, що, «занурившись» в інформаційний простір, зберігає зв'язок зі своїми громадянами. Громадяни отримують нові механізми контролю та кооперації, навіть нові можливості висловити свою політичну волю, проте стикаються з необхідністю розрізняти пропаганду від справжніх новин, справжнього лідера громадської думки від тролів і ботів, а також приватне від публічного. З одного боку, в інформаційному просторі домінує сфера публічності, сфера верховенства суспільної рефлексії, а не приватного інтересу, з іншого боку, держава та її органи управління навчилися функціонувати в кіберпросторі, який від самого початку мав стати альтернативою класичної національної держави.

Отже, в результаті дослідження процесів віртуалізації органів державної влади, ми дійшли таких висновків:

– віртуалізація органів управління зумовлена переміщенням капіталу, зміцненням демократичних цінностей, «розпорошенням» авторитетів, поширенням інформаційно-комунікативних технологій;

– і уряд, і громадяни «занурюються» в інформаційний простір, де отримують змогу увиразнити свою волю, що через сферу публічності може корегувати та змінювати політичну ситуацію;

– віртуалізація уряду пов'язана з процесами розвитку електронної демократії та електронного врядування;

– в інформаційному просторі державна влада змушена постійно боротися за свою владу з численною кількістю інших авторитетів. Небезпеки для влади в

межах кіберпростору мають часто нематеріальний характер. Вони диктують необхідність стежити за інформаційними потоками, не допускаючи власної дискредитації. Інший тип небезпек пов'язаний з підривом віри в державу та пропагандою терористичних дій, вербуванням до терористичних організацій, діяльність яких виходить за межі національних кордонів.

2.4. Міждержавні відносини крізь призму віртуалізації

Впродовж тривалого часу на міжнародній арені держави діють відповідно до принципів державного суверенітету, тобто за ними зберігається право діяти на власний розсуд на своїй території та зберігати рівноправність на міжнародній арені. Цей принцип відомий з 1648 року, від підписання Вестфальського мирного договору. І хоч потім Вестфальську систему змінила двополярна, а зараз говорять і про систему «світового безладу» і «нової ненормальності» [153], певні принципи Вестфальського договору не втрачають актуальності. Йдеться передусім про принцип державного суверенітету, що передбачає принцип (юридичної) рівності держав; принцип невтручання однієї держави в міжнародні справи іншої.

Принцип суверенітету проглядається у тому, що в міжнародних організаціях кожна держава має таке ж право голосу, як й інша. Також суверенітет означає те, що в межах свої території держави можуть здійснювати владу на власний розсуд. Радикальним прикладом дотримання принципу суверенітету є ті випадки, коли навіть здійснюючи злочини проти людяності (наприклад геноциди), влада певної країни не зазнавала втручання міжнародної спільноти. Проте принцип суверенітету зіштовхується з іншою тенденцією – поширенням ризиків, які не під силу подолати державам самостійно, необхідністю діяти разом та потребою, щоб у цій взаємодії всі дотримувалися визначених правил. Тобто, хоч відносини між державами все ще здійснюються з дотриманням принципу суверенітету, але вони зазнали певних трансформацій. І створення Міжнародного кримінального суду, тобто зміна відносин у сфері правосуддя, що виконує також виховну та ціннісну функції, це лише один з

вимірів цих змін. Йдеться також і про небезпеку ядерного конфлікту, кліматичні зміни та інформаційні війни [190]. Крім того, актуальними в сучасному світі залишаються ризики терористичних атак, міграційних потоків, антиглобалізаційного руху, екологічної та економічної кризи тощо.

За таких обставин невтручання у внутрішньодержавні справи набувають іншого характеру, як і взаємодія держав на міжнародній арені загалом. З цього приводу З. Бауман зазначав: «Якщо принцип суверенітету національних держав нарешті дискредитований і видалений з кодексів законів міжнародного права, якщо здатність держав до ефективного опору подолана, так що на неї не потрібно зважати при обчисленні глобальних сил, то заміна «світу націй» на наднаціональний порядок (глобальну політичну систему сил, що стримують і врівноважують, покликані обмежувати та регулювати глобальні економічні сили) – це всього лише один із небезперечних, проте можливих сценаріїв. Глобальне поширення того, що П. Бурдьє називав «політикою невизначеності», є в рівній, якщо не більшою мірою ймовірним наслідком» [10, с. 207]. У цьому ладі держава може втратити монополію на примус (яку М. Вебер і Н. Еліас вважали найбільш характерною особливістю і водночас неодмінним атрибутом сучасної раціональності або цивілізованого порядку, тобто держави). Негативні наслідки такого розпорошення права на насильство можуть проявитися в тому, що його почнуть застосовувати безконтрольно: «Якщо „удар, нанесений державному суверенітету, виявляється смертельним і остаточним”, з цього не обов’язково випливає, що загальна кількість насильства, зокрема насильства з потенційними наслідками геноциду, зменшиться; насильство може стати тільки нерегульованим, опустившись з рівня держави на рівень „спільноти” (неоплемінний рівень)» 10, с. 207].

Нині ще зарано говорити про остаточне зникнення суверенної держави. Якщо зміна обставин функціонування держави залишається безсумнівною, то наслідки цих змін для суверенітету – неоднозначні. Може здаватися, що суверенна держава, яка характерна сучасній політиці, застаріла, у порівнянні з новими моделями глобального управління, транснаціональною інтеграцією,

космополітичною правовою системою і фрагментарною нормотворчістю, що руйнує межі конституційної держави [168]. Своєю чергою У. Бек посилається на аргументацію Д. Хелда про те, що через міжнародні угоди, інтернаціоналізацію процесів прийняття політичних рішень, все більшу залежність у гарантуванні безпеки, міжнародний обіг товарів, поділ праці національна державна політика втрачає те, що становить ядро її влади, – свій суверенітет [13, с. 72]. На думку вченого, поняття «міжнародних відносин» спустошене, бо в світі ризику спільноти не можуть більше вирішувати національні проблеми на національному рівні; права людей протистоять державі та захищаються нею від інших держав; надмобільний капітал позбавляє сили територіально визначені держави та змушує їх змінюватися [Цит. за: 150].

Проте не всі вчені погоджуються з тим, що в результаті збільшення учасників міжнародних відносин, глобалізаційних процесів суверенітет зникає як такий. «Суверенітет забезпечує зв’язок між демократичною політикою і верховенством права – настільки необхідний зв’язок, особливо в контексті транснаціональних режимів м’якого права з дефіцитом демократії або транснаціональних надзвичайних режимів економічного управління та військових втручань» [168]. Для прикладу, аналізуючи суверенітет на регіональному рівні, І. Забокрицький доходить висновку: реалізація суверенітету за законодавством ЄС є одним з основних критеріїв визнання його конституційності. «Держави-члени, поєднуючи свій суверенітет з метою досягнення своїх цілей, встановлених на рівні ЄС, створюють систему правових норм для реалізації цього повноваження. Інституції ЄС створюють, виконують і забезпечують дотримання цих правил, ці правила є обов’язковими для вирішення певних суспільних відносин, а джерелом цих правил і їхньої загальної чинності є ніщо інше, як суверенітет. А джерелами суверенітету є громадяни тих держав, які є членами ЄС, тому ми можемо підтвердити думку, що ЄС та його правова система створювалася конституційною владою народів ЄС» [202].

З такого погляду, глобалізаційні процеси не нівелюють суверенітет, але ґрунтуються на ньому. Дискусії про зникнення чи зміцнення суверенітету в сучасну епоху можна розвивати. Врешті, поєднання воєдино процесів суверенних та міжнародних підмічає й У. Бек: «Глобалізація, яку розуміють експансією транснаціональних просторів і організацій […] залишається, як це не парадоксально, залежною від національно-державного авторитету, точніше, від гегемоніальної влади. Передумовою для глобалізації є, так би мовити, мовчазний дозвіл з боку національної державної влади. Відкритість, пермісивність, необхідна для того, щоб забезпечити розвиток світового ринку, світових церков, міжнародних концернів і численних неурядових організацій […] може існувати і процвітати тільки під покровом відповідної концентрації державної влади» [13, с. 71].

У. Бек обґрунтував існування певного парадокса суверенітету, що зумовлений передусім правовим аспектом врегулювання міжнародних відносин. З одного боку, гарантія основних прав передбачає, на перший погляд, наявність національної держави. Проте з іншого боку, «як можна обґрунтувати та гарантувати космополітичні правовідносини між державами і громадянами різних країн, що перетворює саме національну державу як його гаранта на релятивне поняття, не спокушаючись при цьому помилковими альтернативами: або прагнути до світової держави, або впроваджувати основні права в просторі без прав і держав?» [13, с. 71]. Тож попри, здавалось би, неминучу втрату суверенітету, його існування стає запорукою створення наднаціонального суду та уряду. І попри втілення міжнародних правових ініціатив, не всі вони можуть бути ефективними, особливо без підтримки суверенної держави.

Право як механізм гарантування суверенітету залишається легальним і легітимним механізмом здійснення політики демократичних держав. Міжнародний кримінальний суд, що діє на підставі Римського статуту (1998) передбачає відповідальність за геноцид, злочини проти людяності, військові злочини, злочини агресії [101]. Женевські конвенції (1949) визначають правила

ведення бойових дій, а за порушення норм міжнародна спільнота застосовувати санкції, обходячи принципи суверенітету держави.

Унормовуючи спільні «правила гри» на міжнародній арені, основні орієнтири державного розвитку та принципи ведення бойових дій, міжнародне право також починає поширюватися на кіберсферу. Нині діють міжнародні нормативно-правові акти, що регулюють правовідносини в кіберпросторі. Йдеться передусім про Конвенцію Ради Європи про кіберзлочинність (2001), резолюція Генеральної Асамблеї ООН «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» (2005), Женевська Декларація принципів «Побудова інформаційного суспільства: глобальне завдання в новому тисячолітті» (2003) та ін.

Тобто, в епоху глобалізації національні держави втрачають нехай і не номінальну правову владу приймати рішення, а можливість контролювати їхнє виконання. І з огляду на свою ситуативну безпорадність, держави повинні виходити за власні межі та заручатися підтримкою інших. Оскільки дії окремих держав в Інтернеті, спрямовані на збір податків або протидії економічним злочинам не дають результатів, індивідуальні держави змушені співпрацювати з іншими – для здійснення власного національного інтересу.

Тобто, державний інтерес змушує жертвувати приватними національно-державними інтересами заради самих цих інтересів [13, с. 235]. Можна ствердити, що вони приймають рішення бути слабкими, щоб у перспективі ставати сильнішими. Це видно на прикладі боротьби з кіберзлочинністю, адже держава повинна взаємодіяти з іншими на засадах, визначених на міжнародному рівні, щоб отримати допомогу, якщо постраждає зокрема від кібертероризму, а також, щоб інші учасники міжнародного процесу поважали її кордони та самостійність, її суверенітет.

Спільна правова робота, узгодження та, як часто називають глобалізацію, уніфікація «правил гри» призводять до того, що всі держави стають включені в процес конструювання майбутнього. Такий світогляд диктує необхідність не відмежовуватися від сучасних викликів, а напрацьовувати план дій, що дасть

змогу мінімізувати ризики в майбутньому. З огляду на розвиток технологій, можна припустити, що загрози, зумовлені функціонуванням інформаційного суспільства (захист приватності, чистота інформації, цифрова нерівність, кіберзлочини тощо), тільки зростатимуть.

Коли держава відмовляється вести «гру» за новим глобальними правилами, то це сприймається спільнотою як протиправна дія. Найчастіше це покарання є у форматі економічних санкцій, виключення зі складу міжнародних організацій. З. Бауман аналізує ситуацію, коли країна діє всупереч загальним правилам: «Непокірним урядам […] відмовляють у позиках або зменшеннях їхніх боргів; місцеві валюти роблять глобальними прокаженими та сприяють їхньому знеціненню; курс місцевих акцій різко падає на світових біржах; країну оточують економічними санкціями та наказують минулим і майбутнім торговим партнерам ставитися до неї як до глобального вигнанця. Глобальні інвестори, бажаючи скоротити очікувані збитки, збирають речі та відводять свої активи, доручаючи місцевій владі розчищати руїни та витягувати жертв із ще більших злиднів» [10, с. 199–200].

Однак іноді покарання не обмежується «економічними заходами». Особливо впертим урядам (але не надто сильним, які не здатні чинити опір тривалий час) дають показовий урок, призначений для попередження і залякування їхніх потенційних послідовників. На думку З. Баумана, цей урок полягає в рутинній демонстрації переваги глобальних сил, що мало б змусити державу побачити підстави для співпраці з новим «світовим порядком». Якщо це не спрацює, використовуються війська. Прикладом З. Бауман наводить війну НАТО проти Югославії, в якій працювала стратегія продемонструвати нову глобальну ієрархію, нові «правила гри». «Якби не тисячі дуже реальних «людських втрат» і не країна, яка залишиться в руїнах і позбавлена засобів до існування та здатності до самовідновлення на багато років вперед, можна було б піддатися спокусі й описати цю війну як свого роду символічну» [10, с. 200], – вважає З. Бауман. Використовуючи поняття символічної війни, вчений має на увазі, що збройне протистояння було трансльоване на весь світ через медіа.

Нехай 1999 року (коли було згадане бомбардування) Інтернет не був настільки поширеним, як сьогодні, проте телебачення та радіо виявилися цілком достатніми, щоб весь світ побачив наслідки порушення міжнародних правил гри. Зображення руїн та людських жертв в інформаційному просторі стали символами війни та ціни, яку мусить заплатити правопорушник.

Через двадцять років після бомбардування Косово, можна припустити, що до силових зіткнень з іншими державами світова спільнота вдається вкрай обережно. Проте, крім своєї безпосередньої функції (продемонструвати силу глобального об'єднання), Югославська війна стала ще й прикладом для інших учасників міжнародних відносин, як можна провадити протистояння в XXI столітті.

Гібридні, інформаційні війни або війни четвертого покоління впродовж останніх десятиліть передують, супроводжують або й зовсім заміщують фізичні протистояння. Цим конфліктам властиві стирання відмінностей між безпосередньо війною та політикою, між залученими в неї військовими та цивільними, між фізичним та інформаційним простором зіткнень.

Ідея війни четвертого покоління зародилася ще в часи «холодної війни», коли наддержавам в процесі боротьби за свою присутність у різних точках світу стало зрозуміло, що широкомасштабне застосування танків, авіації і ракет в цих умовах малоефективне, і що роль партизанських і різних політичних, економічних, фінансових, інформаційних та психологічних підривних операцій кардинально зросла [82]. Характерною рисою стратегії війни четвертого покоління є те, що країна «маніпулятор» або фактичний агресор для реалізації своїх задумів використовує певного «агресивного недержавного суб'єкта» іншої країни, тобто сили, що перебувають у прямій опозиції до держави-жертви агресії.

В умовах поширення комунікативних технологій з'явилися значні можливості впливати саме на свідомість людей, тобто на недержавних суб'єктів іншої країни, що формують свою ідентичність в кіберпросторі, відірваному від територіальних кордонів національних держав. Так формується ідея гібридної

війни: «Нове у гібридній війні не її складові, а поєднання цих складових, а також додається новий інформаційний елемент, який на різних рівнях забезпечує функціонування і створює умови для визнання війни справедливою для власного населення, без чого не буває сучасних війн» [Цит. за: 99], зазначає Г. Почепцов. На його думку, гібридна війна – це не лише інформаційна війна, це війна економічна, репутаційна, смислова, людська. Пропаганда і маніпуляція мають при цьому визначальну роль, оскільки визначають спосіб мислення людей, їхні цінності та установки.

Є. Морозов посилається на дослідження американської дослідниці Б. Геддес, яка вивчала джерела народної підтримки авторитарних урядів і з'ясувала, яка з груп населення найбільш сприйнятлива до пропаганди: це середній клас. Інші групи, як з'ясувала Б. Геддес, менш сприйнятливі до пропаганди, ніж середній клас [84].

Розгортання в інформаційному полі, демонстрація подій всьому світові, що передбачає певні впливи на глядачів та споживачів інформації (породження космополітичної емпатії за визначенням У. Бека) творить символічну війну XXI століття. І вартість цієї війни значно нижча, ніж тієї, про яку писав ще К. фон Клаузевіц. Для ведення війни сьогодні потрібен лише доступ до незахищеної свідомості, що означає доступ до інформаційного простору, а відтак ці люди вже зможуть взяти на себе ініціативу.

На зміну ідеї міжнародного протистояння вказує також М. Маклюен. Він описує: якщо в Середньовіччі озброєння коштувало так, як все майно селянина, то сьогодні доступ до Інтернету робить конфлікти значно менш затратними [75, с. 49].

За умов легкого доступу до свідомості людей, розмивання меж між суверенними державами та іншими суб'єктами міжнародних відносин, політичної медіатизації, держави послуговуються механізмами «м'якої сили», яка узгоджується з процесами віртуалізації держави на інших рівнях. Інформаційні технології та соціальні медіа належать до головних ресурсів та інструментів посилення іміджевої привабливості соціальних і політичних

інститутів, виступаючи невіддільними компонентами «м'якої сили» держави. Вона дає змогу ненасильницькими методами розширювати сферу ідеологічного, аксіологічного та інформаційного впливу, формувати позитивний імідж країни або організацій, розвивати систему інформаційної політики та безпеки. «М'яка сила» домінує у структурі сили держави в умовах інформаційного суспільства та віртуалізації простору.

Ідея «м'якої сили» ґрунтується на уявленні про медіадискурс як владний ресурс, що здатен і покликаний впливати на масову свідомість з метою ідеологічного поширення медійних образів і текстів [28, с. 122], вигідних певному політичному суб'єктові. Ключовим показником, що дає підстави вважати медіадискурс інформаційною компонентою «м'якої сили», є формування ефекту довіри. В процесі медіатизації політики розвиток і накопичення «м'якої сили» політичними акторами досягається за допомогою створення і зміцнення відносин довіри між учасниками комунікацій [28, с. 123], вважає вчена Є. Грибовод. Для того, щоб «м'яка сила» була ефективною, вона спочатку змінює думки людей, а відтак і формується їх готовність діяти.

Інформаційний простір – широкий майданчик для поширення принципів та цінностей певної держави. У ньому можна як пропагувати цінності мирного, правового врегулювання конфліктів, так і розгортати свою діяльність противниками глобалістичних тенденцій і демократичних перетворень.

Отже, проаналізувавши віртуалізацію відносин з державами, що становить собою четверту ознаку держави, виділену Конвенцією Монтевідео, ми дійшли таких висновків:

– на міжнародній арені держави добровільно відмовляються від частки суверенітету, приймаючи це рішення з метою подальшого збереження суверенітету та керуючись національними інтересами;

– необхідність відмовитися від частини суверенітету продиктована економічною вигідністю співпраці, поширенням технологічного розвитку (розвитком кібербезпеки), позатериторіальними ризиками (ядерними, кліматичними, військовими, терористичними тощо);

– однією з форм врегулювання відносин на міжнародній арені є правотворча та судова діяльність, що повинна визнаватися всіма учасниками міжнародного процесу та поширюватися на відносини в кіберпросторі;

– як результат високої вартості класичної війни, протистояння між державами нині часто супроводжуються або заміщаються інформаційними конфліктами; вони використовують символічну зброю для приваблення на свій бік прихильників та безпосередніх учасників протистояння; йдеться про маніпуляцію, пропаганду, спотворення новин тощо;

– загрози глобалізації та медіатизації часто містяться в інформаційному просторі; це змушує держави все більше звертати увагу на ресурси «м'якої сили», які починають домінувати в структурі сили держави в умовах інформаційного суспільства та віртуалізації простору;

– в результаті віртуалізації держави у кіберпростір переміщуються механізми та стратегії насильства, правового врегулювання злочинів та правопорушень, дипломатії й образотворення, військового протистояння тощо.

Висновки до розділу 2.

Основні тенденції віртуалізації спроєктовані на чотири основні ознаки держави, виділені Конвенцією Монтевідео, що уможливило наступні чотири висновки.

1. Однією з основних класичних ознак держави традиційно вважається наявність постійного населення. Однак нині відбуваються процеси, які засвідчують віртуалізацію цієї фундаментальної ознаки. Вони, найперше, зумовлені технологічною революцією та глобалізацією, які зменшують значення державних кордонів, змінюють підходи до вибору місця проживання та праці. Продукована певною державою національна ідентичність більше не є неодмінною підставою об'єднання людей, котрі проживають на її території. Інформаційний простір, кіберпростір виступають площиною творення новітніх ідентичностей. Різко розширюються можливості спілкування та вибору локації проживання, з'являються нові джерела доходів (завдяки еволюції бізнес-моделі

платформової економіки). Віртуальні бізнес-компанії, формально самостійні роботодавці та працівники-фрілансери, які можуть проживати в будь-якому куточку планети – все це завдяки Четвертій промисловій революції ослаблює зв'язок населення з державою свого громадянства (підданства). Припускаємо, що проявом віртуалізації населення держави може стати наростання тенденції збереження особою громадянства держави без чіткого увиразнення певної національної ідентичності. Окрім цього наявними є такі малодосліджені новітні феномени як віртуальні держави (на зразок Князівства Сіландія, Інтернет-держави Віртландія), які пропонують надання свого громадянства через онлайн-процедуру.

2. Віртуалізація державної території полягає в зменшенні ролі чинника території держави з огляду на нинішню мобільність населення, уможливлення швидкого подолання значних відстаней за здешевлення витрат на переміщення між територіями різних держав. Нині територія – змінна характеристика, адже будучи формою соціально-просторової організації вона змінюється під впливом реалій конкретного часу. Формується нова надтериторіальна географія мереж і потоків, яка витісняє «стару» географію державних територій. У нинішньому «суспільстві швидкості» цінність топосу (місця) зменшується; швидкість фактично реконструює простір: максимально скорочуються відстані завдяки стисненню часу переміщення та передачі інформації на будь-яку відстань. Відтак, що могутність держави дедалі менше пов'язана саме з чинником території. Універсалізація глобальних загроз, вихід небезпек за межі державних кордонів зумовила необхідність спільно шукати відповіді на новітні виклики; це стало основою процесу детериторіалізації (втрати прив'язки соціальних процесів до певного фізичного простору). Детериторіалізація простежується як на рівні формування віртуальних територій, що не мають географічно-територіальної прив'язки, так і на рівні перетворення свідомості людей, що повинні мати справу з питаннями, на які складно впливати з огляду на їх географічну віддаленість.

3. Досліджено віртуалізацію системи органів державної влади, позаяк наявність такої системи віднесено до ознак інституту держави. Визначено, що ці процеси зумовлені демократизацією політики (попри те, що останніми роками дослідники відзначають загальнопланетарне погіршення якості демократії), стрімким поширенням інформаційно-комунікативних технологій, які охопили процеси урядування та низкою інших причин. Констатовано, що віртуалізація органів влади, найперше, полягає у діджиталізації, створенні системи простих, зрозумілих і прозорих послуг для громадян. Перспективою вбачається надання сервісу без наявності державної бюрократії, побудова цифрової держави, «держави у смартфоні». Відзначено тенденцію максимального «виведення» чиновників з процесу надання державних послуг, які автоматизуються. Нині запускаються єдині онлайн-портали державних послуг, відповідні мобільні додатки, електронні кабінети громадянина, відбувається перехід на електронний документообіг. Переведення державних адміністративних послуг в електронний формат уможливлює отримання послуги з будь-якого місця, де є підключення до Інтернету, та звужує ризики корупції. Якщо раніше йшлося про е-демократію, е-урядування, то нині мова йде про повноцінну розбудову цифрової держави.

4. Вивчення віртуалізації міждержавних відносин засвідчило, що впровадження нових інформаційно-комунікативних технологій посилило віртуалізацію соціальних процесів і явищ міжнародного життя. На міжнародному рівні нові технології спрощують контакти між державами, народами, виступаючи важливим важелем глобального управління (global governance, world governance). Водночас на рівні міжнародної взаємодії процеси віртуалізації держави призводять до певного послаблення суверенітету (це відбивається в теоріях «ерозії суверенітету», «обмеженого суверенітету»). Функціонування наднаціональних інтегративних структур, велика кількість транснаціональних акторів, поява різноманітних міжнародних режимів та багато інших феноменів глобалізації світу уможливлюють висновок не стільки про «зникнення» суверенітету сучасної держави, скільки про його

«розмивання». Відзначено, що віртуалізацію міжнародних відносин характеризує універсалізація ризиків, зростання інформаційних протистоянь тощо. За умов інформаційного суспільства переструктуровується весь світовий політичний простір, а відтак міжнародні відносини набувають нових обрисів.

РОЗДІЛ 3. ВІРТУАЛІЗАЦІЯ ІНСТИТУТУ ДЕРЖАВИ: КЕЙСИ США, ФРН І ПОЛЬЩІ

3.1. Постійне населення як об'єкт національних стратегій кібербезпеки

Як відзначалось вище, віртуалізація держави передбачає «перетворення» основних ознак держави – постійного населення, визначеної території, життєздатного уряду та здатності вступати у відносини з іншими державами. Такі зміни зумовлені процесами глобалізації та входженням держав у кіберпростір, в якому вони відстоюють право на існування, взаємодіючи з іншими суб'єктами політичного процесу. В попередніх розділах схарактеризовано тенденції віртуалізації держави. Тепер нашим завданням є прослідкувати, які з описаних процесів відбуваються в сучасному політичному процесі. Матеріалом для дослідження є стратегії кібербезпеки трьох держав – США, ФРН і Польщі.

2018 року в США було прийнято нову Стратегію кібербезпеки. З цього приводу Д. Трамп зазначив: «Америка створила Інтернет і поділилася ним зі світом. Тепер ми повинні переконатися, що ми захистимо себе та збережемо кіберпростір для майбутніх поколінь» [185, с. 29]. Таке формулювання дає підстави стверджувати: США визнають за собою позицію лідера, оперуючи ціннісними та технологічними аргументами.

Стратегія побудована на чотирьох стовпах, що передбачає її поділ на структурні частини: 1) захищати батьківщину, мережі, системи, функції та дані, американський народ, американський стиль життя; 2) сприяти процвітанню США, розвиваючи безпечну й успішну цифрову економіку та сприяючи сильним внутрішнім інноваціям; 3) оберігати мир та безпеку, зміцнюючи спроможність США – спільно з союзниками і партнерами – стримувати та, за необхідності, застосовувати санкції до тих, хто використовує кіберінструменти зі злочинною метою; 4) розширювати вплив США для розвитку ключових

принципів відкритого, придатного для взаємодії, надійного та безпечного Інтернету [185, с. 20].

Два перші завдання передбачають захист американських цінностей, і в їхньому переліку проглядається націоналістична свідомість. Інші два завдання зосереджені на взаємодії за межами держави, в площині міжнародної співпраці США. Кожен з цих пунктів певною мірою затверджує панівну позицію держави у світі та живить націоналістичну свідомість. Зокрема, на уряд покладено завдання перетворення політики відповідно до новітньої реальності, що сприятиме захисту американського народу та його способу життя [185, с. 20].

У Стратегії кібербезпеки США не вказано способи формування ідентичності громадян, проте загальний характер документа є націоналістичний: «Розквіт Інтернету та все більше значення кіберпростору для всіх аспектів сучасного світу відповідає зростанню США як єдиної супердержави світу» [185, с. 1]. Загалом у цій Стратегії, з приблизно 8 900 слів, 35 разів використовується слово «національний» («national»).

Вільний Інтернет розглядається як втілення національного інтересу та об’єкт гордості американців: «Американці продовжують отримувати вигоди від безпечного кіберпростору, що відбиває наші принципи, захищає нашу безпеку та сприяє нашому процвітанню»; «за минулу чверть століття, винахідливість американців зумовила еволюцію кіберпростору, а у свою чергу кіберпростір став основою для створення багатства та інновацій» [185, с. 1].

США ініціювали розробку ідеї свободи в Інтернеті як реалізації в онлайн-вимірі прав людини та основних свобод людини, зокрема свободи слова, асоціації, мирного зібрання, совісті та ін., а також права на конфіденційність в Інтернеті. Це має стати основними принципами взаємодії в Інтернеті, незалежно від кордонів.

Аналізована Стратегія США кіберпростір розглядає як майданчик для просування американських цінностей, серед яких – «віра в силу індивідуальної свободи, свобода слова, вільні ринки і конфіденційність» [185, с. 29]. На підставі наведених аргументів, можна дійти висновку: цей документ не прагне

змінити ідентичність американців, а радше зберегти теперішню, бо американський спосіб життя й американські інтереси стоять на першому місці.

Американський підхід, за документом, має стати орієнтиром для поділу світу на «друзів» і «ворогів»: «Наші конкуренти та супротивники дотримуються протилежних поглядів. Вони беруть участь у відкритому Інтернеті, обмежуючи при цьому доступ до нього свого власного народу, а також активно підривають принципи відкритого Інтернету на міжнародних форумах» [185, с. 29]. Стратегія ділить світ на США з союзниками та «Інших» – Росію, Іран, Північну Корею, КНР. Примітно, що в документі чітко визначені держави-противники. Цього нема ні в німецькій, ні в польській стратегіях, які було проаналізовано нижче.

Оскільки населення США має бути технологічно грамотне, для цього уряд декларує готовність й надалі інвестувати та вдосконалювати програми, які стимулюють розвиток внутрішнього трудового потенціалу, починаючи з початкової освіти. Це дасть змогу США мати конкурентоспроможний технологічний сектор. Аби захисти себе від різноманітних небезпек, передбачається, що американці повинні бути обізнаними з новітніми технологіями, вивчати цифрову безпеку, проблематику пропаганди тощо.

Уявлення про статус особи, що, занурившись в інформаційний простір, не повинна втрачати зв’язку з державою, унаочнюється присутнім у Стратегії порівнянням класичної війни та сучасної боротьби за права та свободи людини: «Багатовікові бої за права людини та фундаментальні свободи зараз розігруються в Інтернеті. Свобода самовираження, мирних зібрань і об’єднань, право на конфіденційність перебувають під загрозою. Попри безпрецедентне зростання економічного та соціального потенціалу, Інтернет продовжують підривати онлайн-цензура та репресії» [185, с. 25]. Тобто кіберпростір США розглядає радше як нове поле бою за незмінні цінності та за умови незмінного американського панування [185, с. 25].

Стратегія кібербезпеки США передбачає кілька форматів віртуалізації відносин з постійним населенням. Передусім, США демонструють свої амбіції

ввійти в кіберпростір на правах лідера, що диктує правила гри іншим партнерам. Ті, хто відмовляється грати за встановленими правилами, розглядаються як суперники, які прагнуть підірвати американську могутність. Стратегія орієнтована на збереження американської ідентичності та цінностей, а не на їхнє перетворення на космополітичний світогляд.

Стратегія декларує намір скеровувати зусилля на те, щоб не допустити або зменшити до мінімуму цифрову нерівність завдяки фінансуванню цифрової освіти громадян, впровадження нових технологій у структури різного рівня. Розробляючи концепт свободи в Інтернеті, США намагається уможливити реалізацію прав людини в кіберпросторі, зокрема йдеться про свободу слова, асоціацій, мирного зібрання, релігії та переконань, а також права на конфіденційність.

Видається, що в результаті усвідомлення того факту, що кордони розмиваються, у США загострюється націоналізм. Як захисна реакція у світі, якому властиві невідомі досі загрози, націоналізм відмовляється переглядати свої цінності та свої роль у світі. Позиція лідерства, яку зайняли розробники Стратегії, лише затверджує націоналістичний світогляд як такий, що може претендувати на загальність, орієнтацію на ті цінності, які вже сформувалися. Доречно згадати визначення Б. Андресена, що пропонує розуміти націю уявленою політичною спільнотою тому, що представники навіть найменшої нації ніколи не знатимуть більшості зі своїх співвітчизників, не зустрічатимуть і навіть не чутимуть нічого про них, і все ж в уяві кожного житиме образ їх співпричетності [4, с. 22]. Через це нація завжди буде обмеженою, бо навіть найбільша має свої межі, поза якими перебувають інші нації. Разом з тим, США визнає за собою відповідальність за загальний порядок у кіберпросторі.

Як і США, ФРН виділили чотири основні блоки, в межах яких держава повинна розгорнути дії, спрямовані на досягнення кібербезпеки. ФРН виділила: 1) безпечні дії в цифровому середовищі; 2) спільне зобов’язання забезпечити кібербезпеку з боку держави та економіки; 3) ефективна і стійка

загальнодержавна архітектура кібербезпеки; 4) активне позиціювання ФРН в європейській і міжнародній кібербезпековій політиці.

Отже, завдання, виписані у німецькому документі, передбачають зміни на національному рівні (перші три) та відповідне позиціювання на міжнародному (четверте). Однак примітно, що ціннісні аспекти (як, до прикладу, в стратегії США «захист американського способу життя») у завданнях не виписані. Всі вони радше зосереджуються на конкретних об’єктах, що мають бути створені, врегульовані або підтримані.

Так, на відміну від США, прописані напрями діяльності держави не дають підстав стверджувати, що ФРН констатує право встановлювати правила гри для всієї світової спільноти чи свою домінантну позицію. ФРН радше наголошує на спільній відповідальності за безпеку в кіберпросторі, на відміну від США, що бере на себе зобов’язання «розширювати американський вплив», «сприяти американському процвітанню», «захищати та зміцнювати державу».

«Держава, економіка, наука і суспільство несуть спільну відповідальність за безпеку кіберпростору» [157, с. 9], – визначено в Стратегії кібербезпеки ФРН. Спільну відповідальність ця держава розділяє не лише з економічними акторами, а й з громадянським суспільством, бізнесом та наукою. Одним з механізмів дотримання принципу розділення відповідальності є створення та зміцнення Національної ради з питань кібербезпеки [157]. Ця Рада була створена 2012 року як така, що є політично нейтральною і має на меті консультувати підприємства, державні органи та політиків у питаннях кібербезпеки та зміцнення їхніх позицій у боротьбі з кіберзлочинністю. Саме на цю Раду Стратегія покладає обов’язок розробити та прийняти федеральну архітектуру кібербезпеки. Адже, в епоху діджиталізації держава здатна постійно виконувати свої завдання лише тоді, якщо надає захист і свободу для розвитку суспільства, зокрема в кіберпросторі [157].

Аби надати державі змогу діяти у відповідний спосіб, Національна рада з питань кібербезпеки шукає шляхи обміну даними з відповідними стратегічними

органами міжнародних партнерів, і створює новий імпульс для національної політики у сфері кібербезпеки.

Аналізуючи процеси віртуалізації відносин держави та громадян, з'ясовано, що в Стратегії закладений обов'язок держави сприяти постійному розвитку в громадян умінь користуватися технологіями, складність яких безупинно зростає. Всі учасники політичного процесу повинні розуміти та вміти оцінювати можливості й ризики, пов'язані з використанням інформаційних технологій; такий обов'язок бере на себе і держава як основний суб'єкт політики.

Окрім сприяння розвитку цифрових компетенцій, держава декларує й готовність протидіяти цифровій недбалості [157, с. 14]. Така поведінка розглядається однією з важливих небезпек, натомість про цифрову нерівність (digital divide), що вважала однією з найбільших ризиків ще на початку XXI століття у Стратегії вже не сказано нічого. Можна дійти висновку, що подолати недбальство та легковажність до поведінки в кіберпросторі для держави стає важливішим, ніж подолати цифрову нерівність. Ймовірною причиною є те, що цифрова нерівність у ФРН відсутня як виражена проблема.

Зазначимо, що акцент на цифровій недбалості артикулюється тільки в німецькій Стратегії; в інших аналізованих нами документах про це не згадується. В намаганнях подолати такий вид недбальства, ФРН запроваджує таку цифрову освіту, яка спрямована на закріплення у свідомості громадян відповідальність за безпеку в кіберпросторі.

Серед інших небезпек для громадян, що приховує кіберпростір, є цільове розповсюдження фальшивих повідомлень, що стало можливим завдяки інтегрованим ІТ-системам, і таке, що можна використати для дезінформації та маніпулювання громадською думкою. Це довгострокова небезпека для вільного суспільства і демократії [157, с. 7], як відзначено в Стратегії. Тут важлива констатація зв'язку між громадською думкою та основами вільного суспільства та демократії. Це узгоджується з припущенням, висловленим вище, про те, що доступ до Інтернету означає доступ до свідомості громадян, а якщо на неї

впливати певним чином, то ліберальна демократія, як така, що коріниться у переконаннях та установках людей, може зазнати поразки. Зміна загального настрою може означати зміну політичного курсу, як це сталося в США та у Великій Британії 2016 року, коли після перемоги Д. Трампа на президентських виборах та після схвального голосування на референдумі за вихід з ЄС на порядок денний вийшли теми закритості суспільства, націоналізму та небезпек, пов'язаних з «Чужими».

Безпечна, конфіденційна, неманіпульована електронна комунікація має визначальне значення для права на комунікацію, права на приватність та для здійснення інших прав громадян [157, с. 14]. Цим констатується, що безпека спілкування в кіберсфері набуває ознак основоположного права людини, гарантованого на законодавчому рівні.

Попри те, захищаючи кіберпростір від негативного впливу на свідомість людей, що мають до нього доступ, ФРН декларує своє прагнення забезпечити свободу та безпеку – як в географічному, так і кіберпросторі, тож бере на себе обов'язок захищати громадян і підприємців у ФРН від кіберзагроз, запобігати злочинам і переслідувати злочинців у кіберпросторі [157, с. 8]. Для цього, зазначено у Стратегії, важливо запровадити надійні електронні ідентифікації та шифрування.

Надійна електронна ідентифікація визначена пріоритетом у сфері кібербезпеки ФРН. «Сприяючи безпечній електронній комунікації, потрібно розширювати концепти безпечної ідентифікації. Користувачі повинні мати можливість використовувати в Інтернеті безпечні засоби для автентифікації. Зараз широко поширений, але небезпечний, метод ім'я-пароль повинен бути доповнений і, якщо можливо, замінений» [157, с. 16], зазначається в документі. У Стратегії вказані способи ідентифікації онлайн із залученням документів, що посвідчують особу. Проте це не означає відкритість даних онлайн. Навпаки, всі дані в Інтернеті повинні бути анонімними або прихованими за псевдонімами. Так, в німецькій Стратегії, на відміну від американської, акцентується не

стільки на спільних національних цінностях, як на практичних рішеннях захисту громадян та користувачів мережі Інтернет.

У документі згадується, що для держави важливо розробляти власні зручні в користуванні технології, але це має відбуватися на основі глобальної технічної архітектури. Тобто, попри амбіції розвивати національний технологічний продукт, ФРН не претендує на те, щоб він став орієнтиром для інших акторів міжнародного процесу. У цьому твердження все ж можна прогледіти націоналістичні амбіції: німецький товар зберігає прив'язку до національної держави. Загалом слово «національний» у Стратегії (що налічує приблизно 8 750 слів) вжито 28 разів; це менше, ніж в аналогічних американському та польському документах.

Отже, на підставі аналізу Стратегії кібербезпеки ФРН можна дійти висновку, що віртуалізація відносин громадян з державою полягає в тому, що держава бере на себе обов'язок гарантувати всім доступ до цифрової освіти. Ця освіта повинна розвинути у громадян необхідні компетенції, а також протидіяти цифровій недбалості громадян. Також кіберосвіта повинна допомогти громадянам виробити вміння оцінювати ризики, зокрема ті, що пов'язані з поширенням неправдивих і маніпулятивних повідомлень, що ставлять під сумнів цінності демократії. Безпечна комунікація в кіберпросторі набуває рис одного з основоположних прав людини та громадянина, тож безпека в ній означає, з одного боку, надійність ідентифікації, а, з іншого боку, збереження анонімності, конфіденційності даних. Декларування амбіцій створювати марковані продукти в ІТ-сфері, зберігає прив'язку кіберпростору до національної держави та ідентичності. Однак все ж в документі акцентується на орієнтації на глобальну архітектуру кіберпростору.

Стратегією кібербезпеки Польщі сформульована мета «забезпечити високий рівень безпеки в процесі надання або використання цифрових послуг з боку державного, приватного секторів, а також приватних осіб». Ця стратегія виділяє чотири завдання: 1) на національному рівні координувати дії, спрямовані на запобігання, виявлення, боротьбу та мінімізацію наслідків

інцидентів, що порушують безпеку функціонування важливих для держави комп'ютерних систем; 2) посилити спроможність протистояти кіберзагрозам; 3) підвищити національний потенціал і компетентність у сфері кібербезпеки; 4) випрацювати сильну міжнародну позицію у сфері кібербезпеки [186, с. 14].

Три з чотирьох завдань передбачають зміни в межах національних кордонів та національного уряду, і лише останній пункт акцентує на міжнародній позиції держави. В цій Стратегії акцентовано: щоб отримувати дані, необхідні для оцінки ризиків, необхідна розробка моделі залежності, що описуватиме, як інцидент на одному суб'єкті впливає на надання послуг іншими суб'єктами.

Проаналізувавши польську Стратегію кібербезпеки, було виділено аспекти віртуалізації держави в контексті віртуалізації відносин з постійним населенням. Передусім держава гарантує підвищення обізнаності громадян через впровадження цифрової освіти до курсів навчальних закладів усіх рівнів. Зазначено, що навчальні заклади заохочуватимуть до розробки міждисциплінарних спеціальностей, що охоплюватимуть, зокрема, інформаційну безпеку, захист персональних даних, захист інтелектуальної власності в Інтернеті, а також питання, пов'язані з розвитком нових технологій. Метою такого навчання буде надання знань щодо ймовірних загроз у кіберпросторі й ефективних способів захисту від цих загроз. З метою підвищення компетенції наукових центрів у сфері кібербезпеки планується створення наукового кластера з кібербезпеки. Це має бути наукова платформа, до складу якої увійдуть університети та дослідницькі центри, що спеціалізуються на технологіях кібербезпеки [186, с. 20].

Освіта в Польщі, зорієнтована на розвиток технологій, визнається важливою не лише для формування поведінки в кіберпросторі, а й для виховання здатності в громадян створювати свої конкурентноздатні продукти. Польська влада звертає особливу увагу на підприємців, уважаючи, що підвищення їхньої обізнаності у сфері технологій сприятиме розвитку національного бізнесу, стартапів.

Польський уряд взяв на себе зобов’язання розробити рекомендації, як поводитися з дотриманням правил технічної безпеки, з огляду на конфігурацію комп’ютерних систем, прописати процедури безпечної експлуатації та безпечного використання новітніх технологій. Крім того потрібно буде реалізувати інформаційні програми для громадян, що матимуть на меті інформувати про загрози кіберзлочинності, описуватимуть поведінку, до якої потрібно вдаватися жертвам комп’ютерних атак.

Стратегією передбачено, що польський уряд повною мірою дотримуватиметься права на приватність, принципів вільного та відкритого Інтернету, що становить собою важливий елемент функціонування сучасного суспільства. Зазначається, що навіть за необхідності дослідження загроз, конфіденційність даних фізичних і юридичних осіб повинна строго дотримуватися [186, с. 9]. Механізми системи обміну інформацією мають бути структуровані так, щоб дати змогу суб’єктам, які беруть участь, захищати свої інтереси, включаючи захист таємниці компанії, захист іміджу тощо.

Як і в німецькій стратегії, у польській разом із вимогою приватності констатується зростання необхідності посилювати механізми ідентифікації серед операторів критичної інфраструктури та ключових послуг, зокрема йдеться про необхідність залучення цих суб’єктів до системи кризового управління. «Створення національної системи оцінювання буде пріоритетним; це допоможе здобути національну незалежність в питаннях оснащення, програмного забезпечення та в криптологічній сфері» [186, с. 14–15].

В польській стратегії, у порівнянні з іншими аналізованими документами, найчастіше зустрічається слово «національний». В документі, що налічує 6 030 слів, його використали 76 разів. Тож на підставі цього можна дійти висновку, що все ж національний аспект для формування ідентичності громадян залишається першочерговим. «Уряд також активно залучатиметься до наявних і потенційних нових форм європейського державно-приватного співробітництва, і так сприятиме розвитку польського бізнесу на міжнародній арені» [186, с. 14–15], – йдеться в документі. Зустрічається згадка про програму «Cyberpark

Enigma», що має потенціал конкурувати на європейському ринку спеціалізованих ІТ-послуг. Це дає підстави припустити, що Польща зберігає національні амбіції, зокрема в ринкових відносинах з ЄС.

Отже, в Стратегії кібербезпеки Польщі віртуалізація відносин з громадянами проглядається в тому, що уряд бере на себе обов'язок розвивати обізнаність громадян у сфері комп'ютерних систем, а через сферу освіти формувати уявлення про можливі кіберзагрози та шляхи протидії їм. Запровадження елементів кіберосвіти передбачається на всіх рівнях навчального процесу. Польща взяла на себе зобов'язання гарантувати всім учасникам конфіденційність їхньої інформації, що повинна дотримуватися навіть за умов аналізу даних. Важливою є постійна вказівка на вдосконалення процесів надання та оцінювання продукту, що робить доступ до Інтернету безпечним. Поряд з вимогою приватності зростає необхідність посилювати механізми ідентифікації серед операторів інформаційних послуг.

Аналіз принципів функціонування в кіберпросторі, прописані в польській Стратегії, можна припустити, що Польща дотримується радше принципів націоналізму, ніж космополітизму. В згаданому документі 76 разів зустрічається слово «національний». Тут зазначається, що Польща повинна розвивати конкурентоспроможність своїх кадрів і служб.

Підсумовуючи виявлені тенденції, зазначимо: віртуалізація постійного населення проявляється в кількох тенденціях, які є спільними для всіх аналізованих країн, а також в тенденціях, що відрізняються.

Серед спільних – це гарантія того, що медіаосвіта буде запроваджуватися на різних рівнях навчального процесу. Адже тільки в такому випадку в громадян сформується належне уявлення про можливості та загрози інформаційного суспільства. Це вимагає співпраці зі спеціалістами сфери освіти та науки. Також в усіх трьох документах визначено, що в кіберпросторі, як і за межами нього, мають домінувати права і свободи людини (свобода слова та ін.). Ідея космополітизму не прослідковується в повній мірі в жодній зі трьох згаданих стратегій.

Серед відмінних тенденцій зазначимо, що кожна держава визначає власну роль, яку хоче виконувати на міжнародній арені. Якщо США відверто заявляють про лідерські претензії визначати правила поведінки для всіх інших, то цього не простежується ні в німецькому, ні в польському документі. Відповідно націоналістичний настрій найбільш помітний в американській стратегії.

3.2. Державна територія як об'єкт національних стратегій кібербезпеки

Аналізуючи процеси віртуалізації території як державної ознаки США, бачимо, що її нівелювання для США важливе передусім у питаннях переслідування кіберзлочинців. «Запобігання кіберзлочинності вимагає ймовірності того, що злочинці будуть ідентифіковані, затримані та притягнуті до відповідальності. Проте окремі іноземні держави не співпрацюють у питаннях екстрадиції, нав'язуючи необґрунтовані обмеження або фактично перешкоджаючи їй. […] Ми будемо заохочувати інші країни прискорювати процес надання допомоги в розслідуванні та дотримуватися двосторонніх або багатосторонніх угод і зобов'язань» [185, с. 11].

США декларують намір сприяти всякому нівелюванню бар'єрів у процесі збирання та обміну доказами, ефективного транскордонного обміну інформацією з правоохоронною метою. Оскільки кіберзлочинність діє без кордонів, це вимагає сильного міжнародного партнерства для організації запобігання та протидії.

США зобов'язалися протидіяти тим політичним режимам, що використовують технології, допускаючи порушення прав і свобод людини: «США сприятимуть інноваціям у сфері кібербезпеки в усьому світі через залучення до торгівлі, підвищення обізнаності про інноваційні інструменти американської кібербезпеки, виявлення та протидію репресивним режимам, які використовують ці інструменти та послуги, щоб підривати права людини, зменшувати бар'єри для надійної глобальної кібербезпеки» [185, с. 15]. Також зазначено, що США працюватимуть над тим, щоб американський підхід до

відкритого Інтернету став міжнародним стандартом. Тут проглядається поділ простору на простір, де панують правила, прийнятні США, і простір тих держав, що не підкоряються цим правилам: «Ми також намагатимемося попередити те, щоб авторитарні держави, які розглядають відкритий Інтернет як політичну загрозу, перетворили вільний та відкритий Інтернет на авторитарну мережу, що перебуває під їхнім контролем, під виглядом безпеки або протидії тероризму» [185, с. 25]. Так ідея позатериторіальності проглядається в поділі простору не на державний та міжнародний, а на простір домінування американських цінностей і простір, де ці цінності не підтримуються.

США протиставляє себе державам, які джерелом власного багатства вважають території. Наприклад, з огляду на територіальні презензії Російської Федерації, ця країна все ще вважає території найважливішим ресурсом, що суперечить тенденції, описаній З. Бауманом: шукати могутність у розвитку технологічних, інформаційних механізмів, що створюють можливості для швидкого та гнучкого реагування на всякі виклики.

Попри те, що США констатує існування своїх інтересів за кордоном, держава визнає існування цих кордонів, що узгоджується з принципами територіальності: «США продовжуватимуть розвивати ринки […] ринки нових технологій, що можуть знизити вартість безпеки» [185, с. 26]. Основною ж метою Стратегії зазначено «Виявити, протидіяти, порушувати, нівелювати та стримувати таку поведінку в кіберпросторі, що дестабілізує національні інтереси та суперечить їм, зберігаючи при цьому домінування США в кіберпросторі» [185, с. 20]. Так, входження у кіберпростір для США пов’язаний, передусім, з необхідністю боротися з небезпеками, джерелом яких є і терористичні групи, і держави, що ставлять за мету підірвати могутність США.

Отже, Стратегія кібербезпеки США визнає існування кордонів, але наголошує на необхідності подолати їхні обмеження, коли йдеться про переслідування кібер- і мережевих злочинців, а також у протидії державам, що

відмовляються діяти за чинними для США правилами. Примітно, що США протистоїть державам, для яких територія залишається вагомим джерелом багатства, а також тих, що зберігають територіальні претензії щодо територій інших держав. Коли держава відмовляється видавати злочинця, використовує технології всупереч основним правам і свободам людини, США прагнуть подолати обмеження, встановлені кордонами та принципом суверенітету. У цьому простежується ідея позатериторіальності – в поділі простору на державний та міжнародний, а на простір домінування американських цінностей та простір, де ці цінності не підтримуються. Натомість у взаємодії зі союзниками США наголошує на повазі до кордонів та суверенітету держав, і зазначає, що діятиме лише в межах, встановлених ООН.

З іншого боку, констатуючи свій лідерський потенціал та свою провідну позицію у розробці, використанні, освоєнні нових технологій, США претендують на позатериторіальний вплив, що не обмежується кордонами жодної держави. Назвавши Інтернет «американським творінням», пропонуючи постійну медіаосвіту своїм громадянам, США претендують на доступ до всіх куточків світу: на території союзників – за їхнього відома та за згодою, на території противників – в ім’я свободи Інтернету.

У німецькій Стратегії кібербезпеки зазначено «внутрішню і зовнішню безпеку в кіберпросторі більше не можна чітко розрізнити» [157, с. 6]. Ця взаємопроникність обох сфер зумовлює нові загрози: «З діджиталізацією сучасного суспільства зростає його вразливість та потенціал зловживання у кіберпросторі. Більш того, конфіденційність громадян стає все більш вразливою, а наслідки кібератак не обмежуються кіберпростором. Успішні атаки можуть завдати соціальної, економічної, політичної та персональної шкоди» [157, с. 7].

Позатериторіальність простежується й у твердженні, що до цифрової сфери перейшла мобільність населення, а як наслідок, збільшується кількість даних, які циркулюють в Інтернеті. Ці умови становлять нові транскордонні виклики в процесі створення безпечної інфраструктури, а також у сфері захисту

прав громадян, констатують у Стратегії. З огляду на це сформульований намір ФРН посилити механізми міжнародного переслідування кіберзлочинців з метою подолання кіберзлочинності на міжнародному рівні: «…будуть посилені транскордонні заходи кримінального переслідування та спільна поліцейська здатність розслідувати» [157, с. 43].

Як стверджував філософ У. Бек, позатериторіальність знаходить свій вияв передусім у нових ризиках, їхніх наслідках для всієї політичної системи не лише щодо однієї держави, а й регіону і світу загалом. Це зумовлює необхідність спільно шукати розв’язання нових проблем. Така тенденція й прослідковується в німецькому документі: «Цільові кібератаки на банківську інфраструктуру або маніпуляції цінами на фондовому ринку можуть становити загрозу для фінансових ринків загалом і мати довгострокові наслідки для економіки ФРН і всього світу» [157, с. 7], – сказано в документі.

Аби впоратися з небезпеками, що з’являються, ФРН готова до співпраці з іншими державами, усвідомлюючи, що діє в умовах взаємозалежності, яка зростає. На європейському рівні ця взаємозалежність особливо проглядається у наявності спільного ринку, тож безпека в цьому випадку означає обмін безпечними та придатними для взаємодії даними [157, с. 39].

Констатуючи, що в певних своїх діях країна повинна менше зважати на державні кордони, передусім у питаннях переслідування кіберзлочинців, ФРН, попри те дотримується й принципу територіальності, акцентуючи на відмінності між регіональними та національними процесами. Також у Стратегії ФРН висловлює готовність активно підтримувати міжнародні зусилля, спрямовані на посилення режиму контролю за експортом, що стає важливим завданням з огляду на технології спостереження [157, с. 41], а в контексті віртуалізації території це можна трактувати як прихильність до класичного визначення державної території – географічного. «З огляду на транснаціональну взаємозалежність в діджиталізованому світі високого рівня кібербезпеки можна досягнути лише шляхом впровадження та зміцнення національних заходів у відповідних європейських, регіональних та

міжнародних процесах» [157, с. 39], йдеться в документі. У Стратегії зазначено, що безпеку потрібно розглядати на глобальному рівні, особливо в епоху діджиталізації, однак разом з тим вказано: ФРН працюватиме над придатною для взаємодії архітектурою і стандартами кібербезпеки для зміцнення національних і регіональних можливостей.

Отже, віртуалізація державної території передбачає вимогу посилити міжнародну співпрацю у сфері переслідування та попередження кіберзлочинності. Це необхідність, оскільки більше неможливо поставити межу між зовнішньою і внутрішньою кібербезпекою; порушені у кіберпросторі права людини часто мають наслідком порушення політичних, економічних та інших прав вже в межах матеріального права. Попри визнання висхідної взаємозалежності між країнами, ФРН зберігає прихильність до поділу на національний, регіональний і глобальний рівень політичних процесів, зобов'язуючись стежити за процесами експорту та зміцнювати національні потуги у сфері кібербезпеки. У цьому можна простежити принципи територіальності.

У польській Стратегії кібербезпеки віртуалізація території як державної ознаки проглядається на кількох рівнях. Передусім, в документі констатується розмивання меж у тому просторі, де відбувається боротьба зі злочинністю. «Беручи до уваги специфіку кіберпростору, боротьба з кіберзлочинністю вимагає транскордонного співробітництва правоохоронних органів та організацій CERT (Computer Emergency Response Teams – Команда з реагування на надзвичайні ситуації). У процесі розслідування злочинів, вчинених у кіберпросторі, час є критично важливим. Це означає, що потрібні ефективні та вірогідні канали обміну інформацією між правоохоронними органами різних країн» [186, с. 14–15], – сказано в документі.

З одного боку, в польському документі присутнє розрізнення національного та іноземного продукту, що дає підстави говорити про принцип територіальності: «З цією метою в національну систему кібербезпеки буде включено елемент, що аналізуватиме матеріали вітчизняних та закордонних

джерел, а також власних дослідницьких та кооперативних установ. Цю роль виконуватиме Національний центр кібербезпеки» [186, с. 17]. Крім того уряд зобов'язується створити спеціальну систему публічного та прихованого спілкування державних органів, і ця система мала б організувати безпечний, своєчасний та надійний обмін інформацією у внутрішніх та зовнішніх відносинах, зокрема з командирами, політичними та військовими структурами НАТО та ЄС. Так зберігається поділ на внутрішню та зовнішню політику.

З іншого боку, розробники польської Стратегії зазначили: потрібно створити синергію внутрішньої та міжнародної діяльності у сфері кіберпростору, що полягатиме у творенні спеціального специфічного простору, в якому і держава зможе реалізовувати свої функції, і права громадян не порушуватимуться. В ідеї творення такого простору можна прогледіти ідею позатериторіальності, що все ще твориться.

У документі згадується спільний простір дії в межах міжнародних організацій: «Набуття нових технологій для розвитку вітчизняних підприємств також буде здійснюватися шляхом участі в європейських ініціативах, орієнтованих на інноваціях, через двостороннє співробітництво і в рамках міжнародних організацій» [186, с. 20]. Також вказано, що з огляду на «всезагальні процеси глобалізації» та зумовлене ними виникнення взаємозалежностей між державами, міжнародне співробітництво має вирішальне значення для створення безпеки глобального кіберпростору» [186, с. 20].

Підсумовуючи, віртуалізація території в Стратегії кібербезпеки Польщі проглядається на двох рівнях: територіальності та позатериторіальності. У документі наголошується, що потрібно розвивати транскордонне співробітництво, зокрема через міжнародні структури, а також взаємодіяти на рівні міжнародних організацій. Крім простору міжнародних організацій та національної території, в цьому документі акцентовано на намірі творити синергію внутрішньої та міжнародної діяльності у сфері кіберпростору. Тут простежується ідея позатериторіальності. Однак помітна і протилежна

тенденція, коли межі національного впливу визначаються кордонами держави, які окреслюють межі внутрішньої та зовнішньої політики. Тож можна дійти висновку, що Польща схильна діяти за принципами та територіальності, акцентуючи на тому, що відбувається в межах її кордонів.

Отже, аналіз того, як питання державної території врегульовується стратегіями кібербезпеки трьох держав, можна дійти висновку, що нині всі вони лише частково переходять до принципів віртуалізації. Детериторіалізація проглядається у боротьбі з кіберзлочинністю, що вимагає об'єднання зусиль, поділі світу на простір «однодумців» та «ворогів» (що особливо чітко простежується в документі США), а не на країни, що існують в межах їхніх територій. У розвитку економічних ініціатив кордони також визначаються як певною мірою зайві. Одначе, поділ на внутрішні та зовнішні політичні процеси (що присутній в німецькій та польській стратегіях) свідчить про дотримання принципу територіальності.

3.3. Відображення механізмів віртуалізації уряду на прикладі кіберстратегій аналізованих держав

В питаннях віртуалізації уряду США демонструють готовність максимального переходу в кіберпростір. Зокрема гарантується, що в усіх органах державної влади буде встановлене відповідне програмне забезпечення, уряд сприятиме навчанню працівників тощо. «Федеральний уряд забезпечить, щоб системи, якими він володіє та користується, відповідали стандартам та передовим практикам промисловості […]. Федеральний уряд також буде лідером у розробці та впровадженні стандартів й передового досвіду в нових сферах» [185, с. 8]. Також у Стратегії кібербезпеки США артикульована вимога до департаментів та інших органів влади видаляти програмне забезпечення, яке є вразливим до різних безпекових ризиків.

У документі зазначено, що США регулярно стає жертвою злочинної кібердіяльності, що здійснюється державними та недержавними суб'єктами, терористами, які використовують мережеву інфраструктуру в США і за

кордоном. Відтак у Стратегії висловлений намір унормувати обов'язки правоохоронних органів щодо затримання, переслідування злочинців, знищення кримінальної інфраструктури, обмеження розповсюдження та використання шкідливих кіберможливостей, попередження діяльність кіберзлочинців і їхніх спонсорів, які отримують прибуток від незаконної діяльності тощо. Важливо, що в цьому документі про кіберзлочинність йдеться найперше в контексті транскордонної діяльності, тобто міжнародних відносин. При цьому важливо, щоб відповідальність за кіберуразливість несли безпосередньо керівники всіх підрозділів владних органів.

Зазначено, що процвітання і безпека США залежать саме від того, як влада реагує на можливості та виклики в кіберпросторі. Тож захист кіберпростору визнаний фундаментальним принципом ефективного функціонування федерального уряду. Стратегія закладає основи для централізованого управління процесом технологізації через затвердження стандартів, директив в Адміністрації президента [185, с. 7].

Попри провідну роль уряду в розвитку технологій та гарантуванні безпеки держави, Стратегія кібербезпеки США акцентує, що важливим і впливовим стає новий актор політичного процесу – постачальники інформаційно-комунікативних технологій. Вони «мають унікальне значення для виявлення, запобігання та згладження ризиків, перш ніж вони вплинуть на клієнтів, тож Федеральний уряд повинен співпрацювати з цими постачальниками, щоб поліпшити безпеку та стійкість ІКТ цілеспрямовано та ефективно, захищаючи приватне життя та громадянські свободи» [185, с. 9].

Отже, віртуалізація уряду в Стратегії кібербезпеки США проглядається у розширенні технологічних можливостей органів державної влади та залученні до процесу управління нового суб'єкта – постачальника інформаційно-комунікативних технологій. Вони на рівні з керівниками підрозділів органів державної влади повинні нести відповідальність за безпеку користування інформаційно-комунікативними технологіями.

Віртуалізація уряду ФРН має кілька вимірів. Передусім визнається його залежність від подій та тенденцій у кіберпросторі. «Напади на державні установи з метою шпигунства або саботажу можуть значно погіршити функціонування адміністрацій, збройних сил і органів безпеки, а отже, мати вплив на громадську безпеку та порядок» [157, с. 7]. Аби відповідати вимогам часу, федеральний уряд розробив план дій щодо оцифровування результатів діяльності управлінь, зокрема створивши проєкт «Мережа федерального уряду» (Netze des Bundes) [187]. Цей проєкт покликаний створити спільну інфраструктуру кібербезпеки на найвищому рівні; до неї мали б повністю переходити міжвідомчі мережі. Проєкт виконує функцію інтеграційної платформи для всіх віддалених мереж федеральної адміністрації, надаючи консультації та експертні поради в процесі переходу до оцифрованого способу взаємодії. Як результат, в майбутньому всі дані мали б транспортуватися до безпечної та високодоступної мережі, а недієві канали мали б бути усунені [187].

Доцільність функціонування такої структури підтверджується статистичними даними (станом на 2016 рік): щодня на адміністративні мережі здійснюються кібератаки, урядові мережі стикаються з близько 400-а нападами; щомісяця надходить понад 44 тис. інфікованих електронних листів; щодня стаються близько 3,6 тис. спроб під’єднатися до серверів зі неправильним кодом; щомісяця органи влади стикаються з 95 тис. шкідливих програм і близько 200-а шкідливими вірусами програмного забезпечення [187]. Німецькою стратегією передбачено, що запуск такого проєкту спростить процес пристосування органів державної влади до все складніших викликів кіберпростору. Завдяки таким діям виникають можливості для створення цифрового уряду (digital government), що здатен діяти в кіберпросторі та протидіяти всім його небезпекам.

Аби впоратися з новими небезпеками в процесі свого функціонування, німецький уряд створює та підтримує на державному рівні спеціальні органи, які відповідальні за кібербезпеку. Так, федеральний офіс кримінальної поліції

відповідає за створення спеціалізованого слідчого підрозділу (групи швидкого реагування), який, консультуючись з відповідним прокурором, повинен здійснювати перші невідкладні заходи кримінального провадження для прокуратури. Створюються «мобільні кіберкоманди», що складаються з ІТ-фахівців, фахівців з оцінки кібератак [157, с. 29].

Крім того, держава створює урядові та неурядові «команди з реагування на надзвичайні ситуації» (Computer Emergency Response Teams») [157, с. 34] як центральні контактні пункти для профілактичних та реактивних технічних заходів у секторі ІТ-безпеки, що становить важливий для держави блок в постійній архітектурі кібербезпеки. Також держава надає німецьким органам правопорядку та безпеки право розшифровувати або оминати зашифровані повідомлення, якщо це необхідно для виконання їх повноважень [157, с. 15].

Органом, що має стати платформою для стратегічного діалогу та оперативного обміну між органами влади, є Рада кібербезпеки. Крім того, федеральний уряд розширив межі дослідницької програми для безпеки в ІТ – «Самовизначення та безпека в цифровому світі 2015–2020», – і тісно взаємодіє з іншими заходами у сфері кібербезпеки, серед яких – Ініціатива з інформаційної безпеки в бізнесі, Німецький центр компетенції проти кіберзлочинності та ін.

ФРН також артикулює прагнення посилити спроможність реагувати на кібернебезпеки на місцях, зокрема і через створення нових органів, які б ефективно взаємодіяли з різними суб’єктами на федеральному рівні, і при цьому зважали на інтереси федеральних земель, які є у складі ФРН.

Очевидно, що важливою сферою віртуалізації ФРН є перетворення її апарату примусу на такий, що здатен ефективно діяти в кіберпросторі. І це стосується не лише поліції та прокуратури, а й війська. «Як високотехнологічна армія, що залучена по всьому світі, Бундесвер постійно відчуває небезпеки в умовах кіберпростору. Водночас використання кіберпростору є передумовою оперативної спроможності збройних сил. Кіберзахист і кібербезпека повинні бути інтегровані в усі плани, структури та процеси загальної оборони» [157, с. 33], – вказано у Стратегії. Щоб дозволити Бундесверу виконувати свої завдання

в кіберпросторі, розширюються повноваження федеральних збройних сил, узгоджується архітектура безпеки їхніх ІТ-систем.

Як і в американському документі, особливістю процесу діджиталізації держави є співпраця уряду з новими гравцями – провайдерами інформаційно-комунікативних послуг і розробниками технологій. Передусім, на цих постачальників покладено відповідальність захищати користувачів від кіберзагроз, сприяти у виявленні кіберінфекцій та згладжувати негативні наслідки від здійснених кібератак. При цьому провайдери повинні захищати державну таємницю та конфіденційну інформацію користувачів, адже саме довіра має стати основною засадою Інтернет-комунікації [157, с. 25].

Попри усвідомлення взаємозалежності світу, в стратегії зазначено: «в епоху діджиталізації суверенітет ФРН повинен бути забезпечений» [157, с. 8], і наголошено: держава здатна зробити ризики, пов’язані з процесом діджиталізації, керованими.

Отже, віртуалізація німецького уряду проглядається в перетворенні самого уряду – переходу його в кіберсферу через створення спеціальних органів, що покликані регулювати віртуальні відносини та консультувати державні органи в процесі переходу в цю сферу. Крім того, важливим в процесі віртуалізації органів державного примусу є те, що і поліція, й армія розглядаються як такі, що повинні мати скоординовану та високотехнічну систему нагляду за кіберпростором й завчасно відповідати на його загрози. Крім того, за поліцією зберігається право обходити механізми ідентифікації та шифрування в разі необхідності. Розширення спектра можливостей та викликів, пов’язаних з процесом включення держави до віртуального простору, зумовлює те, що держава змушена звертатися за допомогою до провайдерів – цілком нових суб’єктів політичного процесу, в руках яких зосереджена влада захищати технологічні системи, дані та відповідати на загрози та напади. Попри те, документ зазначає, що навіть за таких перетворень ФРН не відмовляється від жодних ознак власного суверенітету, який має забезпечуватися. Як й американська стратегія, німецький документ прописує взаємодію з новими

учасниками політичного процесу та необхідність розширювати технологічну потужність органів державної влади. Проте тут детальніше розписані національні структури, що борються з кіберзлочинами на території держави та в інформаційному просторі.

Віртуалізація уряду Польщі полягає в запровадженні нових технологій управління державою. Більше уваги зосереджується на технічному, а не на світоглядному аспекті проблеми, як це зроблено в американському документі.

У польській стратегії визначені основні напрями діяльності уряду в цій сфері: законодавчий, інструментальний, організаційний. Перший полягає в тому, що на міністрів покладено обов’язок підготувати пропозиції щодо законодавчих змін у сфері кібербезпеки; відповідальний за діджиталізацію міністр у співпраці з іншими міністерствами повинен переглянути галузеві та спеціальні нормативні акти, які можуть мати вплив на інші сфери, наприклад, захист персональних даних [186, с. 9].

Відмінним, у порівнянні з іншими стратегіями, є те, що в польському документі закріплено необхідність розглянути можливість правового регулювання так званих програм «bug bounty», завдяки яким люди можуть вносити корективи до роботи певної програми, виправляючи помилки та отримуючи винагороду.

Зазначено, що забезпечення комп’ютерної безпеки Рада міністрів розглядатиме як пріоритет і до 2022 року Польща має стати більш стійкою до атак і загроз, що виникають через зростання кіберзлочинності. Це встановлює певні часові межі та критерії для оцінки досягнень за вказаний період.

Раніше суб’єкти цивільного, військового, державного та приватного секторів, а також інституції, що відповідають за боротьбу з кіберзлочинністю, мали розпорошений характер, а це безпосередньо впливало на те, що їхня діяльність була неефективною. Тож важливим завданням віртуалізації уряду є передусім консолідація та гармонізація діяльності всіх зацікавлених сторін, до яких належать й органи, відповідальні за громадську безпеку,

антитерористичну діяльність, внутрішню безпеку та громадський порядок, прокуратура та судова система [186, с. 11].

Інформувати про ризики покликана спеціальна система поточного управління безпекою в кіберпросторі. Ця система дасть змогу повідомляти про загрози та вразливі місця служб. Загальною проблемою у сфері кібербезпеки визнане небажання суб'єктів обмінюватися інформацією про спостережувані загрози, інциденти та оцінені збитки. Аби цьому запобігти створюється національна мережа «команд з реагування на надзвичайні ситуації». У польській Стратегії перечислюються їхні види – національна, галузева, комерційна та підприємницька, які б утворювали мережу та обмінювалися ключовою інформацією про загрози для безпеки та інциденти в секторі державного управління. Окрім таких команд швидкого реагування передбачено створення та розвиток спеціалізованих структур, що займатимуться виключно проблемами кібербезпеки: «Національний центр з кібербезпеки, центри реагування на інциденти (галузеві CSIRT), центри обміну інформацією [186, с. 9].

Як і ФРН, Польща передбачає спроможність своїх збройних сил здійснювати операції й у кіберпросторі. Польська армія розглядається як основний елемент державної оборонної системи, що повинна здійснювати операції у сфері кіберзлочинності так само ефективно, як і в повітрі, на суші та морі [186, с. 16]. А весь спектр військових операцій у кіберпросторі передбачає: визначення загроз, оборону та захист комп'ютерних систем, боротьбу з джерелами небезпек тощо. Тож можна прослідкувати слідування ідеям «твердої сили».

Польський уряд декларує намір інвестувати в розвиток промислових і технологічних ресурсів, створюючи умови для розвитку підприємств, науково-дослідних центрів, а також стартапів, бізнес яких полягає у напрацюванні нових рішень, зокрема у сфері кібербезпеки. Цікаво, що уряд засвідчує своє бажання втримувати високо кваліфікованих працівників в галузі, тож зобов'язується запроваджувати програми стимулювання, зокрема урядову програму «Золота

сотня» [186, с. 22]. Програма спрямована на фахівців з інформаційних технологій та кібербезпеки, зайнятих у державному управлінні.

Фактично польська стратегія розширює урядову юрисдикцію та компетенцію, що передбачає розвиток нових навичок та розширення сфери повноважень органів, що вже сформувалися. Уряд зобов'язаний до взаємодії з новими акторами, найперше – суб'єктами господарювання, що надають послуги з використанням комп'ютерних систем, наприклад, провайдерами цифрових послуг (платформ онлайн-торгівлі, пошукових систем і хмарних сервісів). Враховуючи, що відповідальність за забезпечення безпеки послуг покладається насамперед на суб'єктів, що їх надають, польський уряд вживає заходів, що сприятимуть розбудові можливостей і компетенції кібербезпеки серед операторів ключових послуг, операторів критичної інфраструктури та постачальників цифрових послуг, враховуючи їхні особливості та рівні зрілості у сфері кібербезпеки [186, с. 13].

В процесі діджиталізації важливою є роль експертів, що взаємодіють з академічним середовищем, розробляючи нові стандарти та рекомендації. Неурядові організації та аналітичні центри, як засвідчує польський досвід, є корисними як організатори освітньої діяльності в суспільстві, постачальники даних для державного управління, тобто їх уряд залучає до розв'язання викликів у кібербезпеці.

Отже, віртуалізація уряду в Стратегії кібербезпеки Польщі передбачає кілька вимірів: законодавчий, інструментальний, організаційний. Законодавчий полягає в декларуванні наміру підготовки законодавчих змін сфери кібербезпеки, перегляді чинного законодавства. Організаційний вимір віртуалізації проглядається у встановленні часових меж реалізації Стратегії – до 2022 року. Важливо також об'єднати розпорошені станом на сьогодні структури, що повинні стежити за безпекою в кіберпросторі, підвищивши ефективність їхньої діяльності.

Передбачено, що польська армія також повинна долучатися до національних і міжнародних навчань, для підвищення спроможності діяти у

кіберпросторі. Збройні сили Республіки Польща розглядаються основним елементом державної оборонної системи, що також повинні діяти в кіберпросторі. Розширюючи свою юрисдикцію в кіберпросторі, польський уряд переходить до взаємодії з новими акторами. Мова про суб'єктів господарювання, що надають послуги з використанням комп'ютерних систем, зокрема провайдерами цифрових послуг, а також неурядовими організаціями та аналітичними центрами.

Інструментальний вимір віртуалізації уряду означає опис специфічних механізмів, платформ, організацій, що відповідатимуть за налагодження порядку в кіберпросторі. Так, правоохоронні органи розширили свої повноваження. Аби гарантувати безпеку, заплановане створення спеціальної системи управління, а також спеціалізовані структури, що займатимуться виключно проблемами кібербезпеки.

Отже, проаналізувавши процеси віртуалізації уряду, описані в стратегіях кібербезпеки США, ФРН і Польщі, визначимо спільні тенденції. По-перше, в усіх документах відзначено, що уряд повинен орієнтуватися на найвищі стандарти технологічного розвитку, напрацьовувати здатність швидко діяти в кіберсфері, відповідаючи на кіберзлочини та попереджаючи їх. По-друге, розширюючи свою юрисдикцію на кіберпростір, уряд вступає у взаємодію з новими акторами, зокрема суб'єктами господарювання, що надають послуги з використанням комп'ютерних систем (провайдерами цифрових послуг) а також з неурядовими організаціями та аналітичними центрами.

«Оцифровування» шляхів взаємодії органів зі всією безпековою інфраструктурою дає підстави говорити про розвиток електронного уряду. Відмінним є те, що в документах неоднакова увага приділяється тому, як має виглядати національна мережа органів протидії кіберзлочинності (в американському документі цього немає), а також в тому, як визначаються кіберзлочини. Зокрема, в США виражена тенденція розглядати кіберзлочини як злочинну діяльність інших держав, що прагнуть підірвати американську

могутність. Натомість у стратегіях Польщі та ФРН більше звернено уваги на механізми власного реагування на такі інциденти.

3.4. Віртуалізація міжнародних відносин у стратегіях кібербезпеки

Аби проаналізувати процеси віртуалізації міжнародних відносин, в які вступає держава, звернемо увагу на те, як змінюється розуміння державною її суверенітету, на яких підставах вона готова взаємодіяти з іншими державами, а що буде достатньою підставою для відмови від можливості вступати у такі відносини.

Серед головних завдань США, сформульованих у національній Стратегії кібербезпеки, – розширення американського впливу за кордоном з метою розширення ключових принципів відкритого, придатного для взаємодії, надійного та безпечного Інтернету [185, с. 29]. У цьому документі не прописано жодного пункту, що давав би підстави говорити від навіть часткову відмову США від державного суверенітету. Навпаки, акцентовано на збереженні могутності США та їх статусі світового лідера. У тексті документа увиразнена впевненість, що країні вистачить могутності та людського потенціалу впоратися з новими викликами та супротивниками: «Інтернет створив величезні переваги всередині країни і за кордоном; він допомагає просувати американські цінності свободи, безпеки та процвітання. Водночас разом з його розширенням прийшли проблеми, що загрожують нашій національній безпеці. Відтак США демонструватимуть послідовний і комплексний підхід до вирішення цих та інших завдань для захисту американських національних інтересів у дедалі висхідному цифровому світі. Мета: зберегти вплив США на технологічну систему та розвиток кіберпростору як двигуна економічного зростання, інновацій та ефективності» [185, с. 21].

США висловили готовність слідувати нормам міжнародного права, зазначаючи, що уряд наполягатиме на ефективному використанні наявних міжнародних інструментів, розроблених для боротьби з транснаціональною організованою злочинністю. Декларується намір зміцнювати міжнародний

консенсус задля виконання Конвенції Ради Європи про кіберзлочинність (Будапештської конвенції) [185, с. 11].

В американському документі чітко визначені супротивники держави на міжнародній арені – Російська Федерація, Іран, Північна Корея, КНР і терористичні організації, що намагаються підірвати авторитет США цифровими способами. Зокрема «Китай займався кіберналагодженим економічним шпигунством і крадіжками в розмірі трильйонів доларів у сфері інтелектуальної власності. Недержавні актори – зокрема терористи та інші злочинці – експлуатували кіберпростір для отримання прибутку, рекрутингу, пропаганди та нападу на США, їхніх союзників і партнерів. Ці дії часто були вигідні ворожим державам» [185, с. 1–2].

США залучені до постійної конкуренції зі стратегічними супротивниками, державами, що не дотримуються загальних правил, терористичними та злочинними мережами. Названі вище держави використовують кіберпростір для того, щоб кинути виклик США та союзникам. Вони прагнуть через кіберінструменти підірвати американську економіку та демократію, викрасти інтелектуальну власність, сіяти розбрат у демократичних процесах: «Ми вразливі до кібератак на об’єкти критичної інфраструктури в мирний час. Зростає ризик того, що ці країни будуть здійснювати кібератаки проти США під час кризи, аж до початку війни» [185, с. 2].

Тут проглядається один з головних критеріїв державної віртуалізації – перенесення конфліктів в інформаційних простір. Вони небезпечні з огляду на те, що їхня організація потребує менше затрат, тож навіть фінансово незабезпечений суб’єкт може їх організувати, поставивши під сумнів легітимність влади загалом. Це можна спостерігати в дискусії про російський вплив на президентські вибори в США 2016 року [25].

США задокументували готовність боротися проти злочинного онлайн-впливу та інформаційних кампаній, недержавної пропаганди та дезінформації. «Це передбачає роботу з іноземними урядовими партнерами, а також приватним сектором, науковими колами та громадянським суспільством для

виявлення, протидії та запобігання використанню цифрових платформ для зловмисних операцій зовнішнього впливу з дотриманням громадянських прав і свобод» [185, с. 21]. У цьому проглядається бажання відстояти свої цінності не лише в кіберпросторі, а й в громадській свідомості, а для цього залучаються нові суб'єкти-інтелектуали, що означає звернення до механізмів «м'якої сили». Акцент на цифрових механізмах боротьби за американські цінності та процвітання дає підстави говорити про розширення механізмів «м'якої сили», адже в документі не йдеться про пряме залучення національних збройних формувань.

Американська адміністрація акцентує на розширенні можливостей притягнути до відповідальності кіберзлочинців і закликає поширювати інформацію про всякі намагання порушити правила взаємодії в інформаційному просторі. США не переходять цілком на «м'яку силу»; країна готова захищати свої позиції методами «твердої сили».

Тож у межах віртуалізації взаємодії на міжнародній арені впадає в вічі прирівняння кіберзагроз до небезпек у фізичному просторі. Серед цих небезпек й економічні, політичні, а також ті, що загрожують об'єктам критичної інфраструктури та зв'язку. США чітко називають своїх супротивників – як державних, так і недержавних, а також констатують, що повинні забезпечити країну всіма механізмами для того, що вона могла відповісти на загрози. Всяке використання інформаційного простору, здійснене з порушенням прав і свобод людини, США розглядає як зазіхання на власну могутність, сигнал про ймовірну підготовку до фізичного конфлікту. Слідування правовим ініціативам та готовність працювати над поглибленням консенсусу, зокрема і через громадські організації, дають підстави стверджувати, що США працюватимуть над створення глобального консенсусу, проте мають бажання ввійти у кіберсередовище на правах лідера.

В німецькій Стратегії кібербезпеки наголошено на сучасних змінах поведінки, до якої вдаються сторони під час конфлікту: «Політично-військові конфлікти часто супроводжуються кіберкампаніями або здійснюються в

кіберпросторі напередодні збройного конфлікту» [157, с. 7], – йдеться в документі. Цим констатується, що кіберкампанії держава може сприймати як попередження про намір вступити в реальний конфлікт з іншою державою.

Як член НАТО, ФРН декларує готовність стати невіддільною частиною процесу адаптації Альянсу до мінливого середовища безпеки з метою підвищення стійкості союзників та Альянсу загалом, а також для підвищення превентивних та оборонних потуг у контексті гібридних загроз [157, с. 7]. Відбувається інституціоналізація гібридних загроз, розв'язання яких належить до обов'язків держави та міжнародних військових організацій. А через законодавство кіберпростір має бути визнаний як операційний простір для НАТО.

На відміну від США, які в Стратегії кібербезпеки називають своїх супротивників, ФРН утримується від назв країн-конкурентів. Проте в документі вказано, що країна перебуває в центрі уваги іноземних розвідувальних служб. Відтак кібершпигунству та кіберсаботажу потрібно ефективно протидіяти. Для іноземних розвідувальних служб кібератаки на ІТ-системи державних установ, підприємства та науково-дослідних установ, а також їхніх співробітників становлять важливий метод отримання інформації [157, с. 31]. Федеральний уряд ФРН задекларував намір інтенсивно стежити за всіма видами діяльності іноземних спецслужб на території держави.

Попередження кіберзлочинів, міжнародна кіберполітика і кібероборона – три методи досягнення кібербезпеки в ФРН, що доповнюють одне одного. При цьому оборонна спроможність Бундесверу в кіберпросторі – також невіддільна частина кібербезпекової архітектури [157, с. 33]. У такий спосіб держава декларує готовність не відступати від механізмів «твердої сили» та доносить, що переміщує в кіберпростір небезпеки, притаманні географічному простору. Інститут держави тут покладається радше на інструменти примусу, а не мотиваційні механізми, тобто стратегії «м'якої сили». Тож «м'яка сила» в Стратегії кібербезпеки ФРН видається менш важливим механізмом впливу на

політичну ситуацію, ніж це декларується в аналогічному американському документі.

ФРН зорієнтована на активну позицію на міжнародній арені, щоб допомогти іншим акторам напрацювати спільні стандарти кібербезпеки. Держава висловлює готовність працювати над посиленням міжнародного кримінального переслідування (у цьому наміри ФРН і США збігаються). Водночас федеральний уряд зобов'язується й надалі використовувати відповідні та єдині стандарти безпеки для ІТ.

ФРН підтримує раніше прийняті принципи дії в кіберпросторі, наприклад, Спільні Критерії оцінки інформаційної безпеки (Common Criteria [194] та ISO/IEC 15408, ISO/IEC 27000), серед яких – конфіденційність, цілісність, доступність. Вони передбачають, що не можна несанкціоновано ознайомлюватися з інформацією, яка захищена, змінювати інформацію, порушуючи її цілісність, порушувати правила доступу до комп'ютерних систем або оброблюваної інформації. Посилання на ці документи та ініціативи засвідчують, що ФРН готова активно підтримувати всякі ініціативи, зорієнтовані на створення міжнародних стандартів належного захисту від маніпулювання та зловживання інформацією.

Також німецькі учасники політичного процесу повинні дотримуватися проєктів ЄС щодо правових, технічних питань, пов'язаних з транскордонною обробкою та використанням даних. «Важливими елементами є транскордонне застосування електронної ідентифікації, кваліфікованого електронного підпису, електронної печатки для компаній та органів влади та інших електронних довірчих послуг» [157, с. 40].

Не стверджуючи, що займатиме провідну позицію, ФРН усе ж зазначає, що в межах ООН продовжуватиме долучатися до роз'яснення питань щодо застосування міжнародного права в кіберпросторі та його розвитку. «Двосторонні консультації та співпраця з вибраними країнами-партнерами можуть поглибити цей процес і допомогти в досягненні глобального мінімуму кібербезпеки» [157, с. 39]. Тобто, попри те, що в документі не названо жодних

«ворожих», «конкурентних» суб'єктів, є зрозуміло, що співпраця вважається важливою не з усіма державами, а лише з «вибраними».

Консультування та підтримка іноземних країн здається пріоритетним завданням, сформульованим Стратегією кібербезпеки ФРН. Зокрема федеральний уряд декларує ініціативу створення Німецького інституту міжнародної кібербезпеки, метою якого є залучення бізнесу, науки та неурядових організацій до розроблення рішень в інтересах міжнародної стабільності та запобігання кризам [157, с. 41]. Також ФРН зорієнтована на надання підтримки окремим країнам і регіонам-партнерам у розробці та покращенні профілактичних, реактивних потужностей у сфері кібербезпеки.

Отже, віртуалізація відносин з іноземними державами для ФРН полягає в визнанні гібридних загроз такими, що є справді небезпечними, та розв'язання яких повинне бути віднесене до компетенції держави. Відповідно до цього визнання, нині відбувається узгодженість дії держав та суб'єктів політичного процесу на міжнародній арені, зокрема з діяльністю НАТО. Кібербезпека, що передбачає механізми регулювання лише на національному рівні, визнається недостатньою для дотримання стандартів, прийнятих зокрема європейськими політиками, а ФРН регламентує свою готовність дотримуватися всіх раніше прийнятих в ЄС та інших міжнародних організаціях норм кібербезпеки. ФРН акцентує на важливості включення кіберпросторових подій до компетенції військових організацій (НАТО, Бундесверу), однак бере до уваги радше той аспект діяльності, який можна назвати «твердою силою». Не стверджуючи, що ФРН прагне зайняти визначальну роль у формуванні міжнародної політики, ця держава декларує готовність займати активну позицію у формуванні міжнародних стандартів кібербезпеки та в процесі надання консультативних послуг щодо дотримання прав людини та попередження кіберзагроз.

Як і в інших аналізованих документах, в Стратегії кібербезпеки Польщі визнано існування гібридних загроз, атак гібридного характеру. Віртуалізацію відносини між Польщею та іншими державами, що відбувається під впливом процесів діджиталізації та медіатизації, можна поділити на процеси в

глобальному та регіональному рівні. У глобальному масштабі передусім йдеться про необхідність підвищення здатності протистояти кіберзлочинності, зокрема кібершпигунству, терористичним інцидентам і гібридним операціям, надаючи підтримку ключовим постачальникам послуг, постачальникам цифрових послуг та операторам критичної інфраструктури – у виявленні та боротьбі з інцидентами в усьому світі на всіх етапах [186, с. 16].

Глобальний вимір віртуалізації ініційований також діяльністю НАТО, що 2016 року на Варшавському саміті визнав кіберпростір напрямком оперативної діяльності, а дії у кіберпросторі такими, що мають бути передбачені в оперативному плануванні та стати невіддільною частиною операцій польських збройних сил, а також Альянсу та коаліції [186, с. 16]. Відтак назріла потреба вдосконалення військових структур для забезпечення більш ефективного планування, командування та управління ресурсами, навичками та здібностями.

Польща визнає, що спровоковані діяльністю в кіберсфері конфлікти можуть бути як державного, так і недержавного характеру: «Зловмисники можуть бути як злочинними групами, що діють з метою отримання прибутку, з терористичними намірами, так і групами, за якими стоять іноземні держави. Такі дії використовуються для отримання інформації, що дестабілізує політику, економіку, провокує суспільне незадоволення» [186, с. 4].

Безпеки в кіберсфері потрібно дотримуватися, оскільки через нього пов’язуються різні країни у єдиний простір: «Це особливо важливо й з того погляду, що Польща тісно пов’язана з іншими країнами через міжнародне співробітництво в межах ЄС, НАТО, ООН, ОБСЄ. Ця співпраця відіграє важливу роль у боротьбі зі наростальною кількістю інцидентів, спричинених незаконною діяльністю в кіберпросторі, що призводить до матеріальних і іміджевих втрат» [186, с. 4]. Акцентуючи на іміджевих втратах, Польща дає зрозуміти, що такий ресурс вона також розглядає важливим, проте в документі не прописано дії, якими вона планувала б оберігати чи поширювати позитивний імідж країни. Тож засоби, які можна було б трактувати як «м’яку силу», в польському документі не прописані.

Отже, на глобальному рівні наявні спроби Польщі об'єднати зусилля міжнародних акторів у запобіганні та протидії кіберзлочинам, гібридним небезпекам, джерелом яких є як злочинні групи, так і держави. На регіональному рівні віртуалізація відносин між державами простежується у взаємодії Польщі в межах міжнародних форумів, наприклад ОБСЄ, щодо зміцнення довіри та заходів безпеки, у намірах посилювати співпрацю в рамках Вишеградської групи, з державами Ради держав Балтійського моря. Спільно з учасниками згаданих організацій Польща матиме змогу долучитися до організації навчань і тренінгів, що відбуватимуть як з ініціативи національних держав, так і з ініціативи міжнародних організацій. В межах таких навчань Польща планує розробити рекомендації щодо вдосконалення системи кібербезпеки [186, с. 24].

Таке удосконалення також можливе через участь у міжнародних форумах, створених для обміну інформацією про загрози в кіберпросторі. З огляду на це важливо врегулювати діяльність провайдерів цифрових послуг окремим режимом. «Уряд цілком усвідомлює міжнародну специфіку цих суб'єктів, а також необхідність створення таких правил, які сприятимуть розвитку цифрового ринку в Польщі» [186, с. 13], – йдеться в документі. Тобто, відносини у кіберпросторі ще потребують унормування.

Польща заявляє про своє бажання бути залученою до розробки міжнародної системи оцінювання та сертифікації на основі міжнародних норм і стандартів, визнаючи інші вимоги до документів і комп'ютерних систем, що були прийняті на міжнародному рівні, зокрема Спільні Критерії оцінки інформаційної безпеки. Польща готова активізуватися, щоб гарантувати безпеку для єдиного цифрового ринку як рушія економічного зростання та інновацій.

У цьому випадку автори польської стратегії оперують радше класичним визначенням держави. Щоб набути навичок, розвинути знання та обмінятися передовим досвідом, Польща приділятиме щораз більше уваги міжнародному,

двосторонньому та багатосторонньому співробітництву в питаннях освіти, навчання, а також розбудові інформаційного суспільства.

Отже, віртуалізація відносин Польщі з іншими державами не сформована, а, радше, відбувається за принципами міжнародної політики класичної держави, що переносить у кіберпростір аналогічні правила поведінки, які діяли в географічному просторі. Попри це доцільно розглядати польський план захисту кіберпростору на глобальному та регіональному рівнях.

На глобальному рівні передусім йдеться, що безпека в кіберсфері – необхідна умова взаємодії, бо через неї різні країни пов'язуються в єдиний простір. Тут постає вимога підвищення здатності протистояти кіберзлочинності, зокрема кібершпигунству, терористичним інцидентам і гібридним операціям. Зловмисники можуть бути як злочинними групами, що діють для отримання прибутку, з терористичними намірами, так і групами, за якими можуть стояти іноземні держави.

На регіональному рівні віртуалізація відносин з іншими державами проглядається у намірі взаємодіяти в межах ОБСЄ, ЄС, Ради країн Балтійського моря та іншими організаціями, напрацьовуючи механізми ефективної протидії викликам у кіберпросторі. Водночас Польща висловлює занепокоєння національним іміджем на міжнародній арені, але, крім тверджень про готовність боротися з кіберзлочинами, не прописує механізмів покращення власного іміджу.

Проаналізувавши шляхи віртуалізації міжнародних відносин, виділимо спільні тенденції. Передусім, США, ФРН і Польща визнають існування гібридних загроз як таких, що мають місце на рівні з фізичними небезпеками, супроводжують їх або передують. Спільним є й намір слідувати правовим ініціативам, працювати над поглибленням консенсусу демократичних країн, що співпрацюють у межах міжнародних організацій, узгоджувати дії держав і суб'єктів політичного процесу на міжнародній арені, зокрема з діяльністю НАТО. Зловмисниками створюються протиправні групи, що діють задля

отримання прибутку, з терористичними намірами, а також існують групи, поява яких зазвичай латентно організована іноземними державами.

Відмінними тенденціями в процесі віртуалізації міжнародних відносин є неоднакове визначення своїх супротивників. Якщо США чітко називають конкретні держави-антагоністи, то ФРН і Польща обмежуються описами злочинних намірів та дій, які можуть бути вчинені проти їхніх державних інтересів. По-різному держави визначать і власну роль в процесі віртуалізації: США констатує право лідера, ФРН – готовність виконувати всі міжнародні угоди, а Польща акцентує на взаємодії у сфері кіберпростору на глобальному та регіональному рівнях. Різною мірою держави визнають вагомість механізмів «м'якої сили» в політиці – для США вона дуже важлива, ФРН не згадує про неї, Польща тільки зазначає, що іміджеві втрати теж значущі.

Висновки до розділу 3.

На основі аналізу національних стратегій кібербезпеки США, ФРН і Польщі виділено спільні та відмінні риси процесу віртуалізації держави:

– серед спільних характеристик у питаннях віртуалізації населення у США, ФРН та Польщі визначено спрямованість на підвищення обізнаності громадян в питаннях кібербезпеки, а також широкого кола питань, пов'язаного з функціонуванням цифрової держави, перевагами та потенційними загрозами інформаційного суспільства. Чітко виражена позиція, що в кіберпросторі мають домінувати права та свободи людини. Ідея космополітизму виражено не прослідковується в жодній зі трьох згаданих стратегій;

– віртуалізація державної території аналізується на основі стратегій кібербезпеки аналізованих держав. Детериторіалізація проглядається у: об'єднанні зусиль для протидії кіберзлочинності, що вимагає об'єднання зусиль; поділі світу на простір «однодумців» і «ворогів» (це особливо простежується в кіберстратегії США). У розвитку економічних ініціатив простежується перегляд ролі кордонів, що продиктовано, найперше, економічною глобалізацією. Одначе, розмежування політичних процесів на

внутрішні та зовнішні свідчить про наразі переважання принципу територіальності над принципом детериторіалізації;

– віртуалізація уряду передбачає його зорієнтованість на найвищі стандарти технологічного розвитку, здатність швидко діяти в кіберсфері, реагуючи на злочини в віртуальному вимірі, запобігати їм. В усіх аналізованих державах (а особливо – у США) зростає увага до проблем кібербезпеки, увиразнена орієнтація на удосконалення технологій гарантування мережевої безпеки. Розширюючи свою юрисдикцію на кіберпростір, уряди усіх аналізованих країн взаємодіють із новими акторами – провайдерами цифрових послуг, неурядовими організаціями, аналітичними центрами. Відмінним в процесі віртуалізації урядів є неоднакова увага до того, якою має бути конфігурація національної мережі органів протидії кіберзлочинності, способів реагування на кіберзлочини. Нині пріоритетом аналізованих держав є розробка механізмів захисту від кібератак об’єктів критичної інфраструктури (енергетика, транспортна система, банківський сектор тощо). Особливою агресивністю у наступі на кіберзлочинність віднедавна характеризується США (2018 р. – прийняття нової стратегії);

– віртуалізація міжнародних відносин полягає в низці процесів, спільних для аналізованих держав. Передусім, США, ФРН і Польща визнають існування гібридних загроз та усвідомлюють важливість міжнародної співпраці для запобігання їм. Відмінним є визначення супротивників: США чітко називають конкретні держави (найперше – Росія, Іран, КНР і КНДР); натомість ФРН і Польща обмежуються визначенням потенційних кіберзлочинів, яким мають намір протидіяти. По-різному держави визначають й власну роль у процесі віртуалізації міжнародних відносин: США констатує право лідера і значною мірою наступальну тактику, ФРН – готовність виконувати всі міжнародні угоди, а Польща зорієнтована на взаємодію у сфері убезпечення кіберпростору на глобальному та регіональному рівнях. Відтак аналізовані держави відрізняються за визначенням вагомості механізмів «м’якої сили» в умовах інформаційного суспільства та віртуалізації простору.

РОЗДІЛ 4. ВІРТУАЛІЗАЦІЯ УКРАЇНСЬКОЇ ДЕРЖАВИ: ДОСВІД 2014–2019 РОКІВ

4.1. Особливості населення як класичної ознаки держави за умов віртуалізації інституту держави в Україні

У відносинах України та фізичних осіб, які постійно проживають на її території, не відбулося очевидних зсувів у віртуальний простір. Мова йде, наприклад, про неможливість отримати громадянство онлайн; документи, які підтверджують громадянство України, не мають електронного еквівалента тощо. Принцип єдиного громадянства та неможливості набуття/позбавлення громадянства України означає, що зв'язок між державою та населенням зберігається сильний, віддалений від ідей космополітизму.

У Стратегії кібербезпеки України (2016) відзначено, що забезпечення кібербезпеки нашої держави, як стану захищеності життєво важливих інтересів особи, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися на таких принципах [123]: 1) верховенства права і поваги до прав та свобод особи; 2) забезпечення національних інтересів України; 3) відкритості, доступності, стабільності та захищеності кіберпростору; 4) державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту; 5) пропорційності та адекватності заходів кіберзахисту реальним і потенційним ризикам; 6) пріоритетності запобіжних заходів; 7) невідворотності покарання за вчинення кіберзлочинів; 8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу; 9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних і воєнних цілях; 10) забезпечення демократичного цивільного контролю над утвореними відповідно до законів

України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки.

При цьому принципами, що безпосередньо стосуються питань віртуалізації відносин держави та особи, є: 1) верховенство права, повага до прав і свобод особи; 2) забезпечення національних інтересів України; 3) відкритість, доступність, стабільність і захищеність кіберпростору; 4) пріоритетний розвиток і підтримка вітчизняного наукового, науково-технічного та виробничого потенціалу.

Закріплення принципу верховенства права в Стратегії кібербезпеки означає, що і регулювання відносин у віртуальній реальності повинне відбуватися за тими ж принципами, що не суперечать дотепер визнаній правовій практиці. Так, кіберпростір не породжує нових практик, він стає середовищем апробації та реалізації основних принципів, якими керують демократичні спільноти сьогодні.

Права і свободи громадянина можна обмежувати в певних ситуаціях (війна, відбування покарання тощо), тож верховенство права вже в кіберпросторі передбачає можливість обмеження свобод в Інтернеті, але виключно в ситуаціях, коли особа є у небезпеці або сама творить її. Це принцип правової визначеності: обмеження основних прав людини та громадянина і втілення цих обмежень на практиці допустиме лише за умови передбачуваності застосування цих правових норм. Тобто обмеження будь-якого права повинне ґрунтуватися на чітких критеріях, які дадуть змогу особі розрізняти правомірну поведінку та протиправну, передбачати юридичні наслідки своєї поведінки [21].

Стратегія кібербезпеки передбачає, що в кіберпросторі держава діятиме за принципами поваги до прав і свобод інших. Загалом цей принцип гарантований ст. 68 Конституції України, відповідно до якої кожен зобов’язаний неухильно додержуватися Конституції та законів України, не посягати на права і свободи, честь і гідність інших людей [27].

Серед прав та свобод особи, які держава зобов’язується поважати в процесі досягнення кібербезпеки, передусім важливі ті, що зазначені в

Конвенції про захист прав людини та основоположних свобод, ратифікованій Україною 1997 року. Передусім йдеться про право на життя, заборону катування, рабства і примусової праці, право на свободу та особисту недоторканність, право на справедливий суд, право на повагу до приватного і сімейного життя, свободу думки, совісті та релігії, свободу вираження поглядів, зібрань та об'єднання, право на шлюб, право на ефективний юридичний захист і заборону дискримінації та ін. [61]. Обмеження прав передбачені лише за рішенням суду, під час війни або іншої суспільної небезпеки, яка загрожує життю нації [61].

Ратифікувавши Загальну декларацію прав людини, Міжнародний пакт про громадянські та політичні права, Міжнародний пакт про економічні, соціальні та культурні права, Конвенцію проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання та інші міжнародні правозахисні акти [23], Україна зобов'язалася гарантувати всі права, що, екстраполюючи на кіберзлочини, означає: особи, засуджені за кіберзлочини, користуються всіма правами, передбаченими міжнародними актами. Переслідуючи кіберзлочинців, держава не може вдаватися до катування підозрюваних чи засуджених, поводитися з ними жорстоко, нелюдяно.

У законодавстві простежується, що одним з національних інтересів є формування української ідентичності. Підстави це стверджувати вбачаємо у правках, внесених до низки законів. Важливо згадати про запровадження квот на українському телебаченні. У Законі України «Про внесення змін до деяких законів України щодо мови аудіовізуальних (електронних) засобів масової інформації» зазначено: телерадіоорганізації здійснюють мовлення державною мовою [40]. У загальному тижневому обсязі мовлення телерадіоорганізацій загальнонаціональної та регіональної категорій мовлення, передачі та/або фільми державною мовою, мають становити не менше 75 % загальної тривалості передач та/або фільмів (або їх частин) у кожному проміжку часу між 07.00 та 18.00 і між 18.00 та 22.00 [40]. Новинні передачі також повинні вестися державною мовою в обсязі не меншому 75 % загальної тривалості новин,

поширених телерадіоорганізацією у кожному проміжку часу між названими вище годинами [40]. А передача вважається виконаною державною мовою, якщо виступи (репліки) ведучих (дикторів) передачі, осіб, які беруть участь у передачі, виконані, дубльовані, українською мовою.

Визначення мови телерадіомовлення дає підстави стверджувати, що держава намагається контролювати процеси творення ідентичності, впливаючи на інформаційний та кіберпростір, творячи національну ідентичність. У процесі виконання цього рішення має формуватися український культурний продукт. Такий намір проглядається і в змінах до Закону України «Про кінематографію» (1998) [46]. У ньому можна побачити «культурне протистояння» між Україною та Російською Федерацією, яку 2018 року було визнано агресором. Зокрема ст. 15-1 цього закону визначає: «В Україні забороняється розповсюджувати і демонструвати фільми, що містять популяризацію або пропаганду органів держави-агресора та їхніх окремих дій, що створюють позитивний образ працівників держави-агресора, працівників радянських органів державної безпеки, виправдовують чи визнають правомірною окупацію території України, а також забороняється транслювати (демонструвати шляхом показу каналами мовлення) фільмів, вироблених фізичними та юридичними особами держави-агресора [46]. Крім того, закон забороняє кінофільми, що популяризують або пропагують органи держави-агресора та їхніх окремих дій, створюють позитивний образ працівників держави-агресора, працівників радянських органів державної безпеки, виправдовують чи визнають правомірною окупацію території України [46].

Згадані норми важливі при аналізі процесів віртуалізації держави, оскільки вони відбивають державні механізми формування ідентичності в інформаційному просторі. Ці норми демонструють, що держава зберігає важелі впливу на інформаційний простір, що стає полем політичного протистояння в результаті поширення певних ідей чи пропаганди. Для цього Україна визначає критерії забороненого контенту та заборонених мотивів у сюжетах і наративах.

В межах порівняльного контент-аналізу було виміряно кількість використання у Стратегії слова «національний» – 34 рази. Для порівняння: у американській – 35, німецькій – 28, польській – 76 разів. З огляду на те, що обсяг українського документа становить приблизно 2 670 слів (американська – 8 900 слів, німецька – 8 750, польська – 7 440), доходимо висновку про значну частоту використання категорії «національний» в українському документі. Отже, дотримуючись принципу забезпечення національних інтересів України, кібербезпеку законодавець підпорядковує національним інтересам, що повинна виявляти загрози проти національної безпеки.

Принцип відкритості, доступності, стабільності та захищеності кіберпростору закріплений Законом України «Про основні засади забезпечення кібербезпеки України». Він передбачає принцип мінімально необхідного регулювання, за яким рішення суб’єктів владних повноважень повинні бути необхідними та мінімально достатніми для досягнення мети і завдань кібербезпеки [50].

У Стратегії кібербезпеки України зазначено, що розвиток безпечного, стабільного і надійного кіберпростору передбачає розвитку технологій кіберзахисту засобів рухомого зв’язку, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв’язку [123]. Безпечний кіберпростір позначає співвідношення відкритості та обмеження доступу до інформації. Йдеться про те, що в умовах інформаційного суспільства виникає необхідність захистити інформацію з обмеженим доступом. А також йдеться про протидію комп’ютерній злочинності та комп’ютерному тероризму, що є необхідною передумовою функціонування усіх галузей виробництва, водночас об’єктів критичної інфраструктури – банківських установ, транспортних організацій, об’єктів підвищеної небезпеки тощо.

Детальніший опис принципів здійснення кібербезпеки міститься в урядовій постанові [95], в якій визначено: відкритість цифрового простору полягає в забезпеченні вільного доступу до відомчих даних (інформації), якщо інше не встановлено законодавством; прозорість – у забезпеченні можливості

використовувати відкриті зовнішні інтерфейси до відомчих інформаційних систем, включаючи інтерфейси прикладного програмування [95]. Принципи інклюзивності та доступності полягають у забезпеченні можливості громадян користуватися новітніми досягненнями інформаційних технологій в доступі до сервісів. Принципи безпечності та конфіденційності передбачають забезпечення для фізичних і юридичних осіб безпечного та надійного середовища, в якому відбувається електронна взаємодія з державою, включаючи повну його відповідність правилам і вимогам, встановленим законами України щодо захисту персональних даних та інформації, що належить державі, електронної ідентифікації та довірчих послуг [95].

В. Фурашев зазначає, що для гарантування безпеки в кіберпросторі має бути створена інформаційно-психологічна безпека, що полягає у захисті суспільної, масової, індивідуальної свідомості від прихованих інформаційних впливів, які загрожують безпеці особи, суспільства та держави. Це нове завдання, актуальність якого обумовлена ефективністю сучасних комунікативних технологій [128].

Отже, реалізація принципів відкритості, доступності, стабільності та захищеності кіберпростору передбачають мінімальне необхідне регулювання кіберсфери органами влади, прозорість процесу прийняття ними рішень, спрямованих на регулювання відносин у цій сфері. Крім того безпечний кіберпростір означає, що поряд з вільним доступом до мережі, користувачам буде гарантоване право на захист інформації, доступ до якої обмежений законом, а також те, що користувачі будуть захищені від шкідливого психологічного впливу, який може здійснювати певний контент.

У Стратегії кібербезпеки визначено, що розвиток безпечного, стабільного та надійного кіберпростору полягає, насамперед, у формуванні конкурентного середовища у сфері електронних комунікацій, захисті інформації та кіберзахисті [123]. У документі артикульований намір розвивати інфраструктуру електронних комунікацій, включаючи широкосмуговий доступ до мережі Інтернет, цифрове та інтерактивне телебачення. Це своєю чергою

передбачає необхідність підвищувати цифрову грамотність громадян і культуру безпекового поводження в кіберпросторі, шляхом розвитку комплексних знань, навичок і здібностей, впровадження державних і громадських проєктів, спрямованих на підвищення рівня обізнаності суспільства щодо кіберзагроз і кіберзахисту [123]. Підвищення такої компетентності має відбуватися через набуття навичок поведінки в умовах надзвичайних ситуацій, інцидентів у кіберпросторі.

Отже, проаналізувавши відносини держави та громадянина в умовах віртуалізації, ми з'ясували чотири основні принципи, що визначають відносини держави та громадянина в Україні в площині кібербезпеки: 1) верховенства права, поваги до прав та свобод людини і громадянина, за яким правила поведінки в фізичному просторі поширюються і на кіберпростір; 2) забезпечення національних інтересів України, за яким кібербезпека повинна підпорядковуватися національному інтересу; 3) відкритості, доступності, стабільності та захищеності кіберпростору, що передбачає мінімально необхідне регулювання кіберсфери органами влади, прозорість процесу прийняття ними рішень, право на захист інформації, доступ до якої обмежений; 4) пріоритетного розвитку та підтримки вітчизняного потенціалу у сфері користування кіберпростором, що означає запровадження цифрової освіти для громадян. Також ми дійшли висновку, що в Україні зберігається сильний, віддалений від ідей космополітизму зв'язок між державою та населенням.

4.2. Державна територія в умовах віртуалізації інституту держави в Україні

Аналіз Стратегії кібербезпеки України уможливив простеження двох позицій, що полягають, з одного боку, в дотриманні принципів територіальності, а, з іншого – появі нових тенденцій, які ґрунтуються на ідеї позатериторіальності.

Принцип територіальності простежується у тому, що захист державного кордону в законодавстві України трактується невіддільною частиною

загальнодержавної системи забезпечення національної безпеки (отже, й основним завданням кібербезпеки, що випливає з законодавчого визначення кібербезпеки та національної безпеки). Відтак він полягає у скоординованій діяльності військових формувань і правоохоронних органів держави, організація та порядок діяльності яких визначаються законом [42].

Захист державного кордону передбачає захист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом. І він має полягати, насамперед, у створенні та забезпеченні функціонування національної телекомунікаційної мережі – єдиної платформи захищених електронних комунікацій органів державної влади [123]. Розвиток безпечного, стабільного та надійного кіберпростору полягає й у розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив щодо кібербезпеки, які відповідають національним інтересам України, що дає підстави виявити розмежування національної території та міжнародного виміру.

У Розпорядженні Кабінету Міністрів України «Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України» йдеться, що Державна прикордонна служба повинна взяти участь у процесі вдосконалення взаємодії між суб’єктами забезпечення кібербезпеки. І це має відбуватися у спосіб створення єдиної інтерактивної бази даних про кіберінциденти для потреб Міністерства оборони України, Держспецзв’язку, СБУ, Національної поліції, Національного банку, розвідувальних органів (серед відповідальних за виконання завдання зазначена Адміністрація Держприкордонслужби) [103]. Такий підхід обмежує компетенцію подолання кіберзлочинів лише національними правоохоронними та військовими формуваннями. Важливість принципу територіальності проглядається і в процесі протистояння з Російською Федерацією.

Принцип територіальності простежується не лише в державній політиці, а й в ініціативах громадян. Зокрема серед електронних петицій, поданих на

офіційному сайті Президента України є така, що мала на меті домогтися невизнання державами-підписантами Конвенції Монтевідео Росії як держави, оскільки вона втратила ознаку «визначена територія». «Єдиний міжнародний документ, що має опис ознак держави, – це Конвенція Монтевідео. Держава Україна повністю відповідає цим ознакам [...] Факт окупації частини території України не міняє приналежності цих територій Україні, та відповідно до Конвенції Монтевідео територія держави Україна є визначеною» [100], – йдеться в петиції. Але, як вважає автор петиції А. Балахнін, Росія вже не є державою, оскільки не відповідає ознакам держави, визначеним в Конвенції Монтевідео, серед яких постійне населення, визначена територія, наявність життєздатного уряду та можливість взаємодіяти із державами на міжнародній арені. Після анексування частини території України, йдеться в петиції, Росія відмовилась від кордонів 1991 року та фактично визнала факт невизначеності своєї території [100]. Петиція не набрала достатньої для розгляду кількості голосів, проте свідчить на користь принципу територіальності, оскільки опирається на класичні визначення держави та її території.

Проаналізувавши Стратегію кібербезпеки України та інші нормативно-правові акти України, доходимо висновку, що принцип територіальності залишається пріоритетним для України, зокрема в контексті протистояння з Російською Федерацією, що анексувала частину території України. Цей принцип став гарантією того, що Україна має підтримку демократичних держав. Принцип територіальності простежується у чіткому визначенні кордонів, сфер державного впливу, що обмежуються державними кордонами, а також у розподілі на національний і міжнародний простір.

Однак, крім принципу територіальності, в Стратегії кібербезпеки проглядаються і нові тенденції, які можна розглядати крізь призму позатериторіальності. Йдеться про констатацію того, що стрімкий розвиток інформаційних технологій поступово трансформує світ. «Кіберпростір поступово перетворюється на окрему, поряд із традиційними „Земля”, „Повітря”, „Море” та „Космос”, сферу ведення бойових дій, у якій активно

діють відповідні підрозділи збройних сил провідних держав світу» [123], зазначено в Стратегії. За інформаційною сферою закріплено статус самостійної сфери, взято до уваги широке застосування сучасних інформаційних технологій у секторі безпеки та оборони, створення єдиної автоматизованої системи управління армією. З огляду на це Українська держава поступово окреслює новий простір протистоянь, у якому виникають нові небезпеки, перед якими держава стає щораз уразливішою [123].

Українська держава усвідомлює, що кіберпростір нині перебрав на себе функцію форуму обговорення питань, що становлять суспільний інтерес, а громадська думка, що твориться в межах цього дискурсивного поля, має ґрунтуватися на принципах доброчесності та раціональності. Беручи до уваги це, формується державна політика захисту цього простору від злочинів.

Для України відправною точкою визначення понять у сфері протидії кіберзлочинності є Конвенція про кіберзлочинність (2001), ратифікована у 2005 році. У 2006 році ратифіковано додатковий протокол до Конвенції щодо криміналізації дій расистського та ксенофобного характеру, вчинених через комп’ютерні системи [52]. Хоч згадана конвенція не визначає основних понять (кіберзлочин, кіберзлочинність), у ній констатуються глибинні зміни, спричинені переходом на цифрові технології, конвергенція та глобалізація комп’ютерних мереж [62]. Тобто, держави-члени Ради Європи та інші держави, які підписали Конвенцію, ще 2001 року вбачали тенденції, що нині дають підстави говорити про розмивання кордонів та взаємопроникність світу. Особливо це стосується творення кіберпростору як площини, де чиняться злочини, що виходять за межі кордонів однієї держави.

Згадана конвенція поєднує принципи територіальності та позатериторіальності. Документ закріплює, що кожна держава вживає необхідних заходів для розслідування та розкриття кіберзлочину в випадках, коли таке правопорушення вчинене: на її території; на борту судна, яке плаває під прапором такої Сторони; на борту літака, зареєстрованого відповідно до законодавства такої Сторони; або одним з її громадян, якщо таке

правопорушення карається кримінальним законодавством у місці його вчинення, або якщо правопорушення вчинено поза межами територіальної юрисдикції будь-якої держави [52]. Тож Конвенція про кіберзлочинність виходить за межі території державної юрисдикції; вона передбачає такі випадки, коли жодна держава не наділена повноваженнями у певному просторі.

На нашу думку, процес віртуалізації території в Україні відбувається фрагментарно; тут поєднуються принципи територіальності та позатериторіальності. Принцип позатериторіальності проглядається у зверненні в тексті Стратегії кібербезпеки України до концепту глобального ринку конкурентних ідей, що має в основі праці ліберальних мислителів і є наслідком розвитку права на самовираження, на свободу думки та слова. З огляду на цю традицію, кіберпростір або інформаційний простір можна розглядати форумом обговорення питань, що становлять суспільний інтерес, а громадську думку, що твориться в межах цього дискусійного поля, такою, що виникає логічно та раціонально в межах культурної взаємодії. Тож важливо, щоб цей простір (не територія) був захищений від злочинних посягань. Кіберзлочинність як протизаконна діяльність, що зазіхає на можливість правильно приймати рішення в межах кіберпростору, пов’язана із функціонуванням кібернетичних комп’ютерних систем, зберігає позатериторіальний характер, але боротьба з нею, що регламентована Конвенцією про кіберзлочинність, здійснюється з дотриманням принципу визначеної територіальної юрисдикції держави. Позатериторіальний характер цього процесу вбачаємо у зобов’язанні держав, що підписали та ратифікували Конвенцію, надавати взаємну допомогу навіть за відсутності відповідних угод, а також у констатації того, що світ глобалізується та зазнає конвергенції за умов поширення комунікативних мереж.

4.3. Віртуалізація на урядовому рівні функціонування інституту держави в Україні

У Стратегії кібербезпеки України зазначено, що «розвиток та безпека кіберпростору, запровадження електронного урядування, гарантування безпеки

й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів мають бути складовими державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні» [123]. Це вихідні критерії аналізу процесу віртуалізації уряду України.

Формування електронного уряду в Україні відбувається в умовах усвідомлення небезпек, джерелом яких є кіберпростір. Серед них в Стратегії виділені: 1) невідповідність інфраструктури електронної комунікації держави, рівня її розвитку та захищеності сучасним вимогам; 2) недостатній рівень захищеності від кіберзагроз (критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом); 3) безсистемність заходів кіберзахисту критичної інфраструктури; 4) недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів; 5) недостатня ефективність суб’єктів сектору безпеки та оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру; 6) недостатній рівень координації, взаємодії та інформаційного обміну між суб’єктами забезпечення кібербезпеки [123].

Питання кібербезпеки особливо гостро постало після початку протистояння з Російською Федерацією. Хоч до 2014 року кіберзагрози для українського уряду також існували. Першим масованим випадком хактивізму, який, на думку О. Дубова, продемонстрував безпорадність українських державних органів перед кіберзлочинами, були події довкола закриття файлообмінного сервісу ex.ua. Ідеться про масовані DDoS-атаки на ресурси органів державної влади, здійснювані різноманітними акторами. У відповідь на втручання правоохоронних органів у роботу файлообмінного сервісу, було здійснено DDoS-атаки на понад 10 інтернет-сайтів органів державної влади, зокрема на сайти Президента України та сайт Міністерства внутрішніх справ

України. Символічно, що сайт інституції, яка має опікуватися питаннями кіберзлочинності, виявився одним з найменш стійких до кібератак [39, с. 212].

З початком збройної агресії Російської Федерації щодо України постала потреба не лише в кіберзахисті, а в організованій, скоординованій, цілеспрямованій та фаховій взаємодії правоохоронних органів, органів оборони країни. Основними органами, відповідальними за національну систему кібербезпеки, є Рада національної безпеки та оборони України, Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.

Рада національної безпеки і оборони України повинна координувати та контролювати діяльності суб'єктів сектора безпеки та оборони, які забезпечують кібербезпеку України. Державна служба спеціального зв'язку та захисту інформації України є спеціалізованим органом у сфері інформаційної безпеки, адже цей державний орган призначений забезпечувати функціонування і розвиток державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формувати та реалізовувати державну політику у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку [47]. Тобто, на Державну службу спеціального зв'язку та захисту інформації України покладаються чи не найбільші повноваження з питань формування та реалізації державної політики щодо захисту кіберпростору. Цей орган повинен виявляти кіберінциденти, реагувати них, усувати їх наслідки, інформувати про кіберзагрози та відповідні методи захисту від них. У межах Державної служби спеціального зв'язку та захисту інформації формується державний центр кіберзахисту.

Спеціалізованими органами, що стежать за дотриманням законів у кіберпросторі, є команда реагування на комп'ютерні надзвичайні події України

(CERT-UA) – структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам, що діє в межах Державної служби спеціального зв'язку та захисту інформації України. Існування таких команд реагування передбачено в стратегіях кібербезпеки інших країн (зокрема ФРН і Польщі). В Україні цей орган заснований 2007 року.

Закон України «Про основні засади забезпечення кібербезпеки в Україні» визначає, що завданнями урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA є, зокрема: 1) накопичення та аналіз даних про кіберінциденти, ведення державного реєстру кіберінцидентів; 2) надання власникам об'єктів кіберзахисту практичної допомоги щодо запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; 3) організація, проведення практичних семінарів щодо кіберзахисту для суб'єктів національної системи кібербезпеки, власників об'єктів кіберзахисту; 4) підготовка, розміщення на офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак і кіберзагроз; 5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; 6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти; 7) взаємодія з українськими командами реагування на надзвичайні події в онлайновому вимірі; 8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту; 9) сприяння державним органам, органам місцевого самоврядування, законним військовим формуванням, підприємствам, установам та організаціям, а також громадянам України розв'язанні питань кіберзахисту, протидії кіберзагрозам [50].

Структурний підрозділ CERT-UA створений, щоб запобігати, попереджати кіберзлочинам, виявляти їх, збирати інформацію та інформувати про них. Його створення відбулося 2007 року, що не дає можливості стверджувати про його виникнення у зв'язку з подіями на Сході України, проте з їх початком функції CERT-UA розширилися та доповнилися.

Служба безпеки України повинна попереджати, виявляти, припиняти та розкривати злочини проти миру та безпеки людства, які скоюються в кіберпросторі; здійснювати контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, а також перевіряти готовність об’єктів критичної інфраструктури до можливих кібератак, кіберінцидентів [123].

У 2015 році в Україні створені спеціальні органи, які повинні гарантувати кібербезпеку, а саме в межах Національної поліції України запрацювала кіберполіція. Кіберполіція стала територіальним міжрегіональним підрозділом Національної поліції, входить до структури кримінальної поліції. Вона зобов’язана реалізовувати державну політику у сфері протидії кіберзлочинності, своєчасно інформувати населення про появу нових кіберзлочинів, впроваджувати програмні засоби для систематизації кіберінцидентів, реагувати на запити закордонних партнерів, які надходять каналами Національної цілодобової мережі контактних пунктів [57].

До основних завдань Департаменту кіберполіції Національної поліції України належать: участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку; сприяння іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень [57].

Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, а й для принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації [123]. 2015 року у своєму блозі тогочасний міністр внутрішніх справ А. Аваков визначив типи кіберзлочинів, яким повинен протидіяти новоутворений Департамент кіберполіції Національної поліції [1]. Мова про злочини у сферах: використання платіжних систем (наприклад, несанкціоноване списання коштів з банківських рахунків);

електронної комерції та господарської діяльності (наприклад, онлайн-шахрайство); інтелектуальної власності (піратство, створення вірусів тощо); інформаційної безпеки. До злочинів у цій сфері віднесено: 1) соціальна інженерія – технологія управління людьми в Інтернет-просторі; 2) мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення; 3) протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості та насильства; 4) рефайлінг – незаконна підміна телефонного трафіку [1]. Розуміння державою необхідності боротися з такими злочинами засвідчує, що держава прагне захистити громадян від неусвідомленого й негативного інформаційно-комунікаційного впливу, гарантуючи психологічний вимір свободи в Інтернеті.

Загалом, національну систему кібербезпеки творять низка державних органів (Міністерство оборони України, Державна служба спеціального зв’язку та захисту інформації України, Служба безпеки України, Національна поліція України), підприємства, установи та організації незалежно від форми власності, які здійснюють діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об’єктів критичної інформаційної інфраструктури [123].

В Указі Президента України «Про Річну національну програму під егідою Комісії Україна-НАТО на 2019 рік» визначено систему інформаційного обміну, зокрема:

– при СБУ функціонує Ситуаційний центр забезпечення кібербезпеки, на який покладено завдання з виявлення, запобігання та нейтралізації загроз для України у кіберпросторі;

– при Державній службі спеціального зв’язку та захисту інформації України утворено Державний центр кіберзахисту та протидії кіберзагрозам, у складі якого функціонує урядова команда реагування на комп’ютерні надзвичайні події України (CERT-UA);

– при Національній поліції України функціонує Національний контактний пункт формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені комп’ютерні злочини [123].

Крім правоохоронних і військових структур, у Стратегії кібербезпеки України артикульована необхідність підготовки суддів, слідчих і прокурорів для роботи з доказами, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів. Це передбачає внесення змін до кримінально-процесуального законодавства. Також на часі підвищення обізнаності працівників усіх державних органів у сфері інформаційної безпеки та кібербезпеки, шляхом відповідних тренінгів, навчань [123].

Додаткові вимоги запроваджуються в Україні стосовно здійснення державними органами ідентифікації та автентифікації джерел, з яких вони отримують оновлення програмного забезпечення для обробки державних інформаційних ресурсів та інформації, яку потрібно захистити. На ці органи покладається обов’язок використовувати лише перевірене програмне забезпечення, щоб уникнути кібератак за збоїв роботи у цифровій сфері з причин власного недбальства. Посадовці державних органів, підприємств, установ та організацій державної форми власності «повинні використовувати електронний цифровий підпис під час використання електронної пошти для виконання своїх службових обов’язків» [123], – зазначено в Стратегії. Це дає підстави стверджувати, що система електронної безпеки в Україні поступово відходить від схеми «логін-пароль» (як передбачено і в німецькій стратегії кібербезпеки), надаючи перевагу надійнішим механізмам ідентифікації.

Як і в аналізованих нами іноземних стратегіях кібербезпеки, вітчизняна також акцентує на важливості захисту об’єктів критичної інфраструктури. Він повинен полягати в формуванні та забезпеченні функціонування державного реєстру об’єктів критичної інформаційної інфраструктури; регламентації вимог до кіберзахисту об’єктів критичної інфраструктури; створенні та забезпеченні функціонування власниками (розпорядниками) об’єктів критичної інфраструктури підрозділів кіберзахисту. Підвищення кваліфікації в цифровій

сфері передбачається і для окремих категорій працівників об’єктів критичної інфраструктури [123]. Щодо власників об’єктів критичної інфраструктури встановлюється відповідальність за захист таких об’єктів.

Пріоритетними завданнями визначено: налагодження співпраці між суб’єктами забезпечення кіберзахисту критичної інфраструктури; розвиток державно-приватного партнерства в запобіганні кіберзагрозам; реагування на кібератаки та кіберінциденти, усунення їхніх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період [123]. Про ймовірні загрози для об’єктів критичної інфраструктури повинні бути поінформовані всі суб’єкти політичного процесу (органи державної влади, приватний сектор та громадяни), задля чого потрібно запровадити ефективні механізми обміну інформацією між ними.

Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів особи, суспільства та держави в кіберпросторі, має базуватися на принципі забезпечення демократичного цивільного контролю над утвореними військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки [123]. З огляду на те, що кібербезпеку безпосередньо пов’язують з основними інтересами як громадян, так і держави, держава зобов’язується сприяти залученню наукових установ, закладів освіти, неурядових організацій, громадян до розробки та реалізації заходів із кібербезпеки та кіберзахисту [123].

Описані тенденції свідчать, що віртуалізація уряду полягає у розмиванні авторитетів та єдиного центру прийняття рішень. Адже до процесу кібербезпеки залучаються нові суб’єкти, не залучені раніше до проблем національної безпеки: наукове середовище, громадянське суспільство, власники об’єктів критичної інфраструктури тощо. Навіть волонтерські організації стають залученими до своєчасного виявлення, запобігання та нейтралізації кіберзагроз. Зокрема, у Розпорядженні Кабінету Міністрів України «Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України» була виражено артикульована необхідність удосконалити

нормативно-правову базу щодо механізму залучення фізичних і юридичних осіб до виконання завдань кіберзахисту державних електронних інформаційних ресурсів у рамках державно-приватного партнерства на умовах аутсорсингу, а також вдосконалення механізму взаємодії з Національною академією наук та її профільними установами для здійснення наукових досліджень кібербезпеки та кіберзахисту критичної інфраструктури [103].

Окрім кіберзахисту, процес віртуалізації держави передбачає також створення цифрового уряду, якому властиві перетворення механізмів державного контролю за посадовцями. Запровадження цифрового уряду здійснюється Постановою Кабінету Міністрів України «Деякі питання цифрового розвитку» [95]. Документ акцентує на потребі переходу «за замовчуванням» органів виконавчої влади до принципу державної політики цифрового розвитку. Це означає переведення у цифровий формат тих аналогових систем, розвиток і підтримка яких невигідні чи неефективні.

Аби досягнути цієї мети, ще з 01.10.2014 року в Україні запрацювало Державне агентство з питань електронного урядування України. Воно має статус центрального органу виконавчої влади, що зобов’язаний здійснювати моніторинг та методичне забезпечення запровадження органами виконавчої влади принципів державної політики цифрового розвитку. Документ визначає принципи здійснення державою цифрової політики, а також передбачає, що цей процес повинен оцінюватися з огляду на свою ефективність і результативність [95]. Державне агентство з питань електронного урядування здійснює експертизу, щоб виявити в урядових актах положення, які перешкоджають створенню сучасних електронних форм взаємодії та створюють труднощі для доступу громадян і суб’єктів господарювання до переваг, можливостей цифрових технологій.

Державне агентство з питань електронного урядування стежить, щоб урядові інституції дотримувалися засад цифрової політики: орієнтація на громадян (першочергове врахування потреб, очікувань громадян під час прийняття рішень щодо форм чи способів здійснення функцій держави);

підтримка прийняття рішень (використання новітніх інформаційних технологій для розробки програмних продуктів, які підтримують прийняття рішень органами виконавчої влади під час реалізації владних повноважень); орієнтація на адміністративне спрощення (забезпечення прискорення та спрощення адміністративних процесів шляхом їх цифрового розвитку) [95].

Крім того, Державне агентство з питань електронного урядування України реалізовує політику уряду у сфері відкритих даних, що становлять суспільний інтерес. У жовтні 2016 року Україна офіційно приєдналася до Міжнародної хартії відкритих даних, зобов'язавшись перед міжнародною спільнотою впроваджувати національну політику відкритих даних відповідно до принципів хартії: відкритість за замовчуванням; оперативність і чіткість; порівнянність та інтероперабельність (рекомендації щодо опису структури метаданих та щодо використання національних класифікаторів під час роботи з пріоритетними наборами даних); покращене урядування та залучення громадян (розвиток відкритих даних на місцевому рівні, навчання у сфері відкритих даних); розвиток та інновації (що передбачає зокрема і міжнародну співпрацю та обмін досвідом з працівниками в державах-членах ЄС, а також просування України у міжнародних рейтингах з відкритих даних) [102].

Серед пріоритетних принципів діяльності у сфері відкритих даних уряд України визначає й необхідність популяризувати відкриті дані через напрацювання відповідних комунікативних стратегій та здійснення відповідних заходів, а також популяризувати інструментарій OSINT (Open Source Intelligence, розвідка на основі відкритих джерел) [102]. Цей інструмент – важливий механізм для журналістів, інститутів громадянського суспільства, що дає змогу знайти інформацію в Інтернеті, яка може бути суспільно важливою, але доступ до якої ускладнений.

Відкриті дані є сильним антикорупційним інструментом, що дає змогу стежити за високопосадовцями, їхнім майно, доходами, витратами та зобов'язаннями фінансового характеру, доходами їхніх родичів тощо [44]. Так, з 01.09.2016 року в Україні працює Єдиний державний реєстр декларацій осіб,

уповноважених на виконання функцій держави або місцевого самоврядування, який був розроблений зокрема для спрощення роботи та як матеріал розвідок для Національного агентства з питань запобігання корупції. У такий спосіб електронні інструменти стають реальним механізмом здійснення контролю за тим, хто наділений владними повноваженнями. Вони дають змогу отримати інформацію, на підставі якої уповноважені органи доходять висновку про невідповідність статків чи стилю життя особи її офіційним доходам, в результаті чого відбувається звернення до Антикорупційної прокуратури та ініціюється провадження корупційного злочину.

Ще одним цифровим механізмом, що впливає на державну політику, є можливість подання електронних петицій. Передбачена ця можливість Законом України «Про звернення громадян», відповідно до якого громадяни можуть звернутися до Президента України, Верховної Ради України, Кабінету Міністрів України, органів місцевого самоврядування з електронними петиціями через офіційний веб-сайт органу, якому вона адресована, або веб-сайт громадського об’єднання, яке здійснює збір підписів на підтримку електронної петиції [45]. Е-петиція розглядається за умови збору на її підтримку не менш 25 тис. підписів громадян упродовж не більше трьох місяців з дня оприлюднення петиції. Органи державної влади, органи місцевого самоврядування та громадські об’єднання під час збору підписів на підтримку електронної петиції зобов’язані забезпечити: безоплатність доступу та користування інформаційно-телекомунікаційною системою, за допомогою якої здійснюється збір підписів; електронну реєстрацію громадян для підписання петиції; недопущення автоматичного введення інформації, у тому числі підписання електронної петиції без участі громадянина; фіксацію дати та часу оприлюднення електронної петиції та підписання її громадянином [45].

З липня 2015 по квітень 2019 року на сайті Президента України відповідну кількість голосів набрали 47 петицій (з близько 32,5 тис.). На більшість з тих, які набрали понад 25 тис. голосів, надійшла відповідь, доступна для перегляду в мережі. Хоч серед онлайн-петицій є радше жартами

(наприклад, «Призначити Тимошенко Юлію Володимирівну послом в Гондурас»), проте сам механізм електронного коригування політики працює.

Отже, український уряд долучається до процесів віртуалізації з огляду на загрози, джерелом яких є кіберпростір. В Україні відбуваються перетворення та розширення мережі органів, відповідальних за безпеку кіберпростору, його відповідність національним інтересам України. Як і в іноземних документах, аналіз української нормативно-правової бази дає підстави говорити про розширення кола осіб, відповідальних за забезпечення кібербезпеки – до них, крім урядовців та правоохоронців, належать науковці, представники громадянського суспільства, власники об'єктів критичної інфраструктури тощо. Віртуалізація української виконавчої гілки влади проявляється у зміні механізмів стеження за посадовцями з боку громадянського суспільства – через відкриті дані зокрема, та у зміні механізмів комунікації між ними (запровадження е-петицій), що може мати вплив на державну політику.

4.4. Міждержавні відносини крізь призму віртуалізації України

У 2014 році Україна зіткнулася з небезпеками, пов'язаними з агресією Російської Федерації. Протистояння, що триває вже шостий рік, розгортається як в географічному просторі (АРК, окуповані території Донецької та Луганської областей), так і в кіберпросторі. Якщо першому типу зіткнень властиві людські жертви, втрата території тощо, то другому – отримання необхідної інформації незаконними шляхами, насадження певного типу світогляду в результаті циркуляції неправдивих новин, пропаганди тощо. Поєднання цих загроз дає підстави стверджувати, що Україна втягнута у гібридний конфлікт. На переконання Г. Почепцова, нове у гібридній війні – не її складові, а поєднання цих складових, додавання нового інформаційного елемента [99, с. 264].

Стратегія кібербезпеки України констатує факт агресії Російської Федерації проти України. Крім того вказано, що відбуваються інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України, що

вимагають невідкладного створення національної системи кібербезпеки як складової системи забезпечення національної безпеки України [123].

Історія цифрового протистояння між державами почалася у квітні 2014 року, коли було проведено низку потужних DDos-атак на урядові ресурси (сайти Кабінету Міністрів України та Генеральної прокуратури України), для чого активно використовувалися бот-мережі [39, с. 215–216]. В Інтернет-протистоянні Росії з Україною проти останньої вперше було застосовано троянські програми, найперше – вірус Uroburos. З одного боку, завданням цього вірусу було формування бот-мережі зі заражених комп'ютерів та отримання доступу до їхнього вмісту, а з іншого – викрадення інформації з цих комп'ютерів. Об'єктами атаки стали веб-ресурси органів державної влади (зокрема, силових структур), медіа, фінансових установ, великих промислових підприємств [39, с. 215–216]. Поширення вірусу Uroburos стало першим випадком цілеспрямованої атаки на державні інформаційні системи.

З огляду на постійний розвиток технологій та поступ інформаційного суспільства, небезпеки в кіберпросторі не зникають. Навіть більше, зловмисники щоразу вчаться обходити заходи безпеки, їхня діяльність стає менш очевидною та прогнозованою. «Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки й оборони України стають дедалі уразливіші для розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі. Цьому сприяє широка, подекуди панівна, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо чи опосередковано пов'язані з Російською Федерацією» [123], – зазначено в Стратегії кібербезпеки України, прийнятій через два роки після початку агресії Росії.

Аби забезпечити можливість протистояти Російській Федерації, Україна декларує готовність підвищувати спроможність суб'єктів боротьби з кібертероризмом протидіяти кібератакам, спрямованим проти України. Йдеться про напади на державні електронні інформаційні ресурси, об'єкти критичної

інфраструктури, а також розвідувально-підривну діяльність іноземних спецслужб, організацій, груп та осіб. Також передбачено, що участь у заходах зі забезпечення інформаційної та кібербезпеки суб'єктів господарювання, які перебувають під контролем держави-агресора, буде обмежена. Це ж стосується держав та осіб, стосовно яких діють спеціальні економічні та інші санкції, прийняті на національному або міжнародному рівні внаслідок агресії щодо України. Обмеження передбачені й щодо використання продукції, технологій та послуг таких суб'єктів, що підконтрольні державі-агресору чи особам, які підпали під санкції, якщо їхні продукти та послуги стосуються технічного та криптографічного захисту державних інформаційних ресурсів [123].

Конфлікт з Російською Федерацією став причиною розробки та впровадження 2016 року «Доктрини інформаційної безпеки України» [122]. У ній зазначено: «Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної та релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України» [122]. У документі зазначено: життєво важливими інтересами особи є захищеність від руйнівних інформаційно-психологічних впливів, а інтересами суспільства та держави – захист від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації; захист від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [122].

Доктрина інформаційної безпеки визначає обов'язки урядових структур у цій сфері, зокрема Міністерства інформаційної політики. Ця урядова інституція повинна забезпечити Україні її інформаційний суверенітет, який законодавство України визначає як здатність держави контролювати та регулювати потоки

інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантувати національну безпеку держави [48].

Крім кіберзаходів, спрямованих на подолання негативного впливу держави-агресора на українське суспільство, важливим напрямом віртуалізації держави є міжнародне співробітництво, спрямоване на зміцнення взаємної довіри у сфері кібербезпеки та напрацюванні спільних підходів у протидії кіберзагрозам, консолідації зусилля у розслідуванні та запобіганні кіберзлочинам, недопущенні використання кіберпростору в протиправних і воєнних цілях [123]. Задокументованими пріоритетами в міжнародній діяльності з цих питань для України є співпраця з НАТО у сфері кібербезпеки та сумісним захистом від кіберзагроз. Крім того, в Стратегії передбачено, що державна політика має пройти адаптацію у сфері кібербезпеки до міжнародних стандартів.

Для розвитку безпечного, стабільного та надійного кіберпростору передбачається поглиблення співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ, а також розвиток підрозділів кібербезпеки та кіберзахисту Збройних Сил України, Державної служби спеціального зв’язку та захисту інформації України, Служби безпеки України, Національної поліції України, розвідувальних органів [123].

В Україні розвивається ідея створення так званих кібервійськ за міжнародними стандартами. Ще 2013 року вперше у світі були створені військові кіберпідрозділи з акцентом на захисті власних інтересів у цифровому просторі в США (U.S. Cyber Command), Великій Британії (урядовий Cyber Security Operations Centre), ФРН (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre) та інших країнах. Примітно, що готовність до створення кіберкомандування (інформкомандування) висловила й Російська Федерація: ще в лютому 2013 року почав роботу спеціальний підрозділ з кібербезпеки. Також 2013 року розпочато створення кібервійськ у Білорусі [39, с. 51].

Водночас в Україні про формування та необхідність сформувати відповідні військові підрозділи почали говорити лише 2018 року, коли тодішній Секретар РНБО О. Турчинов заявив: в лавах Збройних сил України створять кібервійська, без яких неможлива сучасна війна [119].

На момент підготовки дослідження відсутні офіційні документи про створення підрозділів кібервійськ в Україні. Однак на початку 2019 року інформаційне агентство Українські національні новини (UNN) оприлюднило коментар Секретаря комітету з нацбезпеки й оборони, народного депутата І. Винника про те, що в Україні створені кібервійська, які «переважно займаються питаннями оборони нашого кіберпростору, але й роблять інші операції» [76]. Припускаємо, що мова про Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України, який утворений у 2016 році.

Важливим партнером України у напрацюванні механізмів боротьби з кіберзагрозами є США. У 2018 році конгресмени схвалили проєкт акта про співпрацю з Україною з питань кібербезпеки, спрямований активну взаємодію між Україною та США в цій сфері [197]. Законопроєкт розроблено під керівництвом члена комітету з міжнародних справ палати представників Б. Бойла – безпосередньо для України. В процесі обговорення документа Б. Бойл заявив: «Впродовж останніх років Росія використовувала Україну як полігон для кібератак, які ставлять під загрозу національну безпеку нашого великого союзника, України, а також її сусідів в регіоні» [63; 92]. В тексті акта згадується Будапештський меморандум, й Україні пропонується разом зі США перебрати на себе лідерську роль в поліпшенні кібербезпеки у регіоні Центральної та Східної Європи. У прийнятому акті про співпрацю США та України декларується, що американська сторона має намір допомагати Україні в питаннях захисту урядових комп’ютерних мереж, обміні інформацією з метою позбутися російського програмного забезпечення [92].

Про важливість співпраці Україна-НАТО свідчать норми «Річної національної програми під егідою Комісії Україна-НАТО на 2019 рік» [121], що

передбачають: одним з пріоритетних завдань для України є напрацювання національної системи стратегічних комунікацій. Співробітництво України з НАТО у сфері стратегічних комунікацій набуло особливого значення у контексті протидії гібридній війні, що ведеться Російською Федерацією проти України. Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО, підписана 05.11.2015 року, спрямована на розбудову та розвиток спроможностей України у сфері стратегічних комунікацій шляхом надання консультативної та практичної допомоги з боку НАТО.

Україна має намір удосконалити систему захисту інформаційних ресурсів та інформації, кіберзахисту інформаційно-телекомунікаційних систем органів системи Міністерства внутрішніх справ України. Для цього до кінця 2020 року планується: запровадити інноваційні рішення та інструменти системи захисту інформаційних ресурсів, підвищити ефективність роботи та взаємодії через максимальне використання інформаційно-комунікаційних технологій у реалізації завдань органами системи Міністерства внутрішніх справ України. Також передбачається введення в експлуатацію єдиної інформаційної системи Міністерства внутрішніх справ України із впровадженням систем кіберзахисту та захисту інформації, яка в ній оброблялася [121]. Вдосконалення системи урядових комунікацій є умовою для продовження співпраці з НАТО.

До кінця 2020 року Україна запланувала запровадити заходи із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і міжнародних стандартів ISO/IEC. Також держава задекларувала намір поглиблювати міжнародне співробітництво і взаємодію з компетентними органами інших держав у сфері протидії кіберзагрозам національній безпеці, іншим вагомим інтересам держави [121].

Отже, у віртуалізації відносин України з іншими державами вимальовуються дві тенденції. З одного боку, Україна працює над створенням власного безпечного простору кібербезпеки, який би був здатен протистояти загрозам, передусім тим, джерелом яких є держава-агресор Російська

Федерація. З іншого, Україна декларує своє бажання взаємодіяти на міжнародному рівні з іншими державами та доходити спільних рішень у процесі боротьби з кіберзлочинністю. Відтак відбувся поділ на світ партнерів та союзників та світ держав-агресорів, яким потрібно протистояти. Це дає підстави говорити, що віртуалізація міжнародних відносин та визначеної території зумовлюють і визначають одна одну. Також зазначимо, що механізми «м'якої сили» можна вбачати у фактах прийняття Доктрини інформаційної безпеки, створенні Міністерства інформаційної політики, адже вони спрямовані на нівелювання небажаних для України наслідків пропаганди та інформаційного потоку.

Висновки до розділу 4.

У четвертому розділі дисертації виділено основні тенденції віртуалізації Української держави, відповідно до чотирьох основних ознак держави за Концепцією Монтевідео.

1. Щодо віртуалізації постійного населення, то в Україні зберігається доволі сильний, віддалений від ідей космополітизму зв'язок між державою та населенням. Водночас тут під впливом технологічної революції поступово ослаблюються зв'язки населення з інститутом держави. Цьому сприяло стрімке зростання можливостей спілкування, трудова та інші види міграції, впровадження платформової економіки, інтеграція нашої країни у простір глобального інформаційного суспільства, зниження рівня довіри до інституту держави тощо. Для населення у взаємодії з державою дедалі частіше характерне заміщення реальних взаємодій комп'ютерно-симуляційними. За умов вираженого інформаційного протиборства останніх років в Україні інститут держави вимушений активно протидіяти загрозам інформаційно-психологічної безпеки особистості.

2. Різні аспекти проблематики державної території болісно сприймаються Україною з огляду на анексію АР Крим та окупацію територій на Сході нашої держави. Водночас в частині аспекту віртуалізації території як

ознаки держави, то в нашій країні утверджується загальнопланетарна тенденція до зменшення ролі чинника території держави з огляду на нинішню мобільність населення, уможливлення швидкого подолання значних відстаней за здешевлення витрат на переміщення між територіями різних держав. Україна інтегрується в глобальний позатериторіальний простір. Глобалізація як детериторізація призводить до певної «реконфігурації» географічного простору, і ці процеси не можуть оминути нашу країну. Це стає результатом т. зв. «великої війни за незалежність від простору» (З. Бауман), в результаті якої територія втрачає свої характеристики (скорочуються відстані, стираються кордони, а простір перетворюється на єдине ціле).

3. Віртуалізація уряду є чи не найбільш увиразненим елементом системи віртуалізації інституту держави в Україні після взятого урядом курсу на розбудову «держави в смартфоні». Віртуалізація органів влади полягає в діджиталізації, створенні онлайн-системи простих, зрозумілих і прозорих послуг для громадян. Орієнтир на побудову цифрової держави передбачає перспективу надання особі сервісу без наявності державної бюрократії, що є важливим кроком у політиці антикорупції. Також віртуалізація українського уряду потребує перегляду мережі органів, відповідальних за безпеку в кіберпросторі, посилення контролю за діями, які через кіберпростір посягають на національні інтереси України. Це продиктовано дедалі складнішим ландшафтом сучасних кіберзлочинів. Однак нині наявні значні прогалини в галузі кібербезпеки України, що призводить до неготовності реагувати на кіберінциденти та вимагає нової національної концепції кібербезпеки.

4. Віртуалізація міжнародних відносин України зумовлена глобалізацією, уразливістю кіберпростору, наявністю гібридних загроз тощо. Нові технології спрощують контакти України на міжнародній арені, розширюють мережу способів оперативного донесення до міжнародної спільноти важливих питань життєдіяльності нашої країни. Розуміння існування гібридних загроз, та усвідомлюють важливість для України міжнародної співпраці для запобігання їм.

ВИСНОВКИ

1. Еволюція ідеї віртуальності та віртуалізації держави простежується від Античності, коли Платон запропонував поділ реальності на світ речей та світ ідей. Відтоді, зокрема у Середньовіччі, ідею віртуального розглядали в контексті метафізики та онтології: віртуальне виступало позначенням усеможливих ознак і впливів певного об'єкта. Подальша еволюція ідеї віртуальності прослідкована в теорії можливих світів (Г. Лейбніц).

У XX столітті ідею віртуальності доповнили напрацювання: 1) теорії соціального інтеракціонізму, який визначив реальність результатом людських переконань щодо того, чим є ця реальність; 2) соціального конструктивізму, за яким суспільне життя поділяється на суб'єктивне (особистісне) й об'єктивне (інституційне), що корелюють одне одного; 3) постмодернізму, представники якого напрацювали концепції симулякрів (Ж. Бодрійяр), дискурсу (М. Фуко); це уможливило перенесення дискусії щодо результатів функціонування текстів у площину дискусій про віртуальність. Підґрунтям дослідження віртуалізації держави визначено й праці теоретиків інформаційного суспільства (Д. Белл, Е. Тоффлер, М. Кастельс та ін.), представників комунікативних наук (М. Маклюен, Н. Луман, В. Ліппман та ін.), теорії глобалізації (З. Бауман, У. Бек та ін.).

Віртуалізація розглядається на технологічному та символічному рівнях: а) комп'ютерна віртуалізація розглядає трансформацію держави як перенесення виконання державою своїх функцій у вимір Інтернету; б) символічна віртуалізація полягає у перетворенні всіх сфер діяльності держави через різноманітні форми продукування та поширення соціально-політичних символів.

2. Викладено розуміння віртуальної держави як сучасного політичного інституту. Віртуалізація держави відбувається як на технологічному, так і на онтологічному рівнях. Нині не можна констатувати заміщення за допомогою технологій реального інституту держави, як основи

організації та консолідації суспільства, певною уявною моделлю. Інститут держави нині зазнає значних перетворень під впливом технологічних перетворень, але це, найперше, змінює механізми виконання нею своїх функцій, але не підриває консолідаційну здатність цього політичного інституту. Віртуальна держава таким чином нині постає як форма держави, яка модернізується під впливом технологій та публічного дискурсу.

Нинішні процеси віртуалізації держави можна інтерпретувати систему принципів та інструментів (детериторіалізація, дискурсивізація, медіатизація та ін.), які мають як конструктивні, так і деструктивні наслідки, що проявляється у ставленні до інституту громадянства, мірі лояльності до держави, руйнуванні національної ідентичності, обмеженні суверенітету, глобальній технологічній залежності тощо. Наявні дослідження найчастіше відбивають тенденції до інтерпретації віртуалізації держави як: 1) перехід від національної моделі держави до іншої (віртуалізованої); 2) процес адаптації та боротьби за виживання в інформаційному суспільстві; альтернативна форма держави.

Попри те, що політичній науці віртуальними або кібердержавами зазвичай називають ті, які не відповідають усім ознакам міжнародного правосуб’єкта (невизнані держави, держави, що існують лише в Інтернеті тощо), ми під віртуалізацією держави розуміємо, найперше, перетворення механізмів функціонування держави, перенесення виконання державою своєї функцій частково чи уповні в кіберпростір як середовище ризиків і можливостей, утворене в результаті функціонування електронно-комунікаційних систем.

Нині держава поступово видозмінює чотири основні ознаки, закріплені Конвенцією Монтевідео: постійне населення, визначена територія, уряд, здатність вступати у відносини з іншими державами. Названі класичні характеристики держави більшою чи меншою мірою екстраполюються до інформаційного простору (кіберпростору), в результаті чого класичний інститут держави модифікується. Функціонуючи в умовах сучасного кіберпростору, який динамічно розвивається, сучасні держави отримують як

нові можливості для розвитку, так і опиняються перед небезпеками, які загрожують їх функціонуванню.

Відтак віртуалізація інституту держави постає як багатоаспектний процес з наявними перевагами та ризиками, в результаті якого під впливом інформаційно-комунікаційного прогресу видозмінюються характеристики новітнього інституту держави. Це процес, зумовлений переходом діяльності органів держави у віртуальний простір Інтернету, яка виводить реалізацію функцій держави та можливості впливу на населення на новий рівень.

3. Однією з основних класичних ознак держави традиційно вважається наявність постійного населення. Однак нині відбуваються процеси, які засвідчують віртуалізацію цієї фундаментальної ознаки. Вони, найперше, зумовлені технологічною революцією та глобалізацією, які зменшують значення державних кордонів, змінюють підходи до вибору місця проживання та праці. Продукована певною державою національна ідентичність більше не є неодмінною підставою об’єднання людей, котрі проживають на її території. Інформаційний простір, кіберпростір виступають площиною творення новітніх ідентичностей. Різко розширюються можливості спілкування та вибору локації проживання, з’являються нові джерела доходів (завдяки еволюції бізнес-моделі платформової економіки). Віртуальні бізнес-компанії, формально самостійні роботодавці та працівники-фрілансери, які можуть проживати в будь-якому куточку планети – все це завдяки Четвертій промисловій революції ослаблює зв’язок населення з державою свого громадянства (підданства). Припускаємо, що проявом віртуалізації населення держави може стати наростання тенденції збереження особою громадянства держави без чіткого увиразнення певної національної ідентичності. Окрім цього наявними є такі малодосліджені новітні феномени як віртуальні держави (на зразок Князівства Сіландія, Інтернет-держави Віртландія), які пропонують надання свого громадянства через онлайн-процедуру.

4. Віртуалізація державної території полягає в зменшенні ролі чинника території держави з огляду на нинішню мобільність населення,

уможливлення швидкого подолання значних відстаней за здешевлення витрат на переміщення між територіями різних держав. Нині територія – змінна характеристика, адже будучи формою соціально-просторової організації вона змінюється під впливом реалій конкретного часу. Формується нова надтериторіальна географія мереж і потоків, яка витісняє «стару» географію державних територій. У нинішньому «суспільстві швидкості» цінність топосу (місця) зменшується; швидкість фактично реконструює простір: максимально скорочуються відстані завдяки стисненню часу переміщення та передачі інформації на будь-яку відстань. Відтак, що могутність держави дедалі менше пов'язана саме з чинником території. Універсалізація глобальних загроз, вихід небезпек за межі державних кордонів зумовила необхідність спільно шукати відповіді на новітні виклики; це стало основою процесу детериторіалізації (втрати прив'язки соціальних процесів до певного фізичного простору). Детериторіалізація простежується як на рівні формування віртуальних територій, що не мають географічно-територіальної прив'язки, так і на рівні перетворення свідомості людей, що повинні мати справу з питаннями, на які складно впливати з огляду на їх географічну віддаленість.

5. Досліджено віртуалізацію системи органів державної влади, позаяк наявність такої системи віднесено до ознак інституту держави. Визначено, що ці процеси зумовлені демократизацією політики (попри те, що останніми роками дослідники відзначають загальнопланетарне погіршення якості демократії), стрімким поширенням інформаційно-комунікативних технологій, які охопили процеси урядування та низкою інших причин. Констатовано, що віртуалізація органів влади, найперше, полягає у діджиталізації, створенні системи простих, зрозумілих і прозорих послуг для громадян. Перспективою вбачається надання сервісу без наявності державної бюрократії, побудова цифрової держави, «держави у смартфоні». Відзначено тенденцію максимального «виведення» чиновників з процесу надання державних послуг, які автоматизуються. Нині запускаються єдині онлайн-портали державних послуг, відповідні мобільні додатки, електронні кабінети громадянина,

відбувається перехід на електронний документообіг. Переведення державних адміністративних послуг в електронний формат уможливлює отримання послуги з будь-якого місця, де є підключення до Інтернету, та звужує ризики корупції. Якщо раніше йшлося про е-демократію, е-урядування, то нині мова йде про повноцінну розбудову цифрової держави.

5. Вивчення віртуалізації міждержавних відносин засвідчило, що впровадження нових інформаційно-комунікативних технологій посилило віртуалізацію соціальних процесів і явищ міжнародного життя. На міжнародному рівні нові технології спрощують контакти між державами, народами, виступаючи важливим важелем глобального управління (global governance, world governance). Водночас на рівні міжнародної взаємодії процеси віртуалізації держави призводять до певного послаблення суверенітету (це відбито в теоріях «ерозії суверенітету», «обмеженого суверенітету»). Функціонування наднаціональних інтегративних структур, велика кількість транснаціональних акторів, поява різноманітних міжнародних режимів та багато інших феноменів глобалізації світу уможливлюють висновок не стільки про «зникнення» суверенітету сучасної держави, скільки про його «розмивання». Відзначено, що віртуалізацію міжнародних відносин характеризує універсалізація ризиків, зростання інформаційних протистоянь тощо. За умов інформаційного суспільства переструктуровується весь світовий політичний простір, а відтак міжнародні відносини набувають нових обрисів.

6. На основі аналізу національних стратегій кібербезпеки США, ФРН і Польщі виділено спільні та відмінні риси процесу віртуалізації держави:

– серед спільних характеристик у питаннях віртуалізації населення у США, ФРН та Польщі визначено спрямованість на підвищення обізнаності громадян в питаннях кібербезпеки, а також широкого кола питань, пов’язаного з функціонуванням цифрової держави, перевагами та потенційними загрозами інформаційного суспільства. Чітко виражена позиція, що в кіберпросторі мають домінувати права та свободи людини. Ідея космополітизму виражено не прослідковується в жодній зі трьох згаданих стратегій;

– віртуалізація державної території аналізується на основі стратегій кібербезпеки аналізованих держав. Детериторіалізація проглядається у: об’єднанні зусиль для протидії кіберзлочинності, що вимагає об’єднання зусиль; поділі світу на простір «однодумців» і «ворогів» (це особливо простежується в кіберстратегії США). У розвитку економічних ініціатив простежується перегляд ролі кордонів, що продиктовано, найперше, економічною глобалізацією. Одначе, розмежування політичних процесів на внутрішні та зовнішні свідчить про наразі переважання принципу територіальності над принципом детериторіалізації;

– віртуалізація уряду передбачає його зорієнтованість на найвищі стандарти технологічного розвитку, здатність швидко діяти в кіберсфері, реагуючи на злочини в віртуальному вимірі, запобігати їм. В усіх аналізованих державах (а особливо – у США) зростає увага до проблем кібербезпеки, увиразнена орієнтація на удосконалення технологій гарантування мережевої безпеки. Розширюючи свою юрисдикцію на кіберпростір, уряди усіх аналізованих країн взаємодіють із новими акторами – провайдерами цифрових послуг, неурядовими організаціями, аналітичними центрами. Відмінним в процесі віртуалізації урядів є неоднакова увага до того, якою має бути конфігурація національної мережі органів протидії кіберзлочинності, способів реагування на кіберзлочини. Нині пріоритетом аналізованих держав є розробка механізмів захисту від кібератак об’єктів критичної інфраструктури (енергетика, транспортна система, банківський сектор тощо). Особливою агресивністю у наступі на кіберзлочинність віднедавна характеризується США (2018 р. – прийняття нової стратегії);

– віртуалізація міжнародних відносин полягає в низці процесів, спільних для аналізованих держав. Передусім, США, ФРН і Польща визнають існування гібридних загроз та усвідомлюють важливість міжнародної співпраці для запобігання їм. Відмінним є визначення супротивників: США чітко називають конкретні держави (найперше – Росія, Іран, КНР і КНДР); натомість ФРН і Польща обмежуються визначенням потенційних кіберзлочинів, яким мають

намір протидіяти. По-різному держави визначають й власну роль у процесі віртуалізації міжнародних відносин: США констатує право лідера і значною мірою наступальну тактику, ФРН – готовність виконувати всі міжнародні угоди, а Польща зорієнтована на взаємодію у сфері убезпечення кіберпростору на глобальному та регіональному рівнях. Відтак аналізовані держави відрізняються за визначенням вагомості механізмів «м'якої сили» в умовах інформаційного суспільства та віртуалізації простору.

7. Тенденціями віртуалізації Української держави, відповідно до основних ознак держави за Концепцією Монтевідео, визначено:

– щодо віртуалізації постійного населення, то в Україні зберігається доволі сильний, віддалений від ідей космополітизму зв'язок між державою та населенням. Водночас нині під впливом технологічної революції поступово ослаблюються зв'язки населення з інститутом держави. Цьому сприяє стрімке зростання можливостей спілкування, трудова та інші види міграції, впровадження платформової економіки, інтеграція нашої країни у простір глобального інформаційного суспільства, зниження рівня довіри до інституту держави тощо. Для населення у взаємодії з державою дедалі частіше характерне заміщення реальних взаємодій комп'ютерно-симуляційними. За умов вираженого інформаційного протиборства останніх років в Україні інститут держави вимушений активно протидіяти загрозам інформаційно-психологічної безпеки особистості;

– різні аспекти проблематики державної території болісно сприймаються Україною з огляду на анексію АР Крим та окупацію територій на Сході нашої країни. Водночас в частині аспекту віртуалізації території як ознаки держави, то в нашій країні утверджується загальнопланетарна тенденція до зменшення ролі чинника території держави з огляду на нинішню мобільність населення, уможливлення швидкого подолання значних відстаней за здешевлення витрат на переміщення між територіями різних держав. Україна інтегрується в глобальний позатериторіальний простір. Глобалізація як детериторізація призводить до певної «реконфігурації» географічного простору, і ці процеси не

можуть оминути нашу країну. Це стає результатом т. зв. «великої війни за незалежність від простору» (З. Бауман), в результаті якої територія втрачає свої характеристики (скорочуються відстані, стираються кордони, а простір перетворюється на єдине ціле);

– віртуалізація уряду є чи не найувиразненішим елементом системи віртуалізації інституту держави в Україні, особливо після взятого урядом курсу на розбудову «держави в смартфоні». Віртуалізація органів влади полягає в діджиталізації, створенні онлайн-системи простих, зрозумілих і прозорих послуг для громадян. Орієнтир на побудову цифрової держави передбачає перспективу надання особі сервісу без наявності державної бюрократії, що є важливим кроком у політиці антикорупції. Також віртуалізація українського уряду потребує перегляду мережі органів, відповідальних за безпеку в кіберпросторі, посилення контролю за діями, які через кіберпростір посягають на національні інтереси України. Це продиктовано дедалі складнішим ландшафтом сучасних кіберзлочинів. Однак нині наявні значні прогалини в галузі кібербезпеки України, що призводить до неготовності реагувати на кіберінциденти та вимагає нової національної концепції кібербезпеки.

– віртуалізація міжнародних відносин України зумовлена глобалізацією, уразливістю кіберпростору, наявністю гібридних загроз тощо. Нові технології спрощують контакти України на міжнародній арені, розширюють мережу способів оперативного донесення до міжнародної спільноти важливих питань життєдіяльності нашої країни. Розуміння існування гібридних загроз, та усвідомлюють важливість для України міжнародної співпраці для запобігання їм.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аваков, А. (2015). *Кіберполіція (крок реформі)*. Available from: https://blogs.pravda.com.ua/authors/avakov/561a92c183c27/

2. Александрук, І. (2012). Роль теорії можливих світів у сучасній лінгвістиці. *Проблеми семантики слова, речення та тексту, 28,* 21-26.

3. Амелін, О. (2016). Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України, 3*, 1-10.

4. Андерсон, Б. (2001). *Уявлені спільноти. Міркування щодо походження й поширення націоналізму*. Київ: Критика.

5. Андрущенко, М. О. (2009). Концепція хронополітики Поля Вірільйо: від дромократії до дромології. *Політологічний вісник, 41*, 143-151.

6. Арентд, Х. (2003). О насилии. In Б. Г. Капустин (Ed.), *Мораль в политике. Хрестоматия* (pp. 312-377). Москва: Книжный дом «Университет».

7. Афанасьева, В. В. (2005). *Тотальность виртуального*. Саратов: Научная книга.

8. Байтин, М. И. (2002). О понятии государства. *Правоведение, 3*, 4-16.

9. Баришнікова, Н. С. (2016). Глобальні структури за умов ерозії Вестфальської системи. *Зовнішня політика і дипломатія: традиції, тренди, досвід, 22,* 107-112.

10. Бауман, З. (2008). *Текучая современность* (Ю. В. Асочаков, Trans.). Санкт-Петербург: Питер.

11. Беззубова, О. (2011). «Другие пространства» Мишеля Фуко: современные стратегии интерпретации. *Вестник гражданских инженеров, 2 (27)*, 199-204.

12. Бек, У. (2000). *Общество риска. На пути к другому модерну* (В. Седельник, Н. Федорова, Trans.). Москва: Прогресс-Традиция.

13. Бек, У. (2001). *Что такое глобализация?* Москва: Прогресс-Традиция.

14. Белл, Д. (2004). *Грядущее постиндустриальное общество. Опыт социального прогнозирования*. Москва: Academia.

15. Бергер, П., Лукман, Т. (1995). *Социальное конструирование реальности. Трактат по социологии знания*. Москва: Медиум.

16. Бернейс, Э. (2010). *Пропаганда*. Москва: Hippo Publishing LTD.

17. Бєльська, Т. (2015). Глобалізація. In Н. М. Хома (Ed.), *Політологія: навчальний енциклопедичний словник-довідник* (pp. 84-85). Львів: Новий Світ-2000.

18. Біловус, Л. (2013). *Український інформаційний простір: сьогодення та перспективи*. Available from: http://ijimv.knukim.edu.ua/zbirnyk/1_1/bilovus_l_i_ukrayinskyy_informatsiynyy_prostir.pdf

19. Бодрійяр, Ж. (2004). *Симулякри і симуляція* (В. Ховхун, Trans.). Київ: Основи.

20. Бодунова, О. Г, Малышева, А. А. (2018). Конституционно-правовой статус человека в виртуальном государстве. *Ученые записки Санкт-Петербургского имени В. Б. Бобкова филиала Российской таможенной академии, 2 (66)*, 40-46.

21. *Верховенство права*. Конституційний Суд України: офіційний веб-сайт. Available from: http://ccu.gov.ua/storinka-knygy/34-verhovenstvo-prava

22. Вирилио, П. (2002). *Информационная бомба. Стратегия обмана.* Москва: Гносис.

23. Вирилио, П. (2004). *Машина зрения*. Санкт-Петербург: Наука.

24. Волинець, В. (2004). Віртуальна реальність: поняття та сутність. *Питання культурології, 30,* 35-41.

25. *Вплив Росії на виборців в США: дослідники вивчили мільйони публікацій із соцмереж* (2018). Available from: https://www.radiosvoboda.org/a/ ssha-zvit-rosija-vybory-vplyv/29663419.html

26. Гальцова, О. (2017). До питання поваги до прав і свобод людини як міжгалузевого принципу кримінально-виконавчого права. *Підприємство, господарство і право. Серія Кримінологія, 3,* 249-252.

27. Гальцова, О. В. (2014). *Принцип поваги до прав і свобод людини при виконанні-відбуванні покарань як один з напрямів кримінально-виконавчої політики.* Available from: http://law-dep.pu.if.ua/conference2014/articles/haltsova. pdf

28. Грибовод, Е. (2017). *Медиатизация политики как институционально-коммуникативный процесс и информационно-стратегический ресурс.* Екатеринбург: Уральский гуманитарный институт.

29. *Декларация о предоставлении независимости колониальным странам и народам* (1960). Available from: https://zakon.rada.gov.ua/laws/show/ 995_280

30. *Декларація «Про державний суверенітет України»* (1990). Available from: https://zakon.rada.gov.ua/laws/show/55-12

31. *Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті»* (2003). Available from: https://zakon.rada.gov.ua/laws/show/995_c57

32. Делёз, Ж., Гваттари, Ф. (1976). *Ризома*. Available from: http://www.situation.ru/app/j_art_1023.htm

33. Делёз, Ж., Гваттари, Ф. (2007). *Анти-Эдип: Капитализм и шизофрения*. Екатеринбург: У-Фактория.

34. Деррида, Ж. (2000). *О граматологии* (Н. С. Автономова, Trans.). Москва: Ad Marginem.

35. Дзьобань, О., Мануйлов, Є. (2017). Віртуальна реальність: до проблеми концептуалізації поняття. *Вісник Національного університету Юридична академія України імені Ярослава Мудрого, 4 (35),* 21-31.

36. Дискурс. In *Постмодернизм: Энциклопедия*. Available from: http://www.infoliolib.info/philos/postmod/diskurs.html

37. Дмитриев, А. Н. (1997). Опыт сотрудничества П. Лазарсфельда и Т. Адорно в исследовании массовой коммуникации. *Социологический журнал, 3,* 151-158.

38. *Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО* (2016). Available from: https://mfa.gov.ua/mediafiles/sites/nato/files/ Roadmap_Ukr.pdf

39. Дубов, Д. В. (2014). *Кіберпростір як новий вимір геополітичного суперництва*. Київ: НІСД.

40. *Закон України «Про внесення змін до деяких законів України щодо мови аудіовізуальних (електронних) засобів масової інформації»* (2017). Available from: https://zakon.rada.gov.ua/laws/show/2054-19/ed20180722?lang=ru

41. *Закон України «Про громадянство України»* (2001). Available from: https://zakon.rada.gov.ua/laws/show/2235-14

42. *Закон України «Про державний кордон України»* (1992). Available from: https://zakon.rada.gov.ua/laws/show/1777-12

43. *Закон України «Про Державну кримінально-виконавчу службу України»* (2005). *Відомості Верховної Ради України, 30*, Ст. 409.

44. *Закон України «Про запобігання корупції»* (2014). Available from: https://zakon.rada.gov.ua/laws/show/1700-18

45. *Закон України «Про звернення громадян»* (1996). Available from: https://zakon4.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80

46. *Закон України «Про кінематографію»* (1998). Available from: https://zakon.rada.gov.ua/laws/show/9/98-%D0%B2%D1%80

47. *Закон України «Про національну безпеку України»* (2018). Available from: https://zakon.rada.gov.ua/laws/show/2469-19

48. *Закон України «Про Національну програму інформатизації»* (1998). Available from: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80/ed20160801#n20

49. *Закон України «Про основи національної безпеки України»* (2003). Available from: https://zakon.rada.gov.ua/laws/show/964-15

50. *Закон України «Про основні засади забезпечення кібербезпеки України»* (2017). Available from: https://zakon.rada.gov.ua/laws/show/2163-19

51. *Закон України «Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях»* (2018). Available from: https://zakon.rada.gov.ua/laws/show/2268-19

52. *Закон України «Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи»* (2006). Available from: https://zakon.rada.gov.ua/laws/show/23-16

53. Иванов, Д. (2002). *Виртуализация общества. Версия 2.0*. Санкт-Петербург: Петербургское Востоковедение.

54. Іванов, В. (2016). Свобода слова. Еволюція ідеї свободи думки. *Інформаційне суспільство, 23,* 6-19.

55. Іщенко, Н. (2017). *Останній вирок трибуналу в Гаазі: сербський генерал відповість за геноцид.* Available from: https://www.eurointegration.com.ua/articles/2017/11/22/7074039/

56. Кастельс, М. (2000). *Информационная эпоха: экономика, общество и культура* (О. И. Шкаратан, Trans.). Москва: Государственный университет Высшей школы экономики.

57. *Кіберполіція України: офіційний сайт*. Available from: https://cyberpolice.gov.ua/results/2018/

58. Клімова, Г. П., Клімов, О. В. (2006). Держава в політичній системі суспільства. *Гуманітарний часопис, 3*, 94-99.

59. Коврига, С. (2010). Детермінанти політичного простору. *Соціогуманітарні проблеми людини, 4*, 164-171.

60. Коловоротный, С. В. (2003). *Виртуальная реальность: манипулирование временем и пространством*. Available from: http://cyberpsy.ru/articles/virtual-realityl-time-space/

61. *Конвенція про захист прав людини і основоположних свобод* (2013). Available from: https://zakon.rada.gov.ua/laws/show/995_004

62. *Конвенція про кіберзлочинність* (2005). Available from: https://zakon.rada.gov.ua/laws/show/994_575

63. *Конгрес США розглядатиме законопроект щодо України* (2018). Available from: https://ukrainian.voanews.com/a/zakonoproect-po-ukraini/4239695.html

64. Кривенко, С.-В. О. (2016). *Семантична парадоксальність політичного дискурсу (теоретико-методологічний аналіз)*. Львів: Львівський національний університет ім. Івана Франка.

65. Кривошеїн, В. В. (2013). Ризики модернізації в контексті трансформації українського суспільства. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія Філософія, філософія права, політологія, соціологія, 3 (17)*, 186-189.

66. Кривошеїн, В. В. (2016). Постсистемні підходи до аналізу політики. In Н. М. Хома (Ed.), *Історія політичної думки* (pp. 614-631). Львів: Новий Світ-2000.

67. Кузанский, Н. (1980). *Сочинения* (Vol. 2). Москва: Мысль.

68. Лассуэлл, Г. Д. (1929). *Техника пропаганды в мировой войне* Available from: https://cardkit.ru/sites/default/files/page/files/tehnika_propagandi_v_mirovoy_voyne_file.pdf

69. Лефевр, А. (2015). *Производство пространства* (И. Стаф, Trans.). Москва: Strelka Press.

70. Липпман, У. (2004). *Общественное мнение* (Т. В. Барчунова, Trans.). Москва: Институт Фонда «Общественное мнение».

71. Литовченко, В. (2017). *Сучасна війна та нові моделі стратегічного партнерства України* Available from: http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3131/2812

72. Луман, Н. (2005). *Реальность масс-медиа* (А. Антоновский, Trans.). Available from: https://gtmarket.ru/laboratory/basis/3001/3015

73. Маккуайр, С. (2014). *Медийный город: медиа, архитектура и городское пространство* (М. Коробочкин, Trans.). Москва: Институт медиа, архитектуры и дизайна «Стрелка».

74. Мак-Люэн, М. (2003). *Галактика Гутенберга: Сотворение человека печатной культуры*. Киев: Ника-Центр.

75. Маклюэн, М. М., Фиоре, К. (2012). *Война и мир в глобальной деревне* (И. Летберг, Trans.). Москва: АСТ, Аслрель.

76. Мамаєва, М. (2019). *Комітет нацбезпеки: в Україні фактично вже створені кібервійська*. Available from: https://www.unn.com.ua/uk/news/1779815-komitet-natsbezpeki-v-ukrayini-faktichno-vzhe-stvoreni-kiberviyska

77. Манойло, А. (2003). *Государственная информационная политика в особых условиях*. Москва: МИФИ.

78. Маркузе, Г. (1994). *Одномерный человек*. Москва: REFL-book.

79. Мартиняк, Ю. О. (2016). *Взаємодетермінованість антропологічних та часово-просторових вимірів політичного*. Львів: Львівський національний університет імені Івана Франка.

80. Матвієнко, А. С. (2015). *Політико-правові засади територіальної організації держави: світовий досвід і Україна*. Київ: Інститут держави і права ім. В. М. Корецького НАН України.

81. Михайловский, А. А. (2017). Социально-философский анализ процесса виртуализации в контексте проблем системы «человек – общество – киберпространство». *Актуальні проблеми філософії та соціології, 18,* 86-90.

82. *Міністерство інформаційної політики: офіційний сайт*. Available from: https://mip.gov.ua/content/pro-ministerstvo.html

83. Міщук, Н. (2014). Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету. Серія економічна, 51*, 173-179.

84. Морозов, Е. (2014). *Интернет как иллюзия. Обратная сторона сети* (И. Кригер, Trans.). Москва: АСТ, CORPUS.

85. Мукомела, І. (2016). Право на доступ до Інтернету: проблеми визначення та забезпечення. *Вісник Національної академії правових наук України, 4 (87),* 77-85.

86. Мухина, Е. Н. (2015). Методы скрытия пространства: ускорение и симуляция. *Вісник ХНУ імені В. Н. Каразіна. Серія Філософія. Філософські перипетії, 53,* 69-77.

87. Носов, Н. (2000). Словарь виртуальных терминов. *Труды лаборатории виртуалистики, 7.*

88. Носов, Н. (2001). Манифест виртуалистики. *Труды лаборатории виртуалистики, 15*.

89. *Окінавська хартія глобального інформаційного суспільства* (2000). Available from: https://zakon.rada.gov.ua/laws/show/998_163

90. Олексюк, Л. (2017). *Кібербезпека та/або права людини*. Available from: http://vaibit.org.ua/wp-content/uploads/2017/07/%D0%92%D0%90%D0%86% D0%91%D0%86%D0% A2.pdf

91. Панченко, Ю. (2016). *Чому йде у відставку прем'єр Ісландії і чи багато спільного з українським скандалом*. Available from: https://www. eurointegration.com.ua/experts/2016/04/6/7047347/

92. Піскорська, Г. А., Яковенко, Н. Л. (2018). Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки. *Міжнародні відносини. Серія Політичні науки, 18-19.* Available from: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3389/3066

93. Платон (2000). *Держава* (Д. Коваль, Trans.). Київ: Основи.

94. Погребняк, Є. (2014). Електронний уряд (e-government) і електронне урядування (e-governance): поняття та принципи функціонування. *Право та інновації, 3 (7),* 26-35.

95. *Постанова Кабінету Міністрів України «Деякі питання цифрового розвитку»* (2019). Available from: https://zakon.rada.gov.ua/laws/show/56-2019-%D0%BF/print

96. *Постанова Кабінету Міністрів України «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави»* (2016). Available from: https://zakon2.rada.gov.ua/laws/show/563-2016-%D0%BF/paran17#n17

97. *Постоянное население: Демографический энциклопедический словарь* (1985). Москва: Советская энциклопедия, pp. 339-340.

98. Почепцов, Г. (2005). *Революция.com. Основы протестной инженерии*. Москва: Европа.

99. Почепцов, Г. (2016). *Смисли і війни: Україна і Росія в інформаційній і смисловій війні.* Київ: Києва-Могилянська Академія.

100. *Про невизнання державами-підписантами Конвенції Монтевідео суспільного утворення Росії державою у зв'язку з невизначеністю території*. Available from: https://petition.president.gov.ua/petition/20407

101. *Римський статут міжнародного кримінального суду* (2002). Available from: https://zakon.rada.gov.ua/laws/show/995_588

102. *Розпорядження Кабінету Міністрів України «Про затвердження плану дій з реалізації принципів Міжнародної хартії відкритих даних»* (2018). Available from: https://zakon.rada.gov.ua/laws/show/900-2018-%D1%80

103. *Розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України»* (2018). Available from: https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80

104. Ротар, Н. (2012). Политическое участие в эпоху второго модерна: в поисках адекватной модели. *Веснік Брэсцкага універсітэта. Серыя 1. Філасофія. Паліталогія. Сацыалогія, 1,* 89-96.

105. Ротар, Н., Байдич, К. В. (2011). Політичні комунікації в теорії Другого модерну. *Вісник Національного університету «Юридична академія України імені*

Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія, 9, 231-239.

106. Рузавин, Г. И. (2000). Виртуальность. In *Новая философская энциклопедия* (Vol. 1). Available from: http://iph.ras.ru/enc.htm

107. Свищ, І. (2004). Поняття процесу «віртуалізації культури» як категорія наукового дослідження. *Актуальні проблеми історії, теорії та практики художньої культури, 12,* 83-88.

108. Сегал, А. П. (2017). «Образ будущего» или виртуальная реальность? О пространстве формирования личности. *Профессиональное образование в современном мире, 7 (4),* 1380-1387.

109. Сергеева, Л. (2014). Проблема понятийно-категориального аппарата при классификации типов непризнанных (частично-признанных) государств постсоветского пространства. *Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики, 5 (43)*, 169-172.

110. Серёгин, А. В. (2000). *Информационное пространство как феномен культуры*. Москва: Государственная академия славянской культуры.

111. Силаева, В. Л. (2004). *Подмена реальности как социокультурный механизм виртуализации общества*. Москва: Московский государственный технический университет им. Н. Э. Баумана.

112. Славіна, О. В. (2017). «Pax Technica»: політико-філософська рефлексія впливу інтернет-мереж на природу публічної сфери й демократичного врядування. *Грані, 20 (8),* 50-57.

113. *Словник термінів з кібербезпеки* (2012), (О. Копатін, Є. Скулишин Eds.). Київ: АванпостПрим.

114. Солдатенко, О. (2018). Інформаційний простір у мережі Інтернет: правове регулювання та контроль. *Підприємство, господарство і право. Адміністративний процес, 5*, 134-140.

115. Соловов, Д. Н. (2010). Понятие виртуальности в философии Средневековья. *Вестник Российского университета дружбы народов. Серия: Философия, 4,* 72-76.

116. *Спільне звернення до Європейського парламенту, Ради, Європейського соціально-економічного комітету та Комітету регіонів: Стратегія ЄС із кібербезпеки: відкритий, надійний і безпечний кіберпростір* (2013) Available from: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

117. *Спільно з Україною в ролі лідерів з кібербезпеки: Законопроект Конгресу США* (2017). Available from: https://www.ukrinform.ua/rubric-polytics/2399870-spilno-z-ukrainou-v-rolilideriv-z-kiberbezpeki-zakonoproekt-kongresu-ssa.html

118. Тоффлер, Э. (2004). *Третья волна*. Москва: Издательство АСТ.

119. *У лавах Збройних сил створять кібервійська – Турчинов* (2018). Available from: https://www.ukrinform.ua/rubric-culture/2394973-odeskij-kinofestival-do-25-travna-prijmatime-zaavki-vid-volonteriv.html

120. Угрин, Л. (2016). Еволюція парадигми соціального конструктивізму як постнекласичної теорії пізнання. In Н. Хома (Ed.), *Політична думка XX – початку XXI століть: методологічний і доктринальний підходи* (Vol. 1, pp. 326-371). Львів: Новий Світ-2000.

121. *Указ Президента України Про Річну національну програму під егідою Комісії Україна – НАТО на 2019 рік* (2019). Available from: https://zakon.rada.gov.ua/laws/show/117/2019

122. *Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України»* (2017). Available from: https://zakon.rada.gov.ua/laws/show/47/2017

123. *Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»* (2016). Available from: https://zakon5.rada.gov.ua/laws/show/96/2016

124. *Україна має створити свої кібервійська – Осипенко* (2018). Available from: https://www.radiosvoboda.org/a/29250713.html

125. Федоров, О. С. (2017). Характеристика проектов создания новых виртуальных государств. *Локус: люди, общество, культуры, смыслы, 2,* 129-135.

126. Фуко, М. (1996). *Археология знания*. Киев: Ника-Центр.

127. Фуко, М. (1999). *Надзирать и наказывать. Рождение тюрьмы*. Москва: Ad Marginem.

128. Фурашев, В. (2012). Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право, 2 (5),* 162-175.

129. Хинтикка, Я. (1990). Логика в философии – философия логики. In: *Логикоэпистемологические исследований* (pp. 36-67). Москва: Прогресс.

130. Хома, Н. М. (2014). «Громадянин світу» (космополіт). In В. П. Мельник (Ed.), *Політологія: енциклопедичний словник* (pp. 65-66). Львів: Львівський національний університет імені Івана Франка.

131. Хома, Н. М. (2015). Віртуалізація держави: зміна функцій в добу цифромодернізму. *Науковий часопис Національного педагогічного університету імені М. П. Драгоманова, 16,* 64-69.

132. Хома, Н. М. (2015). Громадянство віртуальне (електронне). In М. Требін (Ed.), *Політологічний енциклопедичний словник* (pp. 159-160). Харків: Право.

133. Хома, Н. М. (2015). Детериторіалізація та ретериторіалізація : підходи до визначення ролі територій в умовах глобалізації. *Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін, 17,* 28-32.

134. Хома, Н. М. (2015). Е-резидент. In Н. М. Хома (Ed.), *Сучасна політична лексика: енциклопедичний словник-довідник* (p. 319). Львів: Новий Світ-2000.

135. Хома, Н. М. (2015). Кібердержава. In М. Требін (Ed.), *Політологічний енциклопедичний словник* (p. 329). Харків: Право.

136. Хома, Н. М. (2015). Територія як предмет вивчення політичної науки: основні теоретико-методологічні підходи. In Матеріали міжнародної науково-практичної конференції *Актуальні питання суспільних наук: соціологія, політологія, філософія, історія* (pp. 100-103). Київ: Київська наукова суспільствознавча організація.

137. Хома, Н. М. (2015). Хактивізм. In М. Требін (Ed.), *Політологічний енциклопедичний словник* (p. 773). Харків: Право.

138. Чернявская, В. (2011). Дискурс как объект лингвистических исследований. *Ученые записки Таврического национального университета им. В. И. Вернадского, Серия Филология. Социальные коммуникации.* Available from: http://science.crimea.edu/zapiski/2011/filologiya/uch24_3fn/041.pdf

139. Шопенгауэр, А. (1903). *Мир как воля и представление.* Available from: http://lib.ru/FILOSOF/SHOPENGAUER/s_zhizn.txt_with-big-pictures.html.

140. Шрайнер, Ю. А. (1988). *Концепции интеллектуальных систем. Научно-информационный обзор*. Москва: Наука.

141. Штепа, В. (2004). *Ритопия*. Екатеринбург: Ультра. Культура.

142. Юхвид, А. В. (2013). *Компьютерные виртуальные технологии как новый техно-социальный феномен: социально-философский анализ*. Москва: Российская академия государственной службы.

143. Яковенко, М. (2011). *Інформаційний простір: філософські аспекти формування поняття*. Available from: http://ena.lp.edu.ua/bitstream/ntb/10307/1/4.pdf

144. Яковлев, Д. В. (2009). *Політична взаємодія як комунікативний процес: медіатизація, демократизація, раціоналізація*. Одеса: Астропринт.

145. Якубін, О. (2014). Віріліо Поль. In Н. М. Хома (Ed.), *Історія політичної думки: навчальний енциклопедичний словник-довідник* (p. 132). Львів: Новий Світ-2000.

146. Abdulmula, A. (2017). The Five Models for E-Government. *Imperial Journal of Interdisciplinary Research, 3 (2)*. Available from: https://www.researchgate.net/publication/316829778_The_Five_Models_for_E-Government

147. Amyan, M., Al-saudi, M., Al-Onizat, H. (2016). The Effective Utilization of Knowledge Management in E-Government: A Case Study of E-Government in Jordan. *European Scientific Journal, 12,* 290-308.

148. Appadurai, A. (2000). Grassroots Globalizationandthe Research Imagination. *Public Culture, 12 (1),* 1-19.

149. Barlow, J. A. (1996). *Declaration of the Independence of Cyberspace*. Available from: https://www.eff.org/cyberspace-independence

150. Beck, U. (2006). *Cosmopolitan Vision* (C. Cronin, Trans.). Cambridge: Polity Press.

151. Bhagat, S. et. al. (2016). *Three and a half degrees of separation*. Available from: https://research.fb.com/three-and-a-half-degrees-of-separation/

152. Bühl, A. (1997). *Die virtuelle Gesellschaft: Ökonomie, Politik und Kultur im Zeichen des Cyberspace*. Opladen: VS Verlag für Sozialwissenschaften.

153. Cliffe, M. (2014). The New Abnormal. *Economics, 7.* Available from: https://markcliffe.files.wordpress.com/2014/11/the-new-abnormal-0511141.pdf

154. Couldry, N. (2008). Mediatization or mediation? Alternative understandings of the emergent space of digital storytelling. *New Media & Society, 10 (3)*, 373-391.

155. Couldry, N. (2008). Mediatization or mediation? Alternative understandings of the emergent space of digital storytelling. *New Media Society, 10 (3)*, 373-391.

156. Cukurcayir, M., Celebi, E. (2012). Information Society and Turkey in The Process of Implementing E-government. *ZKU Journal of Social Sciences, 5,* 59-82.

157. *Cyber-Sicherheitsstrategie für Deutschland 2016* (2016). Available from: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheits Strategie.pdf

158. DeLanda, M. (2002). *Intensive Science and Virtual Philosophy*. London: Continuum.

159. *Digital In 2018: World's Internet Users Pass The 4 Billion Mark* (2018). Available from: https://wearesocial.com/blog/2018/01/global-digital-report-2018

160. Featherstone, D., Painter, J. (Eds.) (2013). *Spatial Politics: Essays For Doreen Massey*. Oxford: Wiley-Blackwell.

161. Foucault, M. (2011). *Space, Knowledge, and Power*. Available from: http://www.mara-stream.org/wp-content/uploads/2011/11/Foucault_Space-Knowledge-Power.pdf

162. Franklin, D. K., Stuart, H. S., Larry K. W. (Eds.) (2009). *Cyberpower and National Security*. Washington: Potomac Books.

163. *Global Internet Policy Initiative* (2019). Available from: https://www.internetpolicy.net

164. Grönlund, Å. (2004). *Introducing e-Gov: History, Definitions, and Issues.* Available from: https://www.researchgate.net/publication/234008823_ Introducing_e-Gov_History_Definitions_and_Issues

165. Großklaus, G. (1995). *Medien-Zeit, Medien-Raum: zum Wandel der raumzeitlichen Wahrnehmung in der Moderne*. Frankfurt am Main: Suhrkamp.

166. Grossman, K. L. (1995).*The Electronic Republic: Reshaping Democracy in the Information Age*. New York: Viking.

167. Guibernau, M. (2004). Anthony D. Smith on nations and national identity: a critical assessment. *Nations and Nationalism, 10 (1-2),* 125-141.

168. Gümplová, P. (2015). On Sovereignty and Post-sovereignty. *Philosophica Critica, 1 (2),* 3-18.

169. Heim, M. (1991). The Metaphysics of virtual reality. In S. K. Helsel, J. P. Roth (Eds.), *Virtual reality: theory, practice and promise* (pp. 27-33). Westport and London.

170. Hjarvard, S. (2013). *The mediatization of culture and society*. New York: Routledge.

171. *HRC Affirms that Human Rights Must Also Be Protected on the Internet* (2012). Available from: http://geneva.usmission.gov/2012/07/05/internet-resolution/

172. Ingber, S. (1984). The Marketplace of Ideas: A Legitimizing Myth. *Duke University School of Law*, 33 (1), 1-91.

173. Katz, J. (1997). *The Digital Citizen*. Wired.

174. Kripke, S. A. (1963). Semantical considerations on Modal Logic. *Acta Philosophica Fennica, 16,* 83-94.

175. Krotz, F. (2008). Media Connectivity: Concepts, Conditions, and Consequences. In A. Hepp, F. Krotz & S. Moores (Eds.), *Network, Connectivity and Flow: Key concepts for Media and Cultural Studies*. New York: Hampton Press.

176. Lang, K., Lang, G. (1966). The Mass Media and Voting. In Berelson B., Janovvitz M (Eds.), *Reader in Public Opinion and Communication*. New York: Free Press.

177. Lazarsfeld, P. F., Merton, R. K. (1948). Mass Communication, Popular Taste, and Organized Social Action. In L. Bryson (Ed.), *The Communication of Ideas* (pp. 95-118). New York: Harper.

178. Leflow, B. (1989). A Leibnizian Cosmological Argument. *Philosophical Studies, 57,* 135-155.

179. March, J. C., Olsen, J. P. (2006). Elaborating the New Institutionalism. In R. A. W. Rhodes, S. A. Binder, B. A. Rockman (Eds.), *The Oxford Handbook of Political Institutions* (pp. 3-22). New York: Oxford University Press.

180. Masuda, Y. (1981). *The International Society as Post-Industrial Society*. Washington: World Future Society.

181. Mazzoleni, G., Schulz, W. (1999). „Mediatization" of Politics: A Challenge for Democracy? *Political Communication, 16 (3),* 247-261.

182. Merton, R. K. (1995). The Thomas Theorem and The Matthew Effect. *Social Forces, 74 (2),* 379-422.

183. Milgram, S. (1967). The Small World Problem. *Psychology Today, 2,* 60-67.

184. *Montevideo Convention on the rights and duties of states* (1933). Available from: https://www.ilsa.org/Jessup/Jessup15/Montevideo%20Convention. pdf

185. *National cyber strategy of the United States of America* (2018). Available from: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

186. *National Framework Of Cybersecurity Policy Of The Republic Of Poland For 2017–2022* (2017). Available from: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013

187. *Netze des Bundes* (2019). Available from: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/netze-des-bundes/netze-des-bundes-artikel.html

188. North, D. C. (1989). Institutions and Economic Growth: An Historical Introduction. *World Development, 17 (9),* 1319-1332.

189. Nye, J. S. (2005). *Soft power: the means to success in world politics*. Available from: https://www.academia.edu/28699788/Soft_Power_the_Means_to_Success_in_World_Politics_-_Joseph_S._Nye_Jr?auto=download

190. Piper, K. (2019). *Doomsday clock creators: "We're playing Russian roulette with humanity"*. *Vox Media*. Available from: https://www.vox.com/future-perfect/2019/1/24/18195527/doomsday-clock-2019-two-minutes-from-midnight

191. Robertson, D. S. (1990). *The Information revolution*. *Communication research*. New York.

192. Sajjad, M. (2016). *Media Democracy*. Available from: https://library.fes.de/pdf-files/bueros/pakistan/06540.pdf

193. Strömbäck, J. (2015). *The Mediatization of Politics – Reshaping Politics and Transforming Democracies*. Available from: http://www.grcp.ulaval.ca/ sites/grcp.ulaval.ca/files/stromback_2015.pdf

194. *The Common Criteria* (2019). Available from: https://www.commoncriteriaportal.org/

195. *The Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model* (2017). Available from: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

196. Thomas, W. I., Thomas, D. S. (1928). *The child in America: Behavior problems and programs.* New York: Knopf.

197. *Ukraine Cybersecurity Cooperation Act of 2017* (2017). Available from: https://www.congress.gov/bill/115th-congress/house-bill/1997

198. Virilio, P. (1977). *Speed and Politics: An Essay on Dromology*. Available from: https://archive.org/stream/PaulVirilioSpeedAndPolitics/Paul+ Virilio+-+Speed+and+Politics_djvu.txt

199. Waters, M. (1999). *Globalização*. Oeiras.

200. Waters, T., Waters, D. (2015). *Max Weber in Weber's Rationalism and Modern Society*. Palgrave Books.

201. *Wirtland 2008–2018* (2018). Available from: http://www.wirtland.com/

202. Zabokrytskyy, I. (2014). Sovereignty as one of the main criteria for the constitutionality of eu law. *The Advanced Science Journal, 6,* 102-105.

ДОДАТКИ

Додаток А

Список публікацій здобувача за темою дисертації

Праці, в яких опубліковані основні наукові результати дисертації

1. Потерейко, О. О. (2016). Теоретико-методологічні засади аналізу віртуалізації держави. *Вісник Львівського національного університету. Серія Філософсько-політологічні студії, 8*, 124–129.

2. Потерейко, О. О. (2016). Теоретико-методологічні підходи аналізу детериторіалізації у контексті віртуалізації держави. *Політикус, 1,* 38–40.

3. Потерейко, О. О. (2019). Населення як ознака віртуальної держави. *Гілея, 142,* 97–100.

4. Потерейко, О. О. (2019). Апарат управління як ознака держави в процесі віртуалізації. *Гілея, 144*, 108–111.

5. Potereiko, O. O. (2019). Government as a significant component of the virtual country. *Global Academics, 1 (2).* Available from: https://www.i-journal.org/upload/2.pdf

Праці, які засвідчують апробацію матеріалів дисертації

6. Потерейко, О. О. (2016). Віртуалізація держави як концептуальна характеристика еволюціонуючої політичної реальності. In Матеріали міжнародної науково-практичної конференції *Нове та традиційне у дослідженнях сучасних представників суспільних наук* (pp. 118-120). Київ: Київська наукова суспільнознавча організація.

7. Потерейко, О. О. (2016). Детериторіалізація як характеристика віртуалізації держави: аналіз теоретичних підходів. In Матеріали VI міжнародної науково-практичної конференції *Розвиток політичної науки: європейські практики та національні перспективи* (pp. 33-35). Чернівці: Чернівецький національний університет імені Юрія Федьковича.

8. Потерейко, О. О. (2017). Віртуалізація соціально-політичної реальності: основні риси та аспекти. In Тези звітної наукової конференції філософського факультету Львівського національного університету імені Івана Франка (pp. 194-195). Дрогобич: ТзОВ «Трек».

9. Потерейко, О. О. (2017). Процеси віртуалізації держави в сучасному світі: теоретико-методологічний аналіз. In Тези II всеукраїнської науково-практичної конференції *Сучасна українська держава: вектори розвитку та*

шляхи мобілізації ресурсів (pp. 126-129). Одеса: ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського».

10. Потерейко, О. О. (2017). Вихід інформації за межі територіальних кордонів: проблема регулювання кіберпростору. In Матеріали всеукраїнської науково-практичної конференції *Пріоритетні завдання і стратегії розвитку суспільних наук* (pp. 90-93). Запоріжжя: Класичний приватний університет.

11. Потерейко, О. О. (2018). Криптовалюта як результат тенденції віртуалізації новітнього інституту держави. In Матеріали III всеукраїнської науково-практичної конференції *Соціально-політичні проблеми сучасності* (pp. 73-75). Дніпро: Університет імені Альфреда Нобеля.

12. Потерейко, О. О. (2019). Детериторіалізація в системі ознак віртуальної держави. In Матеріали IV всеукраїнської науково-практичної конференції *Соціально-політичні проблеми сучасності* (pp. 10-12). Дніпро: Університет імені Альфреда Нобеля.

ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

1. Міжнародна науково-практична конференція “Нове та традиційне у дослідженнях сучасних представників суспільних наук” (Київ, 5-6 лютого 2016 р., заочна форма участі).

2. VI Міжнародна науково-практична конференція “Розвиток політичної науки: європейські практики та національні перспектив” (Чернівці, 7-8 квітня 2016 року, очна форма участі).

3. Звітна наукова конференція філософського факультету Львівського національного університету імені Івана Франка (Львів, 2 лютого 2017 р., очна форма участі).

4. II Всеукраїнська науково-практична конференція “Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів” (Одеса, 10 лютого 2017 р., заочна форма участі).

5. Всеукраїнська науково-практична конференція “Пріоритетні завдання і стратегії розвитку суспільних наук” (Запоріжжя, 17-18 листопада 2017 р., заочна форма участі).

6. III Всеукраїнська науково-практична конференція “Соціально-політичні проблеми сучасності” (Дніпро, 28 березня 2018 р., очна форма участі).

7. IV Всеукраїнська науково-практична конференція “Соціально-політичні проблеми сучасності” (Дніпро, 28 березня 2019 р., очна форма участі).