Київський національний університет імені Тараса Шевченка

Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

СУНГУРОВА САЛОМЕ РОМАНІВНА

УДК 323.23:316.776.23:316.324.8:004.056(043.3)

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА ВІЙНА ЯК ЗАСІБ ПОЛІТИЧНОГО НАСИЛЛЯ

Спеціальність 052 – Політологія

Галузь знань – Соціальні та поведінкові науки

Подається на здобуття наукового ступеня
доктора філософії у галузі соціальних та поведінкових наук

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

Науковий керівник (консультант) – **Хилько Микола Іванович**,
доктор філософських наук, професор

Київ – 2022

АНОТАЦІЯ

Сунгурова С.Р. Інформаційна війна як засіб політичного насилля. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії у галузі знань 05 «Соціальні та поведінкові науки» за спеціальністю 052 «Політологія». – Київський національний університет імені Тараса Шевченка, МОН України. – Київський національний університет імені Тараса Шевченка, Київ, 2022.

У сучасному інформаційно-цифровому суспільстві проблема інформаційної війни є однією з найбільш актуальних. Її прояви, інструменти, причини, наслідки тощо потребують детального наукового вивчення в силу загострення протистоянь у інформаційному вимірі, зростання загроз та перманентного удосконалення технологічної складової. Інформаційна війна є викликом для всіх суспільних секторів (приватного, громадського, державного). Мішенню інформаційних атак може стати буть-який актор, організація чи країна. Відповідно, протидія інформаційному насиллю, розробка проактивних заходів є пріоритетом в сучасному інформатизованому світі.

Для України в контексті виходу за межі гібридної і переходу до кінетичної війни з РФ дослідження інформаційної боротьби набуває ще більшої значущості, адже зусилля противника з дезінформації української та міжнародної аудиторій різко зросли і вирізняються небувалою активністю. Сьогодні у вітчизняних реаліях інформаційна війна, яку провадить країна-агресор проти України, є виразним прикладом політичного насилля в силу політичного змісту її цілей і завдань. Стратегія перемоги над супротивником, у тому числі й в інформаційному просторі, потребує системних наукових розвідок, виважених аналітик та обґрунтованих прогнозів. Наявність відповідних теоретичних та прикладних задач пояснює вибір теми даного дисертаційного дослідження та засвідчує його високу актуальність.

Інформаційна війна як засіб політичного насилля має свою специфіку, форми, функції, інструментарій і т. д. Осягнення останніх дозволить не лише забезпечити теоретичний фундамент для розуміння її поняття та феномена, а також дотичних соціально-політичних явищ, а й забезпечить оптимізацію стратегічного планування у практичній площині в умовах реальних воєнних дій. Акцент на політичному аспекті інформаційної війни поглиблює науковий дискурс, розкриваючи політичні мотиви, підтексти та передумови протистоянь у інформаційній площині. Суспільний запит на встановлення прозорих правил функціонування інформаційного поля, налагодження миру в межах останнього, запровадження дієвих інструментів покарання інформаційних злочинців підтверджує значущість політичної складової у розробці цих процесів. Установлення міжнародного публічного консенсусу щодо вирішення проблем політичного насилля, здійснюваного інформаційними засобами, має бути першочерговим завданням для переважної більшості демократичних держав, міжнародних установ та інститутів громадянського суспільства.

Метою дисертаційного дослідження є розкриття сутності інформаційної війни як засобу політичного насилля, обґрунтування її теоретичних засад, інструментального забезпечення та особливостей практичної реалізації. **Об’єкт** дослідження – політичне насилля. **Предмет** дослідження – інформаційна війна як засіб політичного насилля.

Уперше запропоновано авторську класифікацію провідних напрямів теоретичного осмислення політичного насилля (структурний, культурологічний та соціально-психологічний), яка доводить його варіативний детермінізм, а також осягнення дефініції «політичне насилля» через розкриття змісту такої понятійної паралелі, як «політичний інтерес» - «політичний конфлікт» - «політичне насилля»; розкрито зміст кібервійни через каузальний зв'язок кіберпростору, кіберсили та кіберстартегії; виявлено актуальні тендеції кібернетичної війни, а саме - посилення залежності від розвитку апаратного та програмного забезпечення; зниження ресурсної

витратності; домінування нападу над захистом; схильність до тиражування; зменшення вартості входу в кіберпростір тощо;

Удосконалено розуміння інформаційної війни як засобу політичного насилля (досягнення політичних цілей інформаційним інструментарієм) шляхом визначення її основних етапів, груп, форм та функцій, а також ролі атакувальної та захисної стратегій; обґрунтування детермінованості актуалізації інформаційної війни активним розвитком інформаційно-комунікаційних технологій; аналіз інструментарію інформаційної війни (інформаційної зброї), доведено, що він дозволяє викрадати, спотворювати чи знищувати інформацію; обмежувати чи припиняти доступ до неї законних користувачів; порушувати роботу або виводити з ладу телекомунікаційні мережі та комп'ютерні системи, що використовуються у забезпеченні життєдіяльності суспільства та держави; змінювати свідомість людей, змушувати їх неадекватно сприймати реальність, жити у світі ілюзій та робити згубні для себе вчинки тощо. До ключових категорій інформаційної зброї віднесено: збір, передачу, захист, маніпулювання, порушення, деградацію та заперечення;

Набуло подальшого розвитку дослідження міжнародного досвіду демократичних країн з протистояння загрозам у інформаційно-цифровому просторі, що передбачає відбиття кібер-ударів й інформаційних операцій, а також дії з контрнаступу з метою збереження західних демократичних цінностей, інститутів та систем; розширення міжнародної довіри в інформаційному просторі; звуження політичної, економічної та військової гегемонії авторитарних і тоталітарних держав в усьому світі; рефлексія стану політико-правового та інформаційно-технологічного забезпечення захисту інформаційної сфери України на основі дослідження актуальної законодавчо-нормативної бази та прикладних засобів протидії інформаційно-кібернетичним атакам. Боротьба в інформаційному просторі спрямована на протистояння провідним наративам РФ з дискредитації та дестабілізації України у вітчизняному, міжнародному та ворожому інформаційних полях, у

кібернетичному просторі – на протидію кібернетичним атакам на інфраструктурні об’єкти (DDoS-атаки, пошкодження веб-сайтів та зараження зловмисним програмним забезпеченням шляхом фішингу).

Стверджується, що політичне насилля поряд з іншими різновидами (економічне, соціальне, фінансове тощо) може відбуватися в інформаційній площині і бути одним із виявів інформаційного насильства. Серед провідних засобів можна виділити інформаційну атаку, інформаційну операцію, інформаційну війну та інформаційну експансію.

Виявлено, що інформаційна війна пов’язана з контролем над інформаційною сферою, що передбачає формування та спрямування інформаційних потоків на тактичному, оперативному та стратегічному рівнях, це контроль над джерелами та розповсюдженням інформації. Ведення інформаційної війни передбачає збір тактичної інформації; перевірку точності інформації; поширення пропаганди та дезінформації з метою деморалізації або маніпулювання опонентом та громадськістю; підривання якості інформації про опонента; позбавлення опонента можливості збирати інформацію тощо. Для досягнення політичних цілей переважно використовується психологічна форма інформаційної війни.

Доводиться, що одна з форм інформаційної війни – кібервійна – вирізняється динамічним розвитком та масштабуванням. Найближчими роками вона може стати домінуючою формою через низку причин економічного, географічного, політичного, технологічного порядку тощо. Осягнення суті кібервійни набуває логічності та комплексності в результаті розкриття каузальності між такими феноменами, як кіберпростір, кіберсила та кіберстратегія.

Ключові слова: інформаційна війна, політичне насилля, інформаційна зброя, кібернетичні атаки, стратегія, наративи, дезінформація, хакерські групи, інформаційне суспільство, інформація.

ANNOTATION

Sunhurova S.R. Information Warfare as a Means of Political Violence. - Qualification Scientific Work as a Manuscript.

Dissertation submitted for obtaining PhD in the field of study 05 " Social and Behavioral Sciences" on the specialty 052 "Political Science". - Taras Shevchenko National University of Kyiv, Ministry of Education and Science of Ukraine. - Taras Shevchenko National University of Kyiv, Kyiv, 2022.

In today's information and digital society, the problem of information warfare is one of the most pressing. Its manifestations, tools, causes, consequences, etc. require detailed scientific study due to the escalation of confrontations in the information dimension, the growth of threats and the permanent improvement of the technological component. Information warfare is a challenge for all social sectors (private, civil, public). Any actor, organization or country can be the target of information attacks. Accordingly, combating information violence and developing proactive measures is a priority in today's informatized world.

For Ukraine, in the context of going beyond the hybrid and moving to a kinetic war with Russia, the study of information warfare is even more important, as the enemy's efforts to misinform Ukrainian and international audiences have increased sharply and are unprecedented. Today, in the domestic realities, the information war waged by the aggressor country against Ukraine is a clear example of political violence due to the political content of its goals and objectives. The strategy of victory over the enemy, including the information space, requires systematic scientific research, balanced analysis, and grounded forecasts. The presence of relevant theoretical and applied problems explains the choice of the topic of this dissertation research and testifies to its high relevance.

Information warfare as a means of political violence has its own specifics, forms, functions, tools, etc. Understanding the latter could not only provide a theoretical foundation for understanding its concept and phenomenon, as well as related socio-political phenomena, but also optimize strategic planning, and practical plane in the conditions of real military actions. The emphasis on the political aspect

of information warfare deepens the scientific discourse, revealing the political motives, subtexts, and preconditions of confrontation in the information plane. The public demand for the establishment of transparent rules for the functioning of the information field, the establishment of peace within the latter, the introduction of effective tools for punishing information criminals confirms the importance of the political component in the development of these processes. Establishing an international public consensus for overcoming political violence, conducted by means of information tools, should be a priority for most democracies, international institutions, and civil society.

The **purpose** of the dissertation is to reveal the essence of information warfare as a means of political violence, substantiation of its theoretical foundations, tools and features of practical implementation. The **object** of the research is political violence. The **subject** of the research is information warfare as a means of political violence.

For the first time, the author's classification of the leading directions of political violance theoretical understanding (structural, cultural and socio-psychological) has been proposed, which proves its variable determinism, as well as understanding of the main definition through the logical parallel "political interest" – "political conflict" – "political violence"; the content of cyber war is revealed through the causal connection of cyberspace, cyber power and cyber strategy; the current trends of cyber warfare were revealed, namely - increased dependence on the development of hardware and software; reduction of resource consumption; dominance of attack over defense; propensity for replication; reducing the cost of entering cyberspace, etc.;

Understanding of information warfare as a means of political violence (achieving political goals with information tools) by identifying its main stages, groups, forms, and functions, as well as clarifying the role of offensive and defensive strategies **has been improved**; substantiation of the determinism of the actualization of information warfare by the active development of information and communication technologies took place;

Analysis of the tools of information warfare (information weapons), proven to allow stealing, distorting or destroying information; restrict or terminate access to it by legitimate users; to disrupt or disable telecommunications networks and computer systems used to ensure the vital activities of society and the state; to change people's consciousness, make them perceive reality inadequately, live in a world of illusions and do things harmful to themselves, etc. was conducted. Key categories of information weapons include collection, transmission, protection, manipulation, violation, degradation, and denial;

The study of the international experience of democratic countries in countering threats in the information and digital space, which involves repelling cyber attacks and information operations, as well as counteroffensive actions aimed at preserving Western democratic values, institutions and systems; expansion of international trust in the information space; narrowing of the political, economic and military hegemony of authoritarian and totalitarian states throughout the world **was further developed**; as well as reflection of the state of political-legal and information-technological support for the protection of the information sphere of Ukraine based on the study of the current legislative and regulatory framework and applied means of countering information-cybernetic attacks. The fight in the information space is aimed at countering the leading narratives of the Russian Federation on discrediting and destabilizing Ukraine in the domestic, international and hostile information fields, in the cyber space - at countering cyber attacks on infrastructure objects (DDoS attacks, website damage and phishing software).

It is argued that political violence, along with other forms (economic, social, financial, etc.) can occur in the information plane and be one of the manifestations of information violence. Among the leading means are information attack, information operation, information warfare and information expansion.

It was found that the information war is associated with control over the information sphere, which involves the formation and directing of information flows at the tactical, operational and strategic levels, it is a control over the sources and dissemination of information. Information warfare involves the collection of tactical

information; checking the accuracy of information; dissemination of propaganda and misinformation to demoralize or manipulate the opponent and the public; undermining the quality of information about the opponent; depriving the opponent of the opportunity to gather information, etc. The psychological form of information warfare is mainly used to achieve political goals.

It turns out that one of the forms of information warfare - cyber warfare - is characterized by dynamic development and scaling. In the coming years, it may become the dominant form for a few reasons, economic, geographical, political, technological, and so on. Understanding the essence of cyber warfare becomes logical and complex because of revealing the causality between such phenomena as cyberspace, cyberspace and cyber strategy.

Key words: information warfare, political violence, information weapons, cyber-attacks, strategy, narratives, misinformation, hacker groups, information society, information.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України, які входять до міжнародних наукометричних баз:

1. Сунгурова С.Р. Феномен та методи протидії інформаційному насильству в умовах сучасних інформаційних протистоянь. Гілея: науковий вісник. 2019. Вип. 148 (№9). С. 68-73.
2. Сунгурова С.Р. Концептуальні підходи до дослідження поняття та феномену інформаційної війни. Вісник Львівського університету. Серія філософсько-політологічні студії. 2020. №29. С. 251-256.
3. Сунгурова С.Р. Теоретико-методологічні засади дослідження політичного насилля: ключові підходи. Гілея: науковий вісник. 2020. Вип. 159 (№ 11-12). Ч. 3. Політичні науки. С. 129-135.
4. Сунгурова С.Р. Політико-інформаційна війна: функціонально-інструментальний аспект. «Politicus». Науковий журнал. 2021. № 6. С. 67-72.
5. Сунгурова С.Р. Види кібернетичних атак РФ та їх соціально-політичні наслідки для України. Регіональні студії: журнал. 2022. № 28. С. 88-91.
6. Сунгурова С.Р. Міжнародний досвід боротьби з політичним насиллям засобами інформаційної війни. Політологічний вісник: Збірник наукових праць/голов.ред. О.В.Батрименко, Київський національний університет імені Тараса Шевченка. Київ: ТОВ «ВАДЕКС», 2022. Вип.88. С.202-218

Тези, опубліковані за матеріалами наукових конференцій:

1. Сунгурова С.Р. Використання соціальних мереж у здійсненні інформаційно-психологічних впливів під час проведення операції Об’єднаних сил. Українське військо: сучасність та історична ретроспектива, Матеріали Всеукраїнської науково-практичної конференції, 29 листопада, Київ, 2019. С. 39-40.
2. Сунгурова С.Р. Інформаційна війна як елемент інформаційного

суспільства: політичний аспект. Нові завдання суспільних наук у XXI столітті, Матеріали Міжнародної науково-практичної конференції, 19-20 червня, Київ, 2020. С. 60-63.

3. Сунгурова С.Р. Політичне насилля в інформаційній сфері: особливості та ключові проблеми. Суспільні науки сьогодні: постулати минулого і сучасні теорії, Матеріали Міжнародної науково-практичної конференції, 6-7 листопада, Дніпро, 2020. С. 86-90.

4. Sunhurova S. Political Violence: Conceptual and Category Aspect. The Days of Science of the Faculty of Philosophy - 2021, International Scientific Conference Materials 21-22 Apr. Kyiv, 2021. P. 352-354.

5. Сунгурова С.Р. Інформаційний тероризм як різновид злочинної діяльності політичної спрямованості. Пріоритетні напрями вирішення актуальних проблем суспільних наук, Матеріали Міжнародної науково-практичної конференції, 15-16 жовтня, Одеса, 2021. С. 66-69.

6. Сунгурова С.Р. Інформаційна війна РФ проти України: ключові дискурси. Інноваційні наукові дослідження в умовах світових змін, Матеріали Міжнародної науково-практичної конференції, 29-30 квітня, Вінниця, 2022. С. 75-79.

LIST OF PUBLISHED PAPERS ON THE TOPIC OF THE DISSERTATION

Articles in the Ukrainian Scientific Editions, Included in the International Online Databases:

1. Sunhurova S. The Phenomenon and Methods of Counteracting Information Violence in the Conditions of Modern Information Conflicts. Hileya: Scientific Bulletin. 2019. Volume 148 (№ 9). P. 68-73.
2. Sunhurova S. Conceptual Approaches to the Study of the Concept and Phenomenon of Information War. Visnuk of the Lviv University. Series Philos.-Political Studies. Issue 29. P. 251-256.
3. Sunhurova S. Theoretical and Methodological Grounds of the Political Violence Study: Key Approaches. Hileya: Scientific Bulletin. 2020. Volume 159 (№ 11-12). Part 3. Political sciences. P. 129-135.
4. Sunhurova S. Political and Information War: Instrumental and Functional Aspect. Politicus. Scientific journal. 2021. Vol. 6. P. 67-72.
5. Sunhurova S. Types of Cybernetic Attacks of the Russian Federation and their Socio-Political Consequences for Ukraine. Regional Studies: journal. 2022. Vol. 28. P. 88-91.

Abstracts Published on the Materials of Scientific Conferences:

6. Sunhurova S. The Use of Social Networks in the Smplementation of Informational and Psychological Influences during the Operation of the United Forces. Ukrainian Army: Modernity and Historical Retrospective, Materials of the All-Ukrainian Scientific and Practical Conference, November 29, Kyiv, 2019. P. 39-40.
7. Sunhurova S. Information Warfare as an Element of the Information Society: Political Aspect. New Tasks of Social Sciences in the XXI Century, Proceedings of the International Scientific-Practical Conference, June 19-20, Kyiv, 2020. P. 60-63.
8. Sunhurova S. Political Violence in the Information Sphere: Features and Key Issues. Social Sciences Today: Postulates of the Past and Modern Theories, Proceedings of the International Scientific-Practical Conference, November 6-7,

Dnipro, 2020. P. 86-90.

9. Sunhurova S. Political Violence: Conceptual and Category Aspect. The Days of Science of the Faculty of Philosophy - 2021, International Scientific Conference Materials 21-22 Apr. Kyiv, 2021. P. 352-354.

10. Sunhurova S. Information Terrorism as a Kind of Criminal Activity of Political Orientation. Priority Areas for Solving Current Problems of Social Sciences, Proceedings of the International Scientific and Practical Conference, October 15-16, Odesa, 2021. P. 66-69.

11. Sunhurova S. Russia's Information War Against Ukraine: Key Discourses. Innovative Scientific Research in the Conditions of World Changes, Proceedings of the International scientific-practical conference, April 29-30, Vinnytsia, 2022. P. 75-79.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. У сучасному інформаційно-цифровому суспільстві проблема інформаційної війни є однією з найбільш актуальних. Її прояви, інструменти, причини, наслідки тощо потребують детального наукового вивчення в силу загострення протистоянь у інформаційному вимірі, зростання загроз та перманентного удосконалення технологічної складової. Інформаційна війна є викликом для всіх суспільних секторів (приватного, громадського, державного). Мішенню інформаційних атак може стати буть-який актор, організація чи країна. Відповідно, протидія інформаційному насиллю, розробка проактивних заходів є пріоритетом в сучасному інформатизованому світі.

Для України в контексті виходу за межі гібридної і переходу до кінетичної війни з РФ дослідження інформаційної боротьби набуває ще більшої значущості, адже зусилля противника з дезінформації української та міжнародної аудиторій різко зросли і вирізняються небувалою активністю. Сьогодні у вітчизняних реаліях інформаційна війна, яку провадить країна-агресор проти України, є виразним прикладом політичного насилля в силу політичного змісту її цілей і завдань. Стратегія перемоги над супротивником, у тому числі й в інформаційному просторі, потребує системних наукових розвідок, виважених аналітик та обґрунтованих прогнозів. Наявність відповідних теоретичних та прикладних задач пояснює вибір теми даного дисертаційного дослідження та засвідчує його високу актуальність.

Інформаційна війна як засіб політичного насилля має свою специфіку, форми, функції, інструментарій і т. д. Осягнення останніх дозволить не лише забезпечити теоретичний фундамент для розуміння її поняття та феномена, а також дотичних соціально-політичних явищ, а й забезпечить оптимізацію стратегічного планування у практичній площині в умовах реальних воєнних дій. Акцент на політичному аспекті інформаційної війни поглиблює науковий дискурс, розкриваючи політичні мотиви, підтексти та передумови протистоянь у інформаційній площині. Суспільний запит на встановлення

прозорих правил функціонування інформаційного поля, налагодження миру в межах останнього, запровадження дієвих інструментів покарання інформаційних злочинців підтверджує значущість політичної складової у розробці цих процесів. Установлення міжнародного публічного консенсусу щодо вирішення проблем політичного насилля, здійснюваного інформаційними засобами, має бути першочерговим завданням для переважної більшості демократичних держав, міжнародних установ та інститутів громадянського суспільства.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційна робота виконана на кафедрі військової політології Військового інституту Київського національного університету імені Тараса Шевченка в межах Комплексної наукової програми Київського національного університету імені Тараса Шевченка «Модернізація суспільного розвитку України в умовах світових процесів глобалізації».

Мета і завдання дослідження. Метою дисертаційного дослідження є розкриття сутності інформаційної війни як засобу політичного насилля, обґрунтування її теоретичних засад, інструментального забезпечення та особливостей практичної реалізації.

Досягнення поставленої мети зумовило необхідність розв'язання таких **завдань**:

− проаналізувати концептуальні підходи до визначення поняття і сутності політичного насилля;

− розкрити зміст інформаційної війни як наукової дефініції та соціально-політичного феномена;

− дослідити стратегічний та інструментально-функціональний аспекти інформаційної війни;

− з'ясувати провідні тенденції інформаційної війни у кіберпросторі;

− узагальнити міжнародний досвід організації протистояння політичному насиллю засобами інформаційної війни;

− виявити специфіку захисту інформаційної сфери України в контексті інформаціної війни як засобу протидії політичному насиллю.

Об'єкт дослідження – політичне насилля.

Предмет дослідження – інформаційна війна як засіб політичного насилля.

Методи дослідження. Методологічним фундаментом дисертаційної роботи став комплекс загальнонаукових та спеціальних методів. Серед перших ключовими для дослідження були аналіз, аналогія, абстрагування та конкретизація. Серед других – бібліографічний, системний, компаративний, порівняльно-правовий. Використання бібліографічного методу дозволило визначити концептуальні засади дослідження інформаційної війни як засобу політичного насилля шляхом систематизації великого масиву науково-дослідної літератури. Системний метод став у нагоді під час структурування форм інформаційної війни, виокремлення теоретичних напрямків аналізу політичного насилля, систематизації провідних наративів РФ в інформаційній війні проти України та інших держав світу, об'єктивації ключових видів кібернетичних атак РФ тощо. Компаративний підхід використовувався у процесі дослідження інформаційно-воєнних практик РФ, спрямованих проти різних держав (Болгарія, Грузія, Молдова, Мексика, США, Франція тощо), а також діяльності російських APT груп. Порівняльно-правовий метод було задіяно у ході вивчення законодавчої, нормативно-правової та нормативної баз, які регулюють систему захисту інформаційного простору в Україні.

Наукова новизна здобутих результатів зумовлена специфікою детермінованих завдань. У дисертації проведено комплексне дослідження концептуальних засад, структурних та інструментальних особливостей, а також практики інформаційної війни як засобу політичного насилля. Найбільш вагомі результати дисертаційного дослідження, які містять наукову новизну, полягають у тому, що:

уперше:

- запропоновано авторську класифікацію провідних напрямів теоретичного осмислення політичного насилля (структурний,

культурологічний та соціально-психологічний), яка доводить його варіативний детермінізм, а також осягнення дефініції «політичне насилля» через розкриття змісту такої понятійної паралелі, як «політичний інтерес» - «політичний конфлікт» - «політичне насилля»;

- розкрито зміст кібервійни через каузальний зв'язок кіберпростору, кіберсили та кіберстартегії; виявлено актуальні тендеції кібернетичної війни, а саме - посилення залежності від розвитку апаратного та програмного забезпечення; зниження ресурсної витратності; домінування нападу над захистом; схильність до тиражування; зменшення вартості входу в кіберпростір тощо;

удосконалено:

- розуміння інформаційної війни як засобу політичного насилля (досягнення політичних цілей інформаційним інструментарієм) шляхом визначення її основних етапів, груп, форм та функцій, а також ролі атакувальної та захисної стратегій; обґрунтування детермінованості актуалізації інформаційної війни активним розвитком інформаційно-комунікаційних технологій;

- аналіз інструментарію інформаційної війни (інформаційної зброї), доведено, що він дозволяє викрадати, спотворювати чи знищувати інформацію; обмежувати чи припиняти доступ до неї законних користувачів; порушувати роботу або виводити з ладу телекомунікаційні мережі та комп'ютерні системи, що використовуються у забезпеченні життєдіяльності суспільства та держави; змінювати свідомість людей, змушувати їх неадекватно сприймати реальність, жити у світі ілюзій та робити згубні для себе вчинки тощо. До ключових категорій інформаційної зброї віднесено: збір, передачу, захист, маніпулювання, порушення, деградацію та заперечення;

набуло подальшого розвитку:

- дослідження міжнародного досвіду демократичних країн з протистояння загрозам у інформаційно-цифровому просторі, що передбачає відбиття кібер-ударів й інформаційних операцій, а також дії з контрнаступу з метою

збереження західних демократичних цінностей, інститутів та систем; розширення міжнародної довіри в інформаційному просторі; звуження політичної, економічної та військової гегемонії авторитарних і тоталітарних держав в усьому світі;

- рефлексія стану політико-правового та інформаційно-технологічного забезпечення захисту інформаційної сфери України на основі дослідження актуальної законодавчо-нормативної бази та прикладних засобів протидії інформаційно-кібернетичним атакам. Боротьба в інформаційному просторі спрямована на протистояння провідним наративам РФ з дискредитації та дестабілізації України у вітчизняному, міжнародному та ворожому інформаційних полях, у кібернетичному просторі – на протидію кібернетичним атакам на інфраструктурні об’єкти (DDoS-атаки, пошкодження веб-сайтів та зараження зловмисним програмним забезпеченням шляхом фішингу).

Практичне значення здобутих результатів. Основні положення дисертаційного дослідження поглиблюють наукові знання про сутність інформаційної війни як засобу політичного насилля, її форми, інструментальний та стратегічний аспекти, особливості практики у вітчизняних реаліях, а також світовий досвід протистояння інформаційним атакам. Сформовані у дисертації ідеї та висновки можуть використовуватися у процесі складання лекційних курсів та спецкурсів, а також при укладанні навчальних посібників з політичних та інших суспільних наук. Окрім цього, результати наукового дослідження в силу прикладної орієнтації можуть застосовуватися воєнними та політичними практиками для уточнення стратегічних та тактичних кроків у процесі захисту інформаційного простору від деструктивних активностей ворожих акторів.

Апробація результатів дисертації. Провідні положення дисертаційної роботи були оприлюднені під час науково-практичних конференцій, зокрема: «Українське військо: сучасність та історична ретроспектива» (Київ, 2019), «Нові завдання суспільних наук у XXI столітті» (Київ, 2020), «Суспільні науки

сьогодні: постулати минулого і сучасні теорії» (Дніпро, 2020), «Дні науки філософського факультету – 2021» (Київ, 2021), «Пріоритетні напрями вирішення актуальних проблем суспільних наук» (Одеса, 2021), «Інноваційні наукові дослідження в умовах світових змін» (Вінниця, 2022).

Особистий внесок здобувача. Усі пункти новизни, що виносяться на захист, а також висновки, запропоновані у даній дисертаційній роботі, належать виключно авторці дослідження, апробовані й опубліковані дисертанткою наукові праці написані нею самостійно.

Публікації. Основні положення дисертації викладені у 11 публікаціях, зокрема, у п’яти статтях, опублікованих у фахових виданнях України, які включені до міжнародних наукометричних баз, та шести тезах виступів на наукових конференціях.

Структура. Дисертація містить вступ, три розділи, поділені на підрозділи, списки використаних джерел до кожного розділу та висновки. Загальний обсяг дисертації становить 204 сторінки. Список використаних джерел складається з 281 найменування на 26 сторінках.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ В КОНТЕКСТІ ПОЛІТИЧНОГО НАСИЛЛЯ

1.1 Концептуальні підходи до дослідження політичного насилля

Насилля нерозривно пов’язане з політикою, виступаючи вагомим аргументом у досягненні політичних цілей. Воно з необхідністю виникає в зоні конфронтаційних політичних інтересів і є одним із способів розв’язування політичного конфлікту. Політичне насилля попри збільшення демократичних країн на політичній мапі світу не зникає з арсеналу акторів політичних протистоянь, і набуває все більш рафінованих й латентних форм та засобів. Саме тому політичне насильство є однією з провідних тем сучасного наукового дискурсу в політології та інших суспільних науках.

Теоретичні засади дослідження політичного насилля прямо пов’язані з понятійно-категоріальним каркасом цього поняття. Розуміння суті феномену формується значною мірою за рахунок усвідомлення змісту дефініції, що його репрезентує у науковому контексті, а також інших суміжних термінів. Саме тому одне із завдань, яке ми ставимо перед собою у цьому підрозділі, полягає у вивченні ключових для його проблематики понять. Логічно виваженим аналітичним кроком на початку даного підрозділу вважаємо апеляцію до родового по відношенню до «політичного насилля» поняття насильства.

У сучасній науці існує ряд трактувань категорії «насильство», які склались історично та можуть відрізнятись одне від одного залежно від галузі знань. У загальному розумінні насильство – це соціокультурний феномен, вельми складний, багатоаспектний за своєю структурою та включеністю в соціальні мережі [13, с. 25]. Насильство – постійний атрибут історичного процесу і людського життя. При певному його тлумаченні, інтерпретації та поясненні можна вважати, що воно з’явилося задовго до людини [13, с. 29].

Насильство – це дія (зокрема, силова) на людину або групу людей, що суперечить закономірному перебігу подій: фізичним і біологічним закономірностям, юридичним нормам, моральним принципам. Як правило, всі існуючі визначення насильства носять антропоморфний характер, скрізь йдеться про суб'єкт і об'єкт насильства. За традиційного підходу об'єкт насильства – людина, але навіть у цьому разі існує насильство над природою і тваринами. Тобто, об'єкт виходить за рамки соціуму, тому при розширеному тлумаченні насильство може розумітися як таке, що має стосунок до живої і неживої природи [13, с. 49].

Політичні науки трактують поняття «насильство» дещо під іншим ракурсом. По-перше, так звану «монополію на насильство» має держава, яка «легітимізувала» примус, тобто це делеговане народом право держави на насильство в умовах суспільного договору (Ж. Боден, Т. Гоббс, М. Вебер тощо). По-друге, насильство є діяльністю, спрямованою на затвердження політичного домінування певних соціальних верств (класів, еліт) за рахунок обмеження прав і потреб інших суспільних груп.

А. Гусейнов відмітив, що видів насильства нітрохи не менше, аніж сфер людської діяльності. Суть насильства полягає в тому, щоб змусити конкретну людину або спільноту людей до дій, які суперечать їх власним інтересам [10]. На думку Є. Доценко, категорію «обман» можна віднести до одного з видів насильства. Стабілізуюча функція обману широко використовується державними органами, засобами масової інформації, причому в найрізноманітніших формах – від ретельно продуманої дезінформації (добре застрахованої від викриття) до тонких маніпуляційних дій над суспільною свідомістю, що формують вигідну громадську думку, яка підтримує потрібні уряду символи віри [15].

Враховуючи логіку формування та дії політичного насилля, яке з'являється в ході політичного конфлікту, який у свою чергу спричинений протилежними політичними інтересами, вважаємо доцільним розглядати понятійно-категоріальну складову дослідження через наступну паралель:

«політичний інтерес» - «політичний конфлікт» - «політичне насилля». Ця термінологічна тріада постає головною віссю та опорою дослідження наукових засад політичного насилля. Розглянемо окремі авторські підходи до їх трактування.

«Політичний інтерес можна визначити як відношення людини, соціальної групи до будь-яких політичних впливів, процесів, політичної діяльності, засноване на їхніх світоглядних принципах, переконаннях, настановах, є внутрішнім джерелом політичної поведінки, який спонукає людей до встановлення політичних цілей та здійснення конкретних політичних дій, спрямованих на їх досягнення» [28, с. 602].

На думку К. Старостенка, політичні інтереси «виступають в якості основи теоретичної і практичної діяльності в сфері політики, служать формуванню відповідних політико-правових систем, економік, відносин в суспільстві і міждержавних зв’язків» [30, с. 1].

«Політичні інтереси як соціальне явище пов’язані з потребами різних членів суспільства та є важливим елементом механізму регулювання людської діяльності. Через політичні інтереси індивідуальності існують суспільно-соціальні та класові інтереси. Але при цьому політичний інтерес завжди конкретний: індивідуальний та груповий, класовий, суспільний та загальнолюдський. Формування політичного інтересу є процесом усвідомлення суб’єктом своїх потреб у контексті наявних політичних умов та існуючих можливостей їх задоволення» [1].

«Політичні інтереси - це вираження потреб суспільства, соціальних груп, політичної організації, руху в соціальній та політичній сфері. Інтереси служать джерелом, мотивом, підбурюючим до певних дій, наприклад, участі у виборах, організації та проведення мітингу, роботи політичних інститутів тощо» [7].

З усіх вище наведених дефініцій формується чітке резюме, що політичний інтерес спричинений соціально-політичними потребами, оформлюється у конкретну політичну мету, є мотивацією до політичної дії, вирізняється мультисуб’єктністю (переважно групи інтересів) і в разі труднощів в процесі

реалізації (протистояння різних політичних інтересів) може призвести до політичного конфлікту.

М. Примуш визначає політичний конфлікт як «… протиборство реальних суспільних сил (агентів), що уособлюються лідерами, елітами, організаціями, партіями та іншими об'єднаннями і спільнотами. Це протиборство суб'єктів з протилежними політичними інтересами, цінностями, поглядами і цілями, обумовленими становищем та роллю у системі владних відносин. Поняття політичного конфлікту означає не що інше, як боротьбу одних суспільних сил з іншими за вплив у інститутах політичної державної влади й управління, за доступ до ухвалення суспільно значущих рішень, за участь у розпорядженні ресурсами, за монополію своїх інтересів та визнання їх загальними, тобто за все, що утворює владу і політичне панування» [27, с. 97].

І. Федірко тлумачить політичний конфлікт як зіткнення, протиборство політичних суб'єктів, обумовлене протилежністю їх політичних інтересів, цінностей, цілей і намірів, як різновид і результат конфліктної поведінки сторін (груп, держав, індивідів), які прагнуть перерозподілу владних повноважень і ресурсів [31, с. 63].

Г. Жекало визначає політичний конфлікт як «… один із різновидів соціального конфлікту, який характеризується зіткненням протилежних цілей та прагнень, які стикаються з приводу влади, владних відносин у політичному середовищі та зачіпають інтереси великої кількості людей» [16, с. 46].

Отже, політичний конфлікт – це зіткнення соціально-політичних акторів через протистояння їхніх політичних інтересів. Розгортання політичного конфлікту у науково-дослідній літературі, зазвичай, називають політичною боротьбою [24]. Попри видову варіативність, політичний конфлікт має два основні способи реалізації: мирний та агресивний. Мирний спосіб розгортання передбачає толерантне поводження суб'єктів по відношенню один до одного, ведення перемовин і пошук компромісного варіанту розв'язання конфлікту. Агресивний спосіб означає жорстку позицію кожного із суб'єктів протиборства, відмову від конструктивного діалогу, боротьбу за кінцеву мету

будь-якою ціною. Власне, в межах останнього способу найчастіше і знаходить простір застосування політичне насилля.

«Політичне насилля – це зневажання, примушення одним (одними) іншого (інших): особистості, правителя, політика, держави, групи, еліти, класу, панівної нації і національної групи тощо. Його сутність полягає у впливі, що нав'язується, примусі, тискові на об'єкти і суб'єкти з метою виконання ними волі, дій, політики, поведінки, всього способу життєдіяльності, що нав'язується, диктується. Політичне насилля обмежує (або знищує) свободу людей, їх дій і вчинків, призводить до маніпулювання ними, робить їх залежними, в певній мірі рабами провідників насилля. Сенс насилля полягає в тому, щоби блокувати волю індивідів і змусити їх (або утримати) від дій, які диктуються тими, хто здійснює насилля. Насилля взагалі можна коротко визначити як узурпацію свободи волі. Це є панування одних індивідів над іншими, засноване на зовнішньому примусі» [3, с. 163].

А. Кугай пропонує наступне визначення політичного насилля: «придушення або примусове обмеження свободи волі соціального суб'єкта, обумовлене діями соціальних сил: які прагнуть політичної влади, її здійснюють, стверджують певний соціально-політичний ідеал» [18, с. 13].

С. Кузіна розуміє під політичним насиллям «спосіб інституціоналізації суспільних відносин, в ході якого одні індивіди або групи людей за допомогою різних засобів зовнішнього примусу і маніпулювання підпорядковують собі свідомість, волю, здібності, продуктивні сили, власність і свободу інших з метою оволодіння владою, її утримання і функціонування» [19, с. 3].

Отже, політичне насилля – це фізичний та/або психологічний тиск одного політичного актора (акторів) на іншого (інших) з метою реалізації власної політичної волі у вигляді досягнення конкретної політичної цілі, що може мати як ідеалістичний, так і матеріалістичний характер.

Політичне насильство - це насильство, яке здійснюється людьми чи урядами для досягнення політичних цілей. Воно може включати насильство, яке застосовується державою проти інших держав (війна), або може описувати

насильство, яке застосовується щодо недержавних суб'єктів (зокрема, жорстокість міліції або геноцид). Воно може також проявлятися у вигляді політично вмотивованого насильства, яке застосовується недержавними акторами проти держави (заколот, заворушення, державна зрада чи державний переворот), або описувати насильство, яке застосовується проти інших недержавних суб'єктів. Недію з боку уряду також можна охарактеризувати як одну з форм політичного насильства, наприклад, відмову пом'якшити голод або відмову надання ресурсів політично визначеним групам на їх території тощо.

Через дисбаланс влади, що існує між державними та недержавними суб'єктами, політичне насильство часто набуває форми асинхронної війни, коли жодна зі сторін не може безпосередньо напасти на іншу, натомість спираються на такі тактики, як тероризм або партизанська війна, які можуть часто включати напади на цивільні або військові цілі. Багато груп та окремих людей вважають, що їхні політичні системи ніколи не відреагують на їхні вимоги, і, отже, вони вважають, що насильство є не лише виправданим, але й необхідним для досягнення своїх політичних цілей. Подібним чином, багато урядів у всьому світі вважають, що їм потрібно застосовувати насильство, щоб залякати своє населення і схилити до поступки. Окрім цього, уряди застосовують силу, щоб захищати свої країни від сторонніх вторгнень чи інших силових погроз та примушувати інші уряди до певних політичних рішень або ж з метою завоювання територій.

Серед світових мислителів, які проводили ґрунтовні теоретичні розробки політичного насилля, доречно згадати Г. Арендт, Ж. Бодріяра, П. Бурьє, М. Вебера, Т. Гоббса, А. Грамші, Н. Лумана, Н. Макіавеллі, К. Маркса, М. Фуко тощо. Кожен із цих дослідників презентував власну авторську позицію щодо політичного насилля у межах певної філософської традиції. Серед вітчизняних науковців, які займалися ревізією поглядів вище згаданих теоретиків, найбільш зваженими науковими студіями вирізняються О. Балацька, С. Брехаря, В. Кравченко, Л. Левченко, Т. Хомич. Вони

забезпечують аналіз понятійно-категоріального апарату, виявляють специфіку концепцій класиків, але не пропонують системного бачення більшості підходів та теорій у вигляді класифікації. Саме тому одне з завдань цього підрозділу полягає в об'єднанні позицій різних науковців у певні теоретичні напрями за спільністю методологічних настанов, структуруванні теоретичного поля з проблеми політичного насилля за критерієм його джерел.

Вивчення науково-дослідної літератури на обрану тему вказує на наявність трьох основних теоретичних підходів до політичного насилля, при цьому представники кожного з них зосереджують свою увагу на різних аспектах соціальної системи. Дослідники першого напряму шукають детермінанти насильства в соціальній структурі. Науковці, що репрезентують другий підхід, - розглядають культурні зразки та норми, що діють у домінуючій культурі чи субкультурі, як значне джерело насильства. Третій напрям вказує на окремі чинники, як правило, суб'єктивні, пов'язані з емоціями. Ці відмінності є результатом використання різних методологій та парадигм, що існують у трьох групах детермінант політичного насильства, а також призводять до значних розбіжностей в його етичній оцінці. Розглянемо більш предметно особливості кожного з напрямів та ключові позиції їх представників.

Перший напрям – структурний - доводить, що джерела політичного насилля криються у недосконалій системі соціальних та політичних структур. Тут можна виділити три вектори. У межах першого, дослідники шукають детермінанти насильства у сфері відносин та владних структур. Другий вектор вказує на неправильні відносини та соціальні зв'язки між класами, прошарками та іншими соціальними елементами. Третій вектор шукає джерела політичного насилля в незадоволенні об'єктивних потреб певних соціальних груп: центральною пояснювальною категорією є нерівномірність розподілу економічних ресурсів. Дослідники, що працюють у межах структурних детермінант політичного насильства, часто вказують на те, що його джерела кореняться в певній соціально-політичній системі - системі

соціальних класів і прошарків, економічній системі та політичній ієрархії [42]. Дослідники, які шукають джерела політичного насильства в структурах влади, неодноразово вказували, що політична необхідність є головною детермінантою насильства. Політичні процеси провокують діяльність, пов'язану з насильством. Цю думку, серед інших, розвивав В. Парето. Він вірив, що еліта залишатиметься елітою лише в тому випадку, якщо: «… вони готові піти на крайність, вдаючись без будь-яких скрупулів - коли потрібно - до сили та зброї; інакше опір буде не лише ефективним, але може також послужити, іноді навіть значною мірою, опонентам» [74, с. 338].

На думку В. Парето, неправильно для тих, хто при владі, утримувати «і вовка порядку, і вівцю толерантності», оскільки завжди потрібно вибирати між цими двома цінностями. Подібну думку висловлює й американський неоконсервативний політичний аналітик Р. Каган. Він акцентує увагу на суттєвих відмінностях між практикою застосування насильства у міжнародних відносинах з боку Європейського Союзу та США. Причини застосування сили Сполученими Штатами та уникнення її країнами Європейського Союзу криються не лише в історичних обставинах цих утворень, не в конкретній ідеології, а в політичній прагматиці. Автор вважає, що застосування сили визначається лише можливістю її застосування, поточним військовим, політичним та ідеологічним потенціалом конкретного утворення [64, с. 11-16].

Аналогічний спосіб пояснення знаходимо в теорії мобілізації ресурсів [87; 88]. Основне припущення полягає у тому, що вся соціальна діяльність, включаючи насильство, зумовлена певним рівнем агрегації ресурсів. Резерви включають економічні, тимчасові, комунікаційні та людські ресурси, а також соціальний та культурний капітал членів та прихильників й легітимізуючий потенціал. При такому підході насильство розглядається як свідома і продумана реакція раціонального соціального суб'єкта. Якщо керівники зможуть накопичити ці ключові ресурси в достатній кількості, то застосування сили можливе і має шанси на успіх. Варто зазначити, що ця теорія значною мірою дискредитує психологічні чинники (почуття невдоволення,

незадоволення потреб) на користь матеріальних - здатності до мобілізації та організації ресурсів. Критики цього підходу припускають, що він створює помилковий образ надмірно раціональної, холоднорозрахункової, позбавленої емоцій особистості як актора політичної діяльності [37, с. 23-24].

У контексті політичного насилля підкреслюється роль функціонування державних структур у породженні або придушенні цього явища. Демократії - це системи, що генерують численні механізми запобігання насильству, включаючи періодичні вибори, поліцейські процедури, судові розгляди [65]. Той факт, що насильство проявляється, як правило, свідчить про серйозні вади демократичних процесів та структур. У той же час, це вказує на те, що високий рівень легітимності корелюється з низьким рівнем насильства [61]. Насильство, загалом, розглядається як форма протесту, спричинена блокованими каналами політичної участі. Якщо люди не можуть висловити свої потреби законними каналами політичної участі, вони повідомляють їх силою.

Надмірна відстань між державою та громадянами є одним з важливих чинників насильства. Це явище веде до патологічної політичної культури - створення так званої етики соціального зіткнення. Це постійна ситуація двостороннього взаємного блокування. Насильство також може бути «криком тих, хто втратив нормативні акти» - надмірна інституціоналізація та бюрократизація з боку держави може сприйматися як форма насильства і, зрештою, породжувати застосування сили її громадянами [75, с. 144 -145].

Визначальним фактором політичного насильства є система соціальних відносин між класами, верствами та іншими соціальними групами. Роздуми на цю тему можна знайти у К. Маркса, К. Зіммеля та Р. Дарендорфа. Л. Козер підкреслював, що відхилення розподіляються нерівномірно в соціальній структурі, насильство, як правило, здійснюється людьми, які впали на габермасівські «млини маргіналізації» [47, с. 55]. Етнічна приналежність, класова позиція та професійний статус є факторами, що визначають застосування насильства [47, с. 57]. У результаті урбанізації та індустріалізації

люди втрачають свої зв'язки з соціальними групами та суспільством в цілому, вони відчуджуються і, отже, сприйнятливі до ідеологій, що спонукають до застосування насильства.

Я. Блушковський пов'язує використання насильства з процесами глобалізації та невдачею або неадекватністю політичних та соціальних інститутів стосовно очікувань, прагнень та потреб окремих людей та груп, а отже, і явищем інституційного негативного відхилення [40]. Несумісність між потребами та очікуваннями окремих людей та груп, перекриття каналів спілкування між правителями та громадянами можуть фактично призвести до порушення правил соціального життя, включаючи застосування сили. Таку точку зору чітко висловив С. Чарновський, за яким поява достатньої кількості осіб, позбавлених класу, без встановленого соціального статусу, сприймається як непотрібна з точки зору матеріального та інтелектуального виробництва, і вважати себе такими, є достатнім для виникнення насильства. Насилля запускається й спричинюється обуренням цих надлишкових людей [48].

Американський політолог Т. Скокпол розширює цей спосіб мислення стосовно колективного революційного насильства. Вона вважає, що політичне насильство визначається існуючим класовим поділом, особливо коли соціальна структура неефективна [82]. Однак, дані емпіричних досліджень явища насильства, проведених в останні десятиліття XX століття, підірвали цю точку зору. Саме люди та групи, пов'язані міцними соціальними зв'язками на різних рівнях (дружні зв'язки, членство в різних організаціях), найбільш схильні до застосування сили [37].

Другий напрям – культурологічний - розглядає феномен насилля крізь культурну призму, зосереджуючись на фіксованих зразках дій, що існують у спільноті та випливають із санкціонованих цінностей, переконань та поглядів, набутих у процесі соціалізації. Насильство може визначатися культурними чинниками: існуючою та позитивно санкціонованою вірою в те, що воно є ефективним способом досягнення соціальних та політичних цілей у певному суспільстві [58]. Загалом, дослідники акцентують увагу на одному з трьох

факторів, які потенційно можуть породжувати насильство: мікросоціальні фактори (різновид соціалізації окремих людей та груп за використання насильства), макросоціальні фактори (соціально-історичні та навіть антропологічні детермінанти насильства) або фактори, що підсилюють наслідки контакту між різними культурами (вивчення явища насильства з точки зору культурного шоку, зіткнення цивілізацій тощо).

У межах мікросоціального виміру причини насильства пов'язані з дефектною соціалізацією в сім'ї: розбита родина, неорганізована сім'я, неврівноважене сімейне життя, відсутність інтересу з боку родини (підтримка, любов, прийняття), схильність до домашнього насильства, зневажливе ставлення або надмірно суворі батьки, неадекватне або надмірно суворе покарання, жорстоке суперництво між братами та сестрами з сильним почуттям ревнощів, сексуальне насильство з боку батьків, релігійні чи культурні норми вдома, що призводять до неправильного вкорінення моральних норм, заборон, правил.

Неправильна соціалізація в малих соціальних групах також може бути важливим чинником насильства: допустимий вплив субкультури насильства, ідентифікація або лояльність до винуватців насильства, захоплення бандитами та шахраями, рання та тривала госпіталізація, засвоєння моделей насильства з засобів масової інформації без виникнення осудливих чи суперечливих міркувань, жорстоке поводження з боку правоохоронних органів [57]. Це пояснюється концепцією авторитарної особистості Т. Адорно. Основа авторитарної особистості, для якої одним із проявів поведінки є авторитарна агресія, лежить у специфічному стилі соціалізації, заснованому на консервативних методах виховання - серед них - дефіцит у виконанні емоційних потреб, жорстке, незаслужене або недоречне покарання [34].

Культурні чинники насильства досліджуються у новітніх концепціях, що стосуються пошуку ідентичності, соціального конструктивізму чи соціально-конструктивістської перспективи. До представників соціального конструктивізму відносять А. Кукла [68] та Д. Ельдер-Васса [51]. Цей

науковий підхід зосереджено на культурних чинниках, зокрема релігійних, а також на явищі побудови колективної ідентичності для дій, що виконуються групами людей. Колективна ідентичність вважається ключовим елементом, оскільки вона розглядається як розширена особиста ідентичність. Вона формується на основі спільних дій, при цьому домінуючими є емоційні зв'язки.

Багато дослідників вказують на макросоціальні чинники насильства в межах культурологічного підходу - конкретні моделі або цінності, які санкціонуються домінуючою культурою та стимулюють людей до насильницьких дій. Науковий акцент робиться на численних відмінностях між суспільствами у масштабах, стилі, частоті та інтенсивності використовуваного в них насильства. У межах цього напряму підкреслюється, що насильство визначається унікальним історичним досвідом певної культури. Наприклад, у США суспільні науки, серед іншого, використовують «теорію кордону» та «теорію зброї» при дослідженні походження американської держави. Союз був захищений завдяки насильству, завдяки насильству були відібрані території у корінних народів, завдяки насильству конфлікт у суспільстві раннього капіталізму був придушений, відтак, насилля пронизує історію та відносини країни [79].

Деякі дослідники вважають, що культурні детермінанти насильства закладені не в одному періоді чи історичній події, а в усій культурній системі. Таку гіпотезу сформулював Е. Дюркгейм у своїх ранніх роботах. Він вважав, що війна характерна для не до кінця сформованих соціальних утворень - аграрних, домодерністських суспільств, але з розвитком людства системи соціального контролю стають все сильнішими, а війни дедалі рідшими [50].

У зв'язку з цим роздуми Е. Фромма, викладені в «Анатомії людської деструктивності», можуть зіграти роль синтетичного керівництва. Мислитель звертає увагу на багатовимірність проблеми насильства серед людей та вказує на два її основні джерела - біологічне та культурне [55]. Е. Фромм використав вторинні джерела для аналізу тридцяти первісних культур у контексті

застосування ними насильства. Він виділив наступні три типи культур: суспільства, що стверджують життя; агресивні недеструктивні суспільства; та деструктивні суспільства. Основною цінністю життєстверджуючих культур є збереження та розвиток життя у всіх його формах. Ворожість і насильство в таких суспільствах присутні мінімально. Жорстоких покарань немає, рівень злочинності низький, а війна ведеться за дуже рідкісних обставин або невідома. Зазвичай, це культура вседозволеності, відносної рівності. Такі товариства є колективістськими. Вони можуть включати як відносно заможні, так і бідні суспільства. У недеструктивних агресивних суспільствах насильство, війна, ієрархія та індивідуалізм є нормою. Це культурні системи, спрямовані на змагання, виконання завдань, постановку викликів. Взаємне насильство та жорстокість є характерними рисами руйнівного суспільства. Вони проявляються як усередині племені, так і поза ним. Життя засноване на ворожості, напрузі та страху. Існує сильна конкуренція, орієнтація на приватну власність, сувора ієрархія, помітні тенденції до войовничих дій. На думку Е. Фромма, відмінності між цими культурами настільки значні і важливі, що неможливо пояснити їх за допомогою біології, особливостей, загальних для всього людства. І раціональне, і нераціональне насильство можуть бути включені в побудову певної культури.

Важливою сферою досліджень в сучасних соціальних науках є пошук культурних чинників насильства, протиставлених різним культурним програмам. Цей спосіб міркування присутній і в політичній науці, в межах досліджень міжнародних відносин. З цієї точки зору, насильство розглядається як явище, породжене культурою, навіть форма насильства визначається культурою. Наприклад, конкістадори мали перевагу над ацтеками, оскільки перші прагнули ліквідувати ворога під час битви, а другі - взяти їх у рабство, що було результатом різних культурних моделей раціональності.

С. Малешевич називає цей підхід культурологічною перспективою, а О. Шпенглера та Дж. Тойнбі згадує як його першопрохідців [72].

С. Хантінгтон, який опублікував свої думки на цю тему в широко обговорюваній книзі «Зіткнення цивілізацій», є сучасним представником цього підходу. Геополітична концепція автора, сформульована в першій половині дев'яностих років XX століття, стверджує, що у разі зникнення біполярної моделі міжнародних відносин політичні та ідеологічні поділи, а також економічна нерівність перестають бути важливим джерелом конфліктів і, зрештою, насилля [62].

Підхід, який визнає культурні чинники найважливішими, продовжується у моделі етнічної конкуренції, створеній у сімдесятих роках XX століття та розширеній протягом наступних двох десятиліть. Ця модель пояснює, що культурні, етнічні поділи є необхідною умовою, але недостатніми для існування колективного насильства, тому вона також включає численні структурні детермінанти.

Третій концептуальний підхід до розуміння політичного насилля – соціально-психологічний – акцентує увагу на індивідуальних особливостях психологічного (емоційного) сприйняття соціальних подій, ролей, структур тощо. Цей напрям намагається пояснити причини насильства з точки зору окремої людини. Дослідники аналізують, чому одні особи беруть участь у діяльності, пов'язаній з насильством, а інші - ні. Пошук джерел насильства фокусується на емоційних факторах, афективних мотивах та суб'єктивних внутрішніх переживаннях особистості. Це індивідуалістична перспектива, яка стосується суб'єктивних детермінант і часто супроводжується песимістичним антропологічним сприйняттям людини. Окремий наголос робиться на генетичному чиннику людського насильства. Дослідники цього підходу дуже часто спираються на філософські джерела, зокрема напрацювання Т. Гоббса.

Наша неповноцінна людська природа є джерелом насильства, тоді як культура і соціальна структура є охоронцями порядку. Вони створені для стримування злочинних схильностей людей. Хоча сьогодні підкреслюється, що такий спосіб мислення робить людей одновимірними, що це надмірне і

неприйнятне спрощення, все ще існує тенденція пояснювати явище насильства в цих категоріях.

Спочатку науковці, які досліджували детермінанти насильства на основі особистості, сприймали це явище як соціально безглузде, патологічне, ознаку божевілля особистості [35]. «Безглуздість» насильства можна зрозуміти трьома способами. По-перше, можна розглядати насильство як ірраціональне в тому сенсі, що це явище було спричинене випадковими факторами, нещасним випадком; по-друге, «безглуздими» можуть позначатись дії ірраціонально мислячих людей (божевільних, під впливом психотропних речовин, підданих сильному стресу тощо); по-третє, як вчинок, здійснений без моральних роздумів, без урахування наслідків. Віра в ірраціональність насильства полягає у глибокій, усталеній, популярній, щоденній вірі в цю тему.

Прихильників цієї інтерпретації можна знайти, зокрема, в психоаналітичних теоріях. На нераціональність діяльності, пов’язаної з насильством, вказував З. Фройд [54]. Відповідно до психоаналітичної концепції, схильність людини до насильства сильно корелює з її травматичним досвідом раннього дитинства, зокрема сексуальними травмами, що є найважливішим. Також не існує раціонального пояснення колективного насильства через психоаналіз, коли натовп діє як дитина чи примітивна єдність.

Деякі послідовники З. Фройда зробили ряд цікавих теоретичних спроб, аналізуючи явище насильства. Наприклад, Л. Фейєр розглядав це питання в контексті Едіпового комплексу, піддаючи дослідженню конкретні прояви насильства [53]. Прихильники психоаналітичної концепції заявляли, що такі дії сприймаються тими, хто бере участь у них, більш виразними, ніж інструментальними, як емоційні, неорганізовані та позбавлені правил. Як результат, вони відмовились включати їх до політичних категорій, оскільки вони мали на меті не досягнення колективних благ, а індивідуальне задоволення у формі зняття емоційної напруги.

Робиться спроба визнати та класифікувати окремі чинники насильства на основі психології. Таку спробу зробив, зокрема, Р. Хартогс, склавши перелік дванадцяти психологічних факторів, що обумовлюють насильство: імпульсивність, емоційна нестабільність, неправильний психо-статевий розвиток, труднощі в інтерпретації соціального світу, нездатність або труднощі в адаптації до нових умов, необхідність негайного задоволення, гіперчутливість [59]. Окрім психологічних станів, він також перераховує органічні стани, включаючи короткочасні фактори (алкоголізм та наркоманія), довготривалі фактори (надмірна секреція залоз внутрішньої секреції, схильність до поєднання сексу та агресії, стійкий нічний енурез, нервово-м'язова збудливість), а також постійні фактори (пошкодження мозку, особливо скроневої або тім'яної областей, такі дисфункції як епілепсія, особливо психомоторна епілепсія, фізична інвалідність або страх перед хворобою, спадкова схильність до насильства). Відповідно, насильство виникає внаслідок порушеного через різні чинники сприйняття соціального світу і не повинно проявлятися здоровими людьми.

У даному контексті принагідно згадати теорію безглуздого насильства, відому в науці під назвою «теорія збитків». Ця точка зору на чинники насильства є не лише сферою психології, а й соціології, в межах якої було розроблено підхід, який називають «ірраціональним» (популяризований відомими соціологами з Чиказького університету). Ним започаткували традицію досліджень колективної поведінки. Учені сприймали заворушення, заколоти та інші насильницькі дії як неінституційні форми колективної поведінки. Такі події є ознакою краху соціальних норм і вираженням порушення стандартів нормальної соціальної поведінки. Дослідники зазначають, що історичною умовою концепції ірраціональності насильства був ряд травматичних історичних переживань у Європі - починаючи з Французької революції та Світових воєн - і явища політичного тероризму. Досвід потрясінь, збурень, невловимості соціального порядку призвів до визнання діяльності, пов'язаної з насильством, нераціональною.

На початку 1970-х розпочалась критика цієї концепції, що зросла на основі політичних подій, які мали місце в той час у США (рух за громадянські права та антивоєнний рух проти війни у В'єтнамі в США), а також соціальні зміни, що відбувалися у всьому світі. Дослідники відмовлялись аналізувати рухи, що прагнуть визволення, застосовуючи помірне насильство, як безглузді, нелогічні, марні, що є результатом внутрішніх егоїстичних мотивів учасників. Цей новий спосіб пояснення явищ став відомий як теорія мобілізації ресурсів (увага переважно на структурні міркування). М. Крол вказує на небезпечні наслідки такого мислення щодо явища насильства, припускаючи, що людська ірраціональність призводить до елітарної течії в політичній філософії [67]. Якщо люди за своєю природою ірраціональні, тоді вони не здатні приймати правильні політичні рішення, і тому більш освічені правителі повинні нав'язувати їх силою.

У той же час, в межах цієї тенденції є підхід, який розглядає насильство як раціональний вибір особи, прийнятий на основі розрахунку потенційних прибутків і збитків. Пояснення явища насильства здійснюється з точки зору економічної раціональності, це інструментальний, утилітарний підхід. Передбачається, що застосування насильства є дуже дорогим, оскільки воно тягне за собою цілий ряд негативних санкцій і застосовується лише в тому випадку, коли можливі вигоди можуть бути вищими за будь-яку потенційну втрату, або коли ймовірність отримання призу набагато вища за покарання. Отже, така дія є свідомою, продуманою і, як правило, служить певним інтересам. Цей підхід походить від ідей Ш.-Л. де Монтеск'є та А. Сміта, згодом він також розроблявся на основі марксизму та неомарксизму, тоді як у сучасному дискурсі ця точка зору присутня в теорії раціонального вибору. Перспектива раціонального вибору не присвячена поясненню насильства в суспільстві, але може служити цій меті, а також використовуватись для вивчення інших соціальних явищ.

Найбільшою популярністю серед раціональних соціально-психологічних пояснень в даний час користується підхід, який називається «депривація-

фрустрація-агресія», або «фрустрація та відносна депривація», або, ще коротше, - теорія фрустрації-агресії. Ця перспектива розвивалася в межах теорії конфліктів. Основна передумова цієї концепції полягає в тому, що так зване почуття відносної депривації може сформуватися в психіці особистості на основі спостереження за навколишнім середовищем та порівняння з іншими індивідами та соціальними групами (якщо результат порівняння відповідно до якогось соціального аспекту є негативним, людина вирішує, що він чи вона оцінюється гірше, ніж ті, з ким іде порівняння, або якщо результат такого порівняння позитивний - людина виявляє, що її соціальне становище вигідніше, ніж у подібних). Відчуття відносної депривації - враження відносного, суб'єктивного (а можливо, і взагалі неіснуючого) дефіциту - є головним фактором пояснення використання насильницьких дій. Ключовими соціальними цінностями в процесі порівняння особистості з соціальним середовищем, переважно, є: економічне процвітання, влада та міжособистісні стосунки.

Цей напрям почав розроблятися наприкінці 1930-х психологом Дж. Доллардом та його однодумцями. Власне концепція відносної депривації вперше з'явилася в працях С. Стоуффера, американського соціолога та одного з піонерів кількісних методів дослідження. С. Стоуффер та його колеги випробували понад півмільйона американських солдатів під час Другої світової війни і на основі цих досліджень сформулювали тезу про механізм порівняння особи та її соціального оточення [83]. Концепція відносної депривації в рамках досліджень щодо насильства була розроблена Т. Гурром в 1970 році. Вона все ще актуальна і в процесі розробки.

Т. Гурр стверджує, що якийсь елемент раціональності можна знайти в кожному політичному чи соціальному явищі. Він підкреслює, що люди раціонально перевіряють прибуток і збитки, і їх мотивують більше конкретні цілі. Дія із застосуванням насильства в кожному випадку складається з наступних трьох фаз: почуття невдоволення, «політизація невдоволення» та початок насильницьких дій [58]. Відносна депривація є головним чинником,

що визначає невдоволення. Воно розуміється як сприймане протиріччя між очікуваннями індивідів та фактичним втіленням цих очікувань у ході соціальних процесів, в яких особистість бере участь. Дослідник вважає, що цей вид депривації є для людини елементарним стимулом до дії. Він підкреслює, що подібні висновки робляться на основі теорії конфліктів: чим вища незадоволеність - тим вища інтенсивність насильства. Поява нових стилів життя, ідеологій та референтних груп - все це суб'єктивні чинники відносної депривації.

Однак, поняття відносної депривації піддається критиці. Акцент робиться головним чином на тому, що воно не було належним чином підтверджене емпіричними дослідженнями, оскільки наданий для аналізу матеріал обмежений прикладами в часовому та географічному відношенні - заворушення в США в шістдесятих роках XX століття [37]. Однак, новіші дослідження показують, що поява насильства також залежить й від інших чинників, а не тільки від суб'єктивного відчуття дефіциту [56]. Попри наявну критику ця концепція все ще має багато прихильників та захисників. Д. Сноу та П. Олівер заявляють, що процес емпіричного тестування цієї концепції був дефектним і, отже, призвів до спотворених результатів. Вони пропонують інший метод вимірювань, більш адекватний цій концепції, заснований на чинниках обізнаності [46].

Дослідники соціально-психологічних чинників політичного насильства частіше використовують нові методи дослідження, похідні з медичної науки, і поєднують їх з експериментальними методами. Ці нові методи включають електричне тестування мозкової активності (електроенцефалографія), вимірювання магнітної активності мозку (магнітоенцефалографія), а також вивчення процесів метаболічних змін мозку за допомогою позитронно-емісійної томографії або функціональної магнітно-резонансної томографії. Результати цих досліджень свідчать про те, що поведінка людей зумовлена нестачею свідомості в процесах, що відбуваються на нервовому рівні. З точки зору онтології, такий погляд називається епіфеноменалізмом: почуття та

думки є лише вторинними явищами фізичного та хімічного стану мозку, а не реальними автономними процесами [49].

Політичне насилля – соціальний феномен з глибоким історичним корінням, невід'ємна складова соціально-політичної боротьби за владу, вплив, авторитет та реалізацію конкретних інтересів певних осіб, груп, організацій тощо. Політична царина від моменту своєї появи не цуралася цієї методики досягнення політичних цілей та реалізації політичних завдань, особлива роль відводилася політичному насиллю в недемократичних політичних режимах, де терор був головним інструментом втілення політичних амбіцій державних керманичів. Державна влада, що керується страхом окремого громадянина та населення загалом, іде найпримітивнішим, але безпрограшним шляхом, адже законодавчо закріплена за такою державою монополія на політичне насилля, зв'язує руки громадянам і розв'язує державним тиранам.

Однак, політичне насилля можливе не лише за тоталітаризму, і його суб'єктами можуть бути не лише держава та її офіційні представники. За авторитарного політичного режиму, який відрізняється від тоталітарного лише частковою лібералізацією економічної сфери, політична воля повноцінно належить державі, відповідно, й засоби політичного насилля є її інструментами впливу на соціум. Інакше виглядає ситуація за демократії. Тут політичний плюралізм проявляється наявністю різних гравців часом із суперечливими інтересами і більш завуальованими (латентними) формами політичного насилля. Отже, за тоталітаризму та авторитаризму провідним суб'єктом політичного насилля постає держава, а за демократичного – ним може бути будь-який політичний актор (політик, політична партія, громадська організація, орган державної влади, група інтересів тощо) за однієї умови – достатності ресурсів (людських, фінансових, часових, технологічних і т. д.).

«Політичне насилля є невід'ємною складовою механізму здійснення влади. Незалежно від режиму, типу політичної системи, історичних або політико-культурних умов, насилля завжди використовувалося для здійснення панування, реалізації волі суб'єкта владарювання. Незважаючи на значний

прогрес у впровадженні демократії, втіленні принципів правової держави, прав та свобод людини у сучасних розвинутих країнах, політичне насилля залишається одним із головних владних ресурсів» [4, с. 172-173].

Політичне насилля може мати два ключові вектори – фізичний та психологічний. За тоталітарного та авторитарного політичних режимів держава не гребує обома. Фізичне насилля може реалізовуватися низкою засобів, таких як побиття, тортури, обмеження пересування, утримання під вартою, знищення тощо. Психологічне насилля має свій інструментарій: приниження, контроль, погрози, ігнорування, шантаж тощо. За демократичного ладу більшість політичних акторів обмежені психологічними засобами, й переважно, спираються на маніпулятивні техніки впливу на свідомість та підсвідомість. Але в будь-якому випадку, психологічне насилля призводить до виникнення в людини відчуття незахищеності, емоційної невпевненості, що зрештою відбивається на загальному психічному здоров'ї особи і може призвести до незворотних наслідків.

«Українська дослідниця А. Г. Боброва поділяє політичне насилля на два основні типи – традиційне і нетрадиційне. У традиційному політичному насиллі використовується фізичний примус. До нього авторка відносить тероризм та локальні етнічні війни. Нетрадиційне насилля представлене символічним насиллям, інформаційними, психологічними та консцієнтальними війнами. Таке насилля реалізується без застосування фізичного примусу. Натомість його засобами є маніпуляції, залякування, вплив на ірраціональні складові людської психіки» [5, с. 175].

Політичне насилля в інформаційній сфері належить до психологічного виміру. Його особливістю за тоталітаризму та авторитаризму є суб'єкт-об'єктна форма реалізації, в якій суб'єкт, представлений державою, чинить вплив на об'єкт, суспільство, за допомогою різних каналів донесення інформації (телебачення, радіо, преса, листівки, брошури, кіно, театр, література тощо) нав'язує соціуму певну систему ціннісних координат, ідеологічних установок, культурних пріоритетів, чим позбавляє людину

унікальності позиції і, по суті, знищує її індивідуальність, та зрощує масову керовану свідомість. Найбільш дієвий засіб політичного насилля в інформаційній сфері недемократичних держав – пропаганда.

За демократії політичне насилля в інформаційній сфері стає мультисуб'єктним в силу того, що з'являються незалежні від держави ЗМІ та інші автономні соціокультурні авторитети, які або відстоюючи власні інтереси, або ж працюючи на певного замовника, стають учасниками суб'єкт-об'єктного впливу (соціально-політичний актор – цільова аудиторія) чи суб'єкт-суб'єктного протистояння, яке з часом може перерости у інформаційну війну.

Нового імпульсу політичному насиллю в інформаційній сфері надав бурхливий розвиток інформаційно-комунікаційних технологій й спричинене останнім формування інформаційного суспільства. Насамперед, це стосується демократичних спільнот, адже вони повномірно відкрилися для ІКТ, в результаті чого змогли як скористатися їхніми перевагами, так і відчути наслідки недоліків. Тоталітарні й авторитарні режими або ж повністю відкинули можливість популяризації ІКТ, або використовують окремі їх здобутки під жорстким наглядом з боку держави (КНДР, КНР, Куба).

«Сучасний розвиток інформаційних технологій призвів до збільшення інтенсивності застосування латентних форм прояву політичного насилля, до яких належать інформаційно-психологічні війни та операції. Головна відмінність латентного політичного насилля полягає в тому, що воно діє на людей, минаючи свідомість, через це особа позбавляється можливості приймати зважені, логічно обґрунтовані рішення, і отже втрачає свободу волі» [17, с. 172].

Однак, не все насильство в інформаційному полі можна вважати політичним. До останнього можна віднести лише заходи, коли політичні цілі досягаються інформаційним інструментарієм. У більш широкому сенсі доречно говорити про інформаційне насильство. Розкриємо зміст цього поняття.

О. Василевич стверджує, що «інформаційне насильство в широкому значенні – це інформаційний вплив на людину, що призводить до втрати, деформації, обмеження, або неможливості здійснення таких людських якостей, які становлять особистість людини, тобто свідомість і самосвідомість, свобода вибору, індивідуальність, система цінностей, світогляд, система потреб, інтересів та установок. Або, що було б трохи точніше, інформаційне насильство — це наступні здійснювані ЗМК впливи: маніпулювання особистістю за допомогою інформації про різні сфери соціального життя; масовизація, спрямована на стандартизацію всіх можливих аспектів особистісної життєдіяльності; духовна наркотизація, проведена шляхом тотального введення в комунікативний напрям масової культури; відчуження свідомості окремої особистості й особистостей одна від одної, тобто впливу ЗМК, що мають на меті духовно придушити особистість, зруйнувавши, деформувавши або знищивши в зародку сутнісні її складові» [6]

Авторський колектив на чолі з О. Дзобань розглядає інформаційне насильство у широкому та вузькому вимірах. «Інформаційне насильство в широкому сенсі, що припускає існування інформації в будь-яких соціальних системах, — це не силовий впорядкований вплив на об’єкти, що мають антисоціальний або антиособовий характер. Інформаційне насильство у вузькому сенсі — несиловий вплив (дія) на ментальну сферу, що суперечить закономірному перебігу подій» [12, с. 147].

Учені виокремлюють такі властивості інформаційного насильства:

- несиловий (нематеріальний і неенергетичний), ідеальний характер, непідпорядкування фізичним закономірностям (не має маси, ваги, розміру, температури плавлення);
- нелінійність, тобто непропорційна залежність причини й наслідків;
- порушення закону збереження речовини й енергії, кумулятивний характер, можливість зростання інформації як сніжної грудки;
- можливість максимальної дальності та швидкості поширення, яка збільшується з розвитком технічних та технологічних досягнень, хоча межа

швидкості інформаційного насильства теж кінцева – швидкість світла у вакуумі;

- можливість ідеального клонування, оскільки ідеальні копії можна зробити однаковими, вони можуть бути незмінними, замороженими, а матеріальні предмети постійно змінюються, старіють;

- нелокалізованість у часі, оскільки будь-яка матеріальна дія здійснюється в конкретний час, наприклад вбивство, а в інформаційного насильства може бути наслідок – розмитість у часі і просторі (вбивство конкретної людини відбувається в конкретному місці, а інформаційний вплив може бути розмитим, дифузним);

- пандемія (епідемія, що має глобальний характер);

- опосередкований характер і скритність впливу (хоча деякі форми фізичного впливу теж непомітні, наприклад отрута, інформаційна дія може бути абсолютно непомітною);

- віртуальний характер дії; можливість фокусування; селективність; уразливість, крихкість інформаційного світу, легкість доступу, злому інформаційних систем [12, с. 146-147].

З'ясовуючи зміст феномену «інформаційне насильство», слід акцентувати увагу на таких аспектах [12, с. 139]:

По-перше, все більш актуальним стає не захист інформації, а захист від інформації. У цій ситуації змінюється навіть традиційне уявлення про знакові системи. Зокрема, величезний потік інформації перекладає її з дискретного рівня на континуальний, можлива навіть інформація без жодного змісту. Водночас втрачається можливість верифікувати цю інформацію, визначити де правда, а де брехня. Відбуваються зміни в мові як основі комунікації, а це, у свою чергу, породжує глобальні трансформації в суспільстві.

По-друге, інформаційне насильство певним чином переплелося з терором. Феномен тероризму охопив буквально всю планету [21];

По-третє, серед багатоманітних проявів масової комунікації особливе місце посідають ефекти, пов'язані із зображенням насильства в програмах

телебачення та мережі Internet. Ця проблема впродовж останніх десятиліть була й залишається предметом численних досліджень і дискусій [20].

По-четверте, актуалізується проблема маніпуляцією свідомістю. Маніпуляція – це перш за все частина технології влади, що замінила в інформаційному столітті такі види влади, як насильство і примушення.

По-п’яте, доступність інформаційних ресурсів для пересічного користувача частіше сприяє його присиплянню, наркотизації, аніж активності [12, с. 144].

По-шосте, зміст інформаційного насильства багато в чому визначається формами контролю за наслідками впливу засобів масової інформації [9, с. 28].

Учені О. Дзьобань та В. Пилипчук зазначають, що у сучасному суспільстві склалася система державного і приватного інформаційного насильства. Засоби масової інформації нав’язують вигідні їм та їх реальним власникам оцінки, думки, електоральну поведінку. Інформаційним насильством є прославляння культу сили і гангстеризму, вестернізація або, навпаки, заповнення вульгарною вітчизняною естрадою екранів телебачення і кінематографу. Насильство входить у мову, семантику передач, повсякденні комунікації [13, с. 6].

Ефективність застосування інформаційних технологій для вирішення певних політичних, економічних, соціальних чи фінансових проблем, крім іншого, пояснюється тим, що «практично будь-яке сучасне соціальне утворення будь-якої масштабності (чи то локально-територіальні соціуми, чи спільноти загальнодержавного масштабу, чи наднаціонального) потенційно готове і сприйнятливе до того, щоб стати об’єктом маніпулятивного впливу. Такою є сучасна цивілізаційна реальність: більша частина людей планети готові до маніпуляцій ними. Ніхто в світі не може почуватися у безпеці від маніпуляції, хіба що поодинокі суспільства, які культивують моральність і високу раціональну культуру, спроможні на тимчасовий спротив» [14, с. 194].

На думку автора, подібні маніпуляційні дії у тій чи іншій формі використовують уряди всіх держав світу під час роботи з комунікаційним

простором. Результатом такої роботи є формулювання так званих «стратегічних наративів», інструментарій яких іноді може використовувати інформаційне насильство. Очевидним є наступна пропорція: чим потужніша в економічному та технологічному плані держава, тим більш витончені стратегічні наративи вона має.

У цьому відношенні український вчений Г. Почепцов виокремлює декілька базових рівнів роботи з комунікативним простором або з простором будь-якої комунікації – це організаціясимволічної, візуальної, подієвої, міфологічної та, власне, комунікативної складових просторукомунікації [26, с. 11]. Зокрема, він підкреслює, що будь-який інформаційно-політичний вплив створює (провокує) конфлікт, який в подальшому буде вирішуватися у вигідному для комунікатора руслі. Головна мета – це інформаційне домінування, яке б не давало можливості захопити ініціативу опоненту/ противнику [26, с. 63]. Для цього комунікатор організовує та підтримує ситуацію інформаційної асиметрії з метою встановлення реальної та керованої переваги в комунікації [26, с. 32-33].

Ініціатор конфлікту, зазвичай має гандикап: «маніпулятор, який бере на себе роль генератора стратегічних програм, займає найвигіднішу позицію в комунікативному просторі, і шанси на привласнення такої ролі зростають там, де сегментація інформаційного поля-простору вища» [22, с. 205].

Інший український учений С. Демченко виявляє подібну ситуацію у вітчизняному інформаційному просторі. На його думку, національний інформаційний простір набуває «мозаїчного», фрагментарного характеру, він «розмежований» та розподілений між медіахолдингами фінансово-промислових угруповань, які завдяки їх фінансуванню та підтримці «анексують» певні інформаційні зони. У результаті корпоративні, егоцентричні устремління окремих олігархічних груп чи політичних сил видаються за суспільно значущі та необхідні всьому соціуму [11]. Дані прояви є яскравим прикладом інформаційного насильства, що повноцінно використовує інструментарій маніпулятивного впливу. Інформація у таких

випадках висвітлюється під «правильним» кутом, насаджується своя інтерпретація реальності, яка взагалі може не відповідати дійсності.

Аналіз проблематики інформаційного насильства змушує громадянське суспільство активно реагувати на виклики сучасності, удосконалюючи існуючі та створюючи нові методики подолання або хоча би мінімізації наслідків інформаційного насильства в умовах сучасних інформаційних протистоянь.

Отже, політичне насилля в інформаційній сфері є одним із видів інформаційного насилля, одним із інструментів якого постає інформаційна війна. Відповідно, не кожна інформаційна війна є засобом саме політичного насилля. Серед досліджених нами у попередньому підрозділі форм інформаційної війни найбільше завданням політичного насилля відповідає психологічна. Більше того, не лише інформаційна війна може бути інструментом політичного насильства в інформаційному просторі, його технологічний арсенал значно ширший (інформаційна експансія, інформаційна атака, інформаційна операція тощо). Деталізуємо можливі засоби політичного насилля в інформаційній царині.

О. Саприкін вважає, що «терміном «інформаційна експансія» позначають систему, що склалася в засобах інформації розвинених держав, і методи, використані для пропагандистського забезпечення певних геополітичних цілей. Інформаційну експансію можуть створювати і поширювати як державні органи (за допомогою державних і приватних інформаційних установ і заходів), так і транснаціональні корпорації для досягнення власної вигоди…» [29].

В. Панченко пропонує «визначити інформаційні операції як сплановані заходи, спрямовані на суспільно-політичну комунікацію суспільства з метою

схилення до ухвалення управлінських рішень та/або вчинення дій в інтересах суб’єкта впливу» [23].

Інформаційна атака - це попередньо сплановане, цілеспрямоване поширення дезінформації про супротивника. «Від інформаційної експансії її відрізняє локальність мети і часу здійснення» [29].

Зазначимо, що взаємозв'язок цих заходів, а також інформаційної війни як одного з засобів політичного насилля, можна пояснити за принципом піраміди, де кожна попередня ланка може бути задіяна окремо або виступати структурним елементом наступної. Інформаційна атака може бути разовим самостійним заходом або ж у серії інформаційних атак формувати інформаційну операцію, остання, в свою чергу, також може бути одиничною або ж частиною інформаційної війни, яка також може бути окремим інструментом чи структурним проявом інформаційної експансії.

Варто наголосити, що сьогодні перед демократичними суспільствами стоїть низка проблем прикладного характеру, вирішення яких може мінімізувати використання політичного насилля в інформаційній сфері: розширення публічного простору; підвищення рівня політичної освіти та культури громадян; контроль громадянського суспільства над інформаційною політикою держави; використання інструментів прямої демократії при прийнятті політичних рішень; заохочення політичної участі громадян; децентралізація політичної влади; удосконалення нормативно-правової бази, що регулює інформаційну царину тощо.

1.2 Наукова рефлексія поняття та феномена інформаційної війни

Кожна нова віха суспільного розвитку привносить елементи модернізації у способи виробництва, соціальної комунікації та взаємодії, розв'язання політичних конфліктів, ведення військових операцій тощо. Перехід від аграрного до індустріального суспільства, який відбувся більше ніж двісті років тому, став імпульсом для розвитку суспільного потенціалу як в економічній, так і соціально-політичній царинах за рахунок промислових новацій. Становлення ж інформаційного суспільства, спираючись на цифрові

та комунікаційні зрушення, призвело до чергової видозміни усіх без винятку галузей суспільної життєдіяльності. Світ ущільнився, прискорився, став більш відкритим, доступним та уніфікованим.

Інформаційне суспільство створило умови «для вдосконалення устрою держави, розвитку демократії; оптимального використання місцевих умов і ресурсів; економії природних ресурсів та захисту навколишнього середовища; розвитку сфери послуг і освіти; значного підвищення ефективності виробництва; переходу до сталого розвитку; розвитку середнього класу, який є основним суспільним прошарком і найбільш мобільним у всіх передових країнах; оперативного доступу до потрібної інформації для наукових досліджень, освіти, культури, високотехнологічних та наукоємних виробництв, складних видів послуг і вільного поширення інформації; можливості зберігання великих обсягів інформації на зовнішніх носіях – формування зовнішньої системної пам'яті; появи нових форм діяльності з використанням інформаційних мереж» [8, с. 100] тощо.

Разом із тим, інформаційне суспільство відкрило можливість для посилення інформаційної складової військових активностей, по суті, створивши новий вид війни – інформаційної, яка з 90-тих років XX століття стала, з одного боку, одним із найбільш уживаних засобів політичної боротьби, а з іншого – найбільш аналізованим предметом наукових розвідок.

Враховуючи той факт, що політика – це сфера управління усіма суспільними процесами, а держава є єдиним джерелом легітимного насилля, явище інформаційної війни важко помислити за межами політичного. Будь-яка війна, у тому числі інформаційна, переважно носить політичний характер, адже має за мету або ж завоювання, утримання, зміцнення політичної влади, або ж нав'язування політичної волі суб'єктами об'єктам публічного управління.

Інформація завжди була дієвим елементом політичної боротьби (агітація, пропаганда, дезінформація тощо). Але сьогодні інформаційні операції вийшли на новий рівень і можуть нести системну загрозу, приміром, електронним

системам державної інфраструктури, збройних сил, енергетичної царини, національній безпеці загалом і т. д. Сьогодні кіберпростір офіційно занесений до переліку областей, в яких може вестись війна. Він займає п’яте місце після суходолу, моря, повітря та космосу, тому що здатність контролювати, порушувати чи маніпулювати інформаційною інфраструктурою супротивника стала настільки ж визначальною, як перевага зброї у визначенні результату конфліктів. При дослідженні інформаційної війни стрижневим є поняття інформації. Адже інформаційна природа такого роду протистояння проявляється у тому, що інформація є або ціллю, або джерелом або середовищем для досягнення поставленої мети.

Інформаційна війна - один із найпереконливіших виявів переходу суспільства на якісно новий щабель. Вона доводить, що сьогодні існує нове середовище, де фізична та нефізична реальності співіснують і є однаково цінними, і в якому держави повинні довести свій авторитет, для чого спеціально розробляються нові режими ведення війни. Перехід до нефізичного домену створює ґрунт для поперечності інформаційної війни. Цей непростий аспект легше зрозуміти, коли інформаційна війна порівнюється з традиційними формами ведення війни. Традиційно війна тягне за собою застосування насильства держави через державні збройні сили для визначення умов управління визначеною територією. Це обов’язково насильницьке явище, яке передбачає людські жертви та шкоду як військовій, так і цивільній інфраструктурам. Тут держава стикається з проблемою, як мінімізувати збитки та втрати, забезпечуючи перемогу над супротивником.

Інформаційна війна відрізняється від традиційних бойових дій у кількох аспектах, головним чином тим, що вона не обов’язково насильницьке та руйнівне явище. Наприклад, в інформаційній війні може використовуватися комп’ютерний вірус, здатний порушити або заборонити доступ до бази даних супротивника, і тим самим це може завдати серйозної шкоди супернику без фізичних проявів сили чи насильства. Окрім цього, інформаційна війна не

обов’язково залучає людей. У цьому сенсі може використовуватися автономний штучний агент.

«Використання методів інформаційної війни набуває різних форм, і всі вони переносяться через протести за повалення чи істотне ослаблення політичних, економічних та соціальних умов чинної влади. Це інформаційна війна та інформаційно-військові компоненти, які використовуються для так званих «кольорових» революцій» [81, с. 137].

«Інформаційна війна все частіше перераховується поряд із ядерною, хімічною та біологічною зброєю як потенційна зброя масового знищення або, принаймні, як зброя масових зривів» [52, с. 57].

Сьогодні конкурентами в веденні інформаційної війни можуть бути, злочинці, нефункціональний або незадоволений персонал, постачальники, хакери, спецслужби, іноземні та внутрішні уряди, медіа-клієнти та групи тиску. Як зрозуміло з вище наведеного переліку, не завжди суб’єкти інформаційної боротьби є представниками політики, але їхні дії з необхідністю впливають на соціально-політичні процеси у країні або низці держав, і таким чином, набувають політичного змісту.

«Інструменти» інформаційної доби, що включають швидкість і точність, вже стали частиною поля бою. Тільки найвищої якості солдати, керівники, штаби та організації, які розуміють важливість швидкості та точності в обробці інформації та її застосування зможуть досягти успіху в таких умовах» [85, с. 15].

Одна з ключових проблем ведення інформаційної війни пов’язана з розробкою шляхів боротьби з потенціалом швидких радикальних інновацій, з якими стикається публічна політика в умовах інформаційного суспільства. Домен безпеки, можливо, є однією з найбільш постраждалих областей, оскільки «конкуренти» стикаються один з одним безпосередньо, а не на ринку з більш-менш інертною клієнтською базою, і політична влада сама є «конкурентом», а не лише установником правил або замовником.

Державна політика має ініціативну сторону, будуючи інфраструктуру в широкому розумінні цього слова, а також реакційну сторону. У сучасному контексті інфраструктура має включати такі пункти, як стандартизація, законодавство, міжнародні режими, регуляторні агенції та структури для попередження, оповіщення та реагування на загрози. Інноваційний потенціал інформаційного суспільства вимагає розбудови інфраструктури, здатної управляти широким спектром потенційних майбутніх подій, переважна більшість з яких ніколи не здійсниться. Для цього потрібно широко використовувати сценарії та інші якісні методології передбачення. Крім того, цілеспрямоване реагування на кризу проти інноваційного супротивника вимагає, щоб знання, створені в сценарних вправах та прогнозах можливих концепцій нападу, були доступними і корисним для аналітиків.

Інформаційна війна в інформаційну епоху пов’язана з контролем над інформаційною сферою, що передбачає формування та спрямування інформаційних потоків на тактичному, оперативному та стратегічному рівнях в часи миру, напруженості та війни. По суті, це контроль над джерелами та розповсюдженням інформації. Контроль сприйняття реципієнтами в інформаційній сфері означає, що інформація повинна бути створена в інтересах домінуючої сили. Ця інформація може представляти або не представляти фізичну реальність. Іншими словами, інформація, яка надає перевагу домінуючій стороні, може бути підмножиною реальності або, власне, штучною реальністю. У обох виявах вона пов’язана з обманом, маніпуляціями, навіюванням.

Суттєві наукові дослідження інформаційної війни проведені такими фахівцями, як О. Бойченко, Н. Волковський, О. Дубас, А. Кампен, М. Кіца, М. Лойд, Д. Міллер, Г. Почепцов, А. Сірик, В. Ткач, Е. Тофлер тощо. Завдяки теоретичним напрацюванням цих науковців розкрито багато дослідницьких аспектів, зокрема – зв’язок ЗМІ та інформаційної війни, її глобальні прояви, понятійно-категоріальний контекст формування дефініції, практичні кейси ведення інформаційної війни, її сучасні інструменти тощо. У той же час, у

науково-дослідній площині бракує напрацювань, які б розкривали одночасно як сутність феномену, так і поняття інформаційної війни.

Відповідно, мета цього підрозділу полягає у розкритті змісту поняття, що використовується у наукових розвідках, системному дослідженні витоків та генези інформаційної війни як явища соціально-політичної дійсності, а також виявленні її провідних форм.

За визначенням інформаційна війна - це використання та захист інформації. Тут виникає питання: що таке «інформація»? І закономірно постає потреба у тлумаченні взаємозв'язку цього поняття, а також термінів «дані» та «знання». Використовуючи лінійний підхід можна стверджувати, що «дані» описують атрибути речей, «інформація» - це зіставлені дані в контексті, а «знання» - це інформація, яку людина інтерпретувала з огляду на досвід.

У трактуванні М. Буазо «дані» асоціюються з річчю і розрізняють різні стани речі, яку вони описують. Вони складаються з атрибутів подій або об'єктів, які вони описують. З іншого боку, «знання» є атрибутом людини. Знання – це набір взаємодіючих думок про дані, активовані подією. А інформація, у свою чергу, - набір відфільтрованих людиною даних в межах знань, якими володіє ця людина або група людей, вона встановлює зв'язок між пізнанням та даними [41].

Ю. Бабенко розглядає інформаційну війну як сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій, або служб інформаційної інфраструктури загалом, або окремих її елементів [2].

Г. Почепцов стверджує, що інформаційна війна – це будь-які дії, спрямовані на нейтралізацію противника або опонента в інформаційному просторі [25].

А. Фісун визначає інформаційну війну як «комплексний відкритий чи прихований цілеспрямований інформаційний вплив однієї сторони, чи взаємний вплив сторін одна на іншу, який охоплює систему методів та засобів впливу на людей, їхню психіку та поведінку, інформаційні ресурси та

інформаційні системи з метою досягнення інформаційної переваги в забезпеченні національної стратегії, здатної сприяти прийняттю сприятливих для ініціатора рішень або паралізувати інформаційну інфраструктуру супротивника з одночасним зміцненням і захистом власної інформації та інформаційних систем» [32, с. 46].

Інформаційна війна - це цілеспрямовані зусилля зі зниження та нейтралізації систем командування та контролю противника з метою захисту та координації діяльності систем командування та контролю дружніх сил [39].

Інформаційна війна може включати:

- збір тактичної інформації;
- перевірку точності інформації;
- поширення пропаганди та дезінформації з метою деморалізації або маніпулювання опонентом та громадськістю;
- підривання якості інформації про опонента;
- позбавлення опонента можливості збирати інформацію [76].

Попри авторські акценти на різних аспектах інформаційної війни, більш загальний чи конкретний підхід до визначення її поняття, з вище наведених дефініцій стає зрозумілим, що інформаційна війна – це завжди протистояння у інформаційному полі, яке може впливати на людей та системи, мати захисну чи атакуючу логіку.

Витоки феномену інформаційної війни можна пов’язати з кінцем 1980-тих років, коли у західному світі вираз був специфічним для військової сфери. Його вжиток, насамперед, асоціюється з війною у Перській затоці 1991 року. Першопочатково під інформаційною війною розумілася електронна війна, військовий обман, психологічні операції та інформаційно-експлуатаційна безпека. Однак, найважливішим елементом її еволюції став розвиток електронних обчислювальних технологій та комунікаційних технологій. У 1990-тих роках роль цих технологій, на думку А Кампена, була доведена війною у Перській затоці 1991 року [43]. Інформація, а точніше, інформаційні технології дали перевагу у бойовій розвідці, таргетингу, командуванні та

контролі. Однак, у той час акцент все ще робився на технологічній, а не інформаційній стороні. Тим не менш, інший компонент активно розвивався у ході цієї війни - управління ЗМІ.

Починаючи з війни у В'єтнамі, військові докладали багато зусиль розвитку своєї тактики. Війна у В'єтнамі стала переломним етапом у відносинах між ЗМІ та військовими (по суті, урядом). Звітність щодо перебігу цієї війни була, переважно, відкритою для журналістів [71]. Однак, навіть у цьому конфлікті офіційні брифінги в пресі демонстрували жорстко контрольований інформаційний потік. У той же час, розвиток вертолітного транспорту та військових кооперативів дав журналістам можливість неконтрольовано виходити на операції. Телетрансляції з місця подій, які могли побачити по телевізору усі американці були досить впливовими. У подальшій дискусії військові неодноразово звинувачували журналістів у зловживанні такою свободою пересування. Крім того, військові звинувачували знакові образи, які символізували втрату «домашнього фронту», а згодом - і війни [45].

На той момент військові та уряд не усвідомлювали весь потенціал телебачення та його здатність впливати на громадську думку. Подальші тактики використання засобів масової інформації з пропагандистською метою, якими почали користуватися західні держави, суттєво змінились. У США розвиток цієї тактики мав навіть загрожувати життєздатності Першої поправки до Конституції [44].

Фолклендська війна 1982 року створила прецедент для поширення офіційних випусків інформації стосовно інших конфліктів того десятиліття, такі як вторгнення в Гренаду та Панаму. Фолклендська війна відбувалася в географічно ізольованій місцевості з дуже обмеженою комунікацією. Таким чином, усі прес-релізи контролювались та повідомлялися урядом. Журналісти проходили перевірку, і всі їхні репортажі піддавалися військовій цензурі [84]. Це був класичний випадок маніпулювання даними, представленими населенню. Сполучені Штати навчилися з цього досвіду і суттєво стримували журналістів протягом вторгнення до Панами. До цього додалося

маніпулювання контекстом подій. Були влаштовані паради перемоги, телетрансляції яких демонстрували панамців, що святкують американську участь. У той же час, насправді корінні жителі розглядали ці події як вторгнення. Однак, важливим було сформоване у громадськості уявлення про те, що військова операція не тільки була успішною, а й віталася всіма сторонами. Країна звільнена від гніту – це було ключове повідомлення.

Війна в Перській затоці показала рівень витонченості в управлінні інформацією з боку військових і уряду, який повинен був вплинути на спосіб поводження урядів Заходу з уявленнями громадськості протягом наступного десятиліття. Поява прес «пулів» і «затверджених» журналістів переважно означала, що ЗМІ повідомлятимуть лише ті дані, які їм надали урядові чи військові чиновники. Незалежних журналістів тримали подалі і насправді до них ставились як до потенційних ворогів. ЗМІ у відповідь гарантували, що буде представлена лише урядова версія подій [66].

У середині 1990-тих років інформаційна війна під впливом бурхливого розвитку в галузі комп'ютерної та комунікаційної технологій переросла в інтегровану доктрину. Це все ще була технологія зосереджена на домінуючих командах та контролі й окремому керуванні медіа. Однак, технологічні інновації почали сприяти їх злиттю. Стало очевидним, що сучасні війни були також медіа війнами. Проте, інформаційна війна все ще мала військовий характер і вважалося, що вона має відношення лише до воєнного часу.

У одному з наукових текстів того періоду йдеться про те, що інформаційна війна - це поєднання командної та контрольної війни, інтелектуальна війна, економічна війна, кібер-війна та хакерська війна. Ці умови були чітко визначені і свідчили про те, що інформаційна війна стосується використання технологій з допомоги командуванню, контролю та збору розвідувальних даних, і одночасно перешкоджання аналогічним процесам на стороні супротивника. Включення економічної війни є аномалією, хоча в той час було багато дискусій щодо цієї загрози безпеці Америки [69].

У той же час в окремих сферах публічної дипломатії та державних справ відбувалися кардинальні зміни. Західні уряди змінювали відносини зі своєю громадськістю. Незважаючи на те, що в історії і раніше траплялася неправдиві факти, з'явилася нова порода фахівців з громадських зав'язків, які покладалися на можливості сучасних комунікацій для агресивного використання інформації як переваги. Інформація стала елементом, який слід створювати за бажанням, і контрольовано розповсюджувати. Мистецтво вибору відповідної інформації, корисної для підбурювача, що призводило до хибного інформування, було цинічно замінено використанням дезінформації - навмисним використання оманливої інформації. Цей тонкий перехід від викривлення до навмисної брехні змінив характер урядово-військово-медіа-публічного інтерфейсу.

Ця зміна стосунків спочатку пройшла непомітно. Обман не вважався важливим фактором громадсько-державних контактів на Заході. Це вважалося більш характерним для тоталітарних режимів. Наприклад, у Радянському Союзі фактично були відсутні розмежування військових та дипломатичних граней уряду. Обман був функцією держави і не обмежувався лише військовими. Вчення про обман стало відоме як «маскування» («приховування», «камуфляж»). Загалом, радянська концепція маскування включала обман, дезінформацію, секретність, фінти, диверсії, наслідування, приховування, імітацію та безпеку [80], хоча не обмежувалася лише ними. Переважно, вона стосувалася будь-чого, здатного заплутати і, таким чином, послабити ворога [70].

За радянських часів поняття обману не отримувало моральної зневаги, як це було на Заході. Однак, на межі XX-XXI століть західні уряди почали розглядати потенціал обману як тактику, якщо не стратегію. Відповідно, роль маніпулювання інформацією для переваги вийшла на перший план. Саме доступ та використання інформації стали основними чинниками переваги. Практика обману почала розумітися як природне продовження сприйняття інформації, як домінуючий елемент у конкурентній перевазі. Якщо інформація

має значення при прийнятті рішень, тоді її контроль та маніпуляції також мають бути важливими.

У XXI столітті «медійні війни» стали справжнім інтегрованим процесом. Уряди та пов’язані з ними військові групи удосконалили методи впливу на громадськість. Методики зв’язків з громадськістю, розроблені в 1920-тих роках, були вдосконалені експоненцією зростання знань. Теорія соціальної психології та емпіричні дослідження об’єднувались із психологічною війною та методами публічної дипломатії. Це поєднання за допомогою вдосконалених медіа-технологій та методик, а також монополістичних медіа-компаній мали розвитися в ситуацію, коли засоби масової інформації повинні були стати невід’ємною частиною військових зусиль.

Терористичні атаки на Нью-Йорк, Вашингтон та Пенсильванію 11 вересня 2001 року серйозно позначилися на «об'єктивності» звітності ЗМІ. Зараз журналісти в США вважають себе частиною національної команди, а не «сторонніми людьми», які неупереджено передають інформацію. Наслідки зміни ставлення журналістів до їхньої ролі стали зрозумілими в наступні роки. Так, приміром, друга війна з Іраком у 2003 році продемонструвала реальність справжньої інформаційної війни та важливість ЗМІ у ній.

Коментар Ж. Бодріяра з приводу того, що перша війна в Перській затоці «не відбулася» [38] також є актуальним і для другої війни в Іраку 2003 року. Філософ не мав на увазі, що війна фізично не відбулася, а те, що війна, про яку знала громадськість, була ілюзією, створеною бойовою машиною. ЗМІ в обох війнах стали войовничим складом там, де військово-розважальний комплекс створив контент з власною напругою, драмою та хвилюванням. В обох війнах було використано те, що окремі експерти називають «сексуальністю» зброї [33]: візуальні видовищні вибухи ракет на горизонті. Однак, ЗМІ зрідка демонстрували руйнівні наслідки цих вибухів, тіла мертвих та скалічених або ж зруйновані будівлі.

Сьогодні можна виділити три класи медіа-ефектів:

- порядок денний - здатність засобів масової інформації визначати важливі проблеми дня;

- ґрунтування - взаємозв’язок між моделями висвітлення новин та критеріями, за допомогою яких громадськість оцінює політиків;

- обрамлення - зв’язок між якісними особливостями новин та громадською думкою [63].

Автори цієї класифікації стверджують, що різкі зміни в суспільній думці визначаються обсягами висвітлення новин щодо певних політичних питань. Це висвітлення буде диктувати рівень важливості, який громадськість надає цим питанням - це встановлення порядку денного. ЗМІ також мають можливість впливати на те, як сприймають політиків - це обрамлення. Ґрунтування має тенденцію бути важливішим для оцінки ефективності та мати менший вплив на оцінки особистості. Таким чином, порядок денний, сприйняття та взаємозв’язок між подіями можна контролювати. Люди можуть сприймати лише отримані дані.

У наш час інформація та комунікація повністю контролюються на масовому рівні. Вплив інформаційної війни (особливо психологічних операцій та компонентів обману) є першорядним. У певному сенсі сприйняття стало важливішим за реальність. Обман набув глобального, постмодерністського виміру, в якому реальність конструюється, а масова свідомість зазнає щоденних маніпулятивних впливів.

У доступній на сьогодні дослідній літературі, присвяченій інформаційній війні, представлено кілька поглядів на форми її прояву. Найбільш поширеними є думки таких видатних експертів, як В. Швартау та М. Лібіцкі. Загалом, форма інформаційної війни - це спосіб її розгортання, вона виражається через структуру подій та заходів, пов'язаних з процесами, що в ній відбуваються. Це означає, що форма інформаційної війни - це особливість, яка якісно відрізняє її від інших.

В. Швартау класифікує інформаційну війну за трьома групами:

1) персональна інформаційна війна;

2) корпоративна інформаційна війна;

3) глобальна інформаційна війна [78].

Перший клас включає атаки проти приватного життя. Сюди входить розкриття інформації, що зберігається у невизначеній базі даних. На даний час ми не маємо ніякого контролю над власними даними, що зберігаються повсюдно, такими як історія кредитних карток, банківські рахунки, медичні справи, судимість тощо. Сотні баз даних містять цифрове зображення нашого життя. При цьому, наявна інформація не є обов'язково точною, а виправити помилкову інформацію практично неможливо.

Другий клас інформаційних війн відповідає конкуренції між компаніями, які стикаються на війні без жалю. Промислове шпигунство є одним із можливих видів діяльності, але дезінформація є дуже ефективним засобом позбавлення від конкурента. У даний момент дуже просто розповсюдити чутки щодо світового асортименту, використовуючи Інтернет. Більше того, загальновідомо, що чим більше факт суперечливий, тим більше громадська думка йому вірить.

Глобальна інформаційна війна є класом конфлікту, спрямованого на галузі промисловості, на цілі економічні сили, на всю країну. Завдяки значно меншим інвестиціям у порівнянні витратами на «традиційну» зброю, терористична група чи країна можуть поставити на коліна велику економічну державу. Перевага для зловмисника, якщо він належить до категорії країн, що розвиваються, полягає в тому, що він не буде настільки чутливим до репресій подібного характеру. Більше того, для розвиненої демократичної країни буде дуже важко відповісти на такий напад збройними репресіями, не завдаючи шкоди громадській думці.

М. Лібіцькі виокремлює наступні форми інформаційної війни:

1) війна у сфері командування та контролю;

2) розвідувальна війна;

3) радіоелектронна війна;

4) психологічна війна;

5) хакерська війна;

6) економічно-інформаційна війна;

7) кібервійна [69].

Усі ці форми пов’язані, особливо хакерська війна та кібервійна не є повністю диз’юнктивними. Деталізуємо кожну з вище зазначених форм, розкривши їх специфіку.

Міністерство оборони США пропонує таке офіційне визначення війни у сфері командування і контролю – “…це військова стратегія, яка застосовує інформаційну війну на полі бою з метою відокремити командну структуру опонентів від підрозділів, якими вона керує” [69].

Знешкодження можна зробити, відрізавши командування або перекривши зв'язок, залежно від різних тактичних і стратегічних цілей. М. Лібіцькі вважає, що це набагато важливіше, ніж пошук фізичного розташування командира. Атаки командних позицій, особливо якщо цей процес своєчасно коригується, можуть мати виняткові операційні наслідки, і для цього не потрібно, щоб суперник був "обезголовлений". У більшості ситуацій командний пункт – це вузол всієї структури суперника і можливість його усунення зрідка пропускається. Він може бути знищений класичними бомбами, але також і псуванням джерел живлення, за рахунок електромагнітних перешкод, комп’ютерних вірусів, переривання комунікацій тощо. "Пошкодження дверей" означає переривання комунікацій з боку противника, що робить командування і контроль недієздатними, і зрештою має вирішальний вплив на кінцевий результат конфлікту.

Війна у сфері командування і контролю може вестися наступально та оборонно. Виходячи з вищесказаного, можна зробити висновок, що метою цієї форми інформаційної війни є погіршення або знищення потенціалу супротивників з командування та контролю, й одночасно захист власного потенціалу від такої діяльності.

Розвідувальна війна - це діяльність, спрямована на пошук цілей, оцінку бойових дії, запобігання несподіванкам тощо. Первинні джерела розвідки

можуть бути класифіковані на різні категорії (людська, сигнальна, технічна тощо).

У Брюсселі, 23 лютого 2000 року, Європейський Парламент розпочав дебати про планетарну шпигунську мережу під назвою "Ешелон". Мережа зі 120 супутників охоплює всю планету і створює систему, здатну контролювати 2 мільярди повідомлень щодня завдяки штучному інтелекту та ключовим словам. Отже, супутникова шпигунська система має справу зі збором та аналізом різноманітних (політичних, безпекових, економічних, технологічних, торгових та ін.) даних. Єдиний центр управління у Глостері (Велика Британія) нараховує 15 000 працівників, які беруть участь в аналізі зібраних даних.

Електронна війна - це така форма інформаційної війни, в якій використовуються електронні та інші засоби безпосереднього впливу на електронні пристрої та системи супротивника, а також бойові системи та зброю на основі використання ними електроніки. Електронна війна також може бути визначена як військова діяльність, яка передбачає використання електромагнітної та цільової енергії з точки зору домінування та управління подіями в електромагнітному спектрі та з точки зору електронної атаки на супротивника та його бойові системи. К. Шлехер розуміє електронну війну як військову акцію, спрямовану на контроль над електромагнітним спектром [77]. Отже, електронна війна - це сукупність військових дій, основною метою яких є контроль над електромагнітним простором, його доменом.

Для досягнення заявленої мети можуть провадитися дії, що мають наступальний характер (електронна атака) та захисний характер (електронний захист). Крім того, може надаватися електронна підтримка - діяльність, спрямована на збір інформації для потреб електронної атаки чи електронного захисту, уникаючи дій супротивників, використовуючи власні бойові ресурси.

Електронна атака - це частина радіоелектронної війни, пов’язана з використанням електромагнітної енергії або цільової енергії для атаки, щоб деградувати, нейтралізувати або знищити бойовий потенціал супротивників. У ході електронної атаки можуть використовуватися як м’які (електронне

глушення), так і жорсткі засоби (самонаводні ракети на електромагнітній радіації).

Електронний захист є частиною електронної війни, яка охоплює діяльність, спрямовану на захист власного народу та засобів від наслідків радіоелектронної боротьби супротивника, а також від ненавмисних викидів, що генеруються власними передавачами, які можуть погіршити, нейтралізувати або знищити бойовий потенціал власних сил.

Електронна підтримка є частиною електронної війни, яка включає діяльність з розкриття, ідентифікації та розташування джерел навмисного або ненавмисного випромінювання електромагнітної енергії для виявлення дій опонентів, виявлення розташування цілей, планування та здійснення підтримки для радіоелектронної боротьби та інших тактичних заходів. Інформація про супротивника, зібрана за допомогою електронної війни, має значний розвідувальний вимір, відповідно, у такому сенсі електронна війна може розглядатися як розвідувальна війна. Однак, остання радше є функцією планування і ведення електронної війни і, зокрема, формування електронної картини поля бою. Тому співвідношення між електронною та розвідувальною війнами найкраще описує термін координація, яка характерна також для деяких інших форм інформаційної війни.

Психологічна війна передбачає використання інформації проти людського розуму [86]. Психологічні операції мають на меті передавати вибрану інформацію та показники, призначені для іноземних слухачів та глядачів, щоб впливати на їх емоції, мотиви та об'єктивні міркування і, зрештою, поведінку іноземних урядів, організацій, груп та осіб для досягнення власних інтересів та цілей. Головна мета психологічної операції із захисту власної системи командування та контролю полягає в мінімізації наслідків пропаганди та діяльності опонента з метою знезараження власних сил та населення. На думку американського філософа та політолога кінця XX – початку XXI століття, Н. Хомського, метод провадження психологічної війни відіграє важливу роль і зачіпає близько 20% населення, відносно освіченого,

яке бере участь у прийнятті певних рішень. Медійний вплив на цей відсоток людей та їх прийняття доктрини має вирішальне значення для політики. Решта 80% населення є лише спостерігачем подій, вони повинні виконувати замовлення, повідомлення та завдання і не втручатися до справ осіб, які приймають рішення. Ця частина населення є просто ціллю засобів масової інформації, якій не слід перевтомлюватися від того, що відбувається у світі [60].

Хакерська війна - одна з форм інформаційної війни, яка найчастіше виконується окремими особами. Зазвичай, хакерська атака спрямована на перевантаження та зміну вмісту веб-сайту, що атакується. Функціональні та фізичні характеристики комп’ютерних систем представляють ідеальну мішень для нападників. Для того, щоб перевірити стійкість своєї комп'ютерної мережі проти нападів хакерів, у 1994 році Агентство захисту інформаційних систем (DISA) протестувало та сформувало свою власну хакерську команду, наказавши атакувати комп'ютерні мережі Пентагону через Інтернет. Після завершення тестування офіційна позиція полягає в тому, що вони не готові захиститися від "електронної версії" Перл Харбору, відповідно, комп'ютерна структура не є захищеною. Використання хакерської війни залежить значною мірою від кількості використовуваних комп'ютерів та кількості користувачів Інтернету. Ступінь інтеграції комп’ютерних мереж є обернено пропорційною наслідкам хакерської війни. У сучасних конфліктах хакерські війни особливо успішні проти технологічно слабких країн.

Термін "економічно-інформаційна війна" досі не визначений повністю, але очевидно, що ця форма інформаційної війни керується інформацією, що має економічне значення для конфліктуючих сторін. Інформацією, що має економічне значення, може бути інформація про різні контракти, стратегію розвитку компанії, внутрішню структуру та організацію, маркетингові та виробничі плани, інвестиції тощо. Очевидно, що у глобальному контексті конфлікт економічних та розвідувальних служб є постійно присутнім навколо конфіденційної інформації, яка може бути використана проти своїх

конкурентів в інтересах своїх компаній. Цей конфлікт по суті є економічним (або промисловим) шпигунством.

Колишній директор ЦРУ Дж. Тенет зазначив, що економіка була основною сферою розвідувальних робіт у 1990-тих роках. Іноземне шпигунство і через стільки років після закінчення "холодної війни" залишається основною загрозою національним інтересам Росії, заявив тодішній глава Федеральної служби безпеки (ФСБ) Росії М. Ковальов.

Відомо, що шпигунські атаки на IBM (International Business Machines), які здійснили близько двадцяти людей, які працювали в японській Hitachi, призвели до викрадення конфіденційної інформацію на суму від 750 мільйонів до 2,5 мільярдів доларів протягом трьох років. Операція була припинена в 1982 році завдяки ФБР. У 1997 році General Motors втратила 100 мільйонів доларів лише тому, що був розроблений транспортний засіб на основі викрадених даних [73].

Проаналізувавши всі методи та прийоми (легальні та нелегальні) економічної та інформаційної війни на світовому ринку, особливо через те, що більшість країн не мають технологічно оснащених та ефективних систем економічної розвідки, з'явилася ідея створення спеціальних відомств, які можуть забезпечити такі фахові послуги у цій сфері. Робота агентства може бути атакуючою (допомога у просуванні певної компанії чи держави на світовому ринку за рахунок розкриття конфіденційної економічної інформації про певний ринок або його сегмент та конкуруючі компанії або усуненні конкурента з гри різними методами) чи оборонною (захист країні чи компанії від крадіжки виробничої та ділової таємниці, розкриття корупційних чи інших незаконних засобів, використовуваних конкурентом у певному бізнесі тощо).

Зростаюча залежність суспільства від інформаційно-комунікаційних технологій створює численні слабкі місця. Через ці критичні точки, а також через посилену складність та сильну взаємозалежність, національні інфраструктури, що з'єднують, запускають та обслуговують комп'ютери, стають надзвичайно чутливими. Зв'язок мережевих комунікацій збільшує їхню

вразливість через зростаючий доступ до інформаційної структури з різних частин світу. Кіберпростір - це сфера, яка надає нові можливості для ведення війни. Дж. Арквілла та Д. Ронфілд визначали кібервійну як низку дій, які підривають або руйнують інформаційно-комунікаційні системи супротивників [36].

Кібервійна може вестись як напад, так і як захист. Об’єктом кібератаки може бути все, що підключає, запускає та обслуговує комп’ютери (військові комп’ютерні системи, системи державного управління, системи управління повітряним та залізничним рухом, системи постачання газу, води та електроенергії тощо). З огляду на їх важливість, призначення та кількість, особливо в розвинених країнах Заходу, очевидно, що інформаційне середовище пропонує кібер-зловмисникам широкий вибір дуже значущих цілей.

Кібератаки є більш масштабними та досконалими, краще скоординованими, ніж хакерські атаки, і спрямовані на значні цілі ворога. Застосування кібервійни значною мірою залежить від кількості використовуваних комп’ютерів та кількості користувачів Інтернету. У збройному конфлікті комп'ютерні атаки можуть здійснювати лише члени збройних сил з ретельною оцінкою потенційного збитку об'єкту, що атакується.

Висновки до першого розділу

Поняття політичного насилля розкривається шляхом виявлення його категоріальної генези. У даному дослідженні логіка осягнення ключового поняття відбувається через розкриття змісту такої понятійної паралелі, як «політичний інтерес» - «політичний конфлікт» - «політичне насилля». Обов’язковою умовою комплексної рефлексії політичного насилля як наукового поняття є усвідомлення його видового статусу по відношенню до родової дефініції «насилля».

Феномен політичного насилля досліджується в численних наукових розвідках. Вивчення літератури, представленої у даному розділі, свідчить про наявність трьох провідних напрямів: структурного, культурологічного та соціально-психологічного. Відповідно, у випадку політичного насилля ми можемо говорити про варіативний детермінізм, оскільки політичне насильство індукується згортанням багатьох чинників. Визнання цього факту здається природним кроком у дослідженні цього соціально-політичного явища. Результати такої рефлексії мають не лише когнітивне, а й прогностичне значення.

Політичне насилля поряд з іншими різновидами (економічне, соціальне, фінансове тощо) може відбуватися в інформаційній площині і бути одним із виявів інформаційного насильства, яке збагатило свій інструментальний арсенал у контексті активного розвитку інформаційно-комунікаційних технологій. Серед провідних засобів можна виділити інформаційну атаку, інформаційну операцію, інформаційну війну та інформаційну експансію.

Інформаційна війна пов’язана з контролем над інформаційною сферою, що передбачає формування та спрямування інформаційних потоків на тактичному, оперативному та стратегічному рівнях, це контроль над джерелами та розповсюдженням інформації. Ведення інформаційної війни передбачає збір тактичної інформації; перевірку точності інформації; поширення пропаганди та дезінформації з метою деморалізації або маніпулювання опонентом та громадськістю; підривання якості інформації про опонента; позбавлення опонента можливості збирати інформацію тощо. Для досягнення політичних цілей переважно використовується психологічна форма інформаційної війни.

Список використаних джерел до першого розділу

1. Аверина О. Политический интерес как категория социальной философии. URL: http://cheloveknauka.com/politicheskiy-interes-kak-kategoriya-sotsialnoy-filosofii.

2. Бабенко Ю. Інформаційна війна зброя масового знищення! URL: http://www.pravda.com.ua/rus/articles/2006/04/20/4399050.

3. Бабієва А. Політичне насилля: теоретичний аспект. Політичний менеджмент. 2005. № 5, С. 161-168.

4. Балацька Б. Сутність та специфічні риси політичного насилля як засобу здійснення влади. Грані, 2015. № 5 (121). С. 172-178.

5. Балацька Б. Типологія політичного насилля як складової сучасного політичного процесу. Вісник маріупольського державного університету серія: Історія. Політологія, 2015. Вип. 13-14. С. 172-182.

6. Балацька О. Політичне насилля як політикокультурний феномен: специфіка, детермінація, тенденції : монографія. Старобільськ : ДЗ «ЛНУ імені Тараса Шевченка», 2018. 385 с.

7. Баровська А. В. Інформаційні виклики гібридної війни: контент, канали, механізми протидії, НІСД. Київ. 2016. 109 с.

8. Боброва А. Основні форми сучасного політичного насилля : автореф. дис. … канд. політ. наук : 23.00.01. Київ, 2005. 19 с.

9. Василевич О. Інформаційне насильство як соціальний феномен. URL: http://eprints.zu.edu.ua/2024/1/22.pdf.

10. Волгушева А. Политические интересы общества. URL: https://center-yf.ru/data/stat/politicheskie-interesy-obshchestva.php.

11. Галтунг Д. Культурное насилие. Социальные конфликты: экспертиза, прогнозирование, технологии разрешения. Москва, 1995. Вып. 8. С. 34–38.

12. Голубовська В. Інформаційне суспільство: можливості, проблеми та перспективи розвитку. URL: http://ippi.org.ua/sites/default/files/13gvsppr.pdf.

13. Гуменюк Л. Соціальна конфліктологія URL: https://pidruchniki.com/78442/psihologiya/sotsialna_konfliktologiya.

14. Гурковський, В., 2002. Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання. Вісник УАДУ: наук. журн. №3, с.27–32.

15. Гусейнов, АА., 2004. Возможно ли моральное обоснование насилия?'. [online] Доступно: https://guseinov.ru/publ/Mor_obosn_nasiliya.html

16. Демченко, СВ., 2011. Масова комунікація у процесі розбудови громадянського суспільства: історія, теорія, українські реалії: автореф. дис. д-ра наук із соц. комунікацій: 27.00.01, Київ. нац. ун-т ім. Т. Шевченка, Ін-т журналістики. Київ. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/suak/corp.exe?&I21DBN=SAUA&P21DBN=SAUA&S21STN=1&S21REF=10&S21FMT=elib_all&C21COM=S&S21CNR=20&S21P01=0&S21P02=0&S21P03=ID=&S21COLORTERMS=0&S21STR=0006003

17. Денисенко В. Ціннісні основи історичних форм буття людини. Вісник Львівського університету. Серія : Філософсько-політологічні студії. Львів : Вид-во ЛНУ ім. Івана Франка, 2011. Вип. 1. С. 75–86.

18. Дзьобань О., Панфілов О., Соболєва С. Інформаційне насильство: змістовний аспект. URL: https://cyberleninka.ru/article/n/informatsiyne-nasilstvo-zmistovniy-aspekt/viewer.

19. Дзьобань, О.П., Пилипчук, В.Г., 2011. Інформаційне насильство та безпека: світоглядно-правові аспекти: монографія. Харків, Майдан, с.244.

20. Додонов, Р.О., 2017. Гібридна війна: in verbo et in praxi: монографія. Вінниця: ТОВ «Нілан-ЛТД», 410 с.

21. Доценко, Е.Л., 1997. Психология манипуляции: феномены, механизмы и защита. [online] Доступно: http://libarch.nmu.org.ua/bitstream/handle/GenofondUA/44695/4fa42deac644be1fd4e5d610ddc1e8d3.pdf?sequence=1&isAllowed=y

22. Жданенко С. Б. Соціальна комунікація в умовах інформаційного суспільства. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія. 2016. № 1. С. 36-48.

23. Жекало Г. Природа та сутність політичного конфлікту. URL: file:///C:/Users/dell%2015z/Downloads/159-Article%20Text-266-1-10-20160929.pdf.

24. Жижек С. О насилии. Москва : Изд-во «Европа», 2010. 184 с.

25. Зубкова І. Напрямки попередження та зменшення проявів прямого та латентного політичного насилля в сучасних умовах. Молодий вчений, 2015. № 2 (17). С. 172-175.

26. Інформаційна безпека держави у воєнній сфері / Ю. Г. Даник, М. М. Биченок, В. О. Кацалап та ін. К.: НУОУ ім. І. Черняховського, 2019. 301 с.

27. Капустин Б. К понятию политического насилия. Полис. 2003. № 3. С. 104.

28. Кастельс М. Информационная эпоха: экономика, общество и культура / пер. с англ. М.: ГУ ВШЭ, 2000. 458 с.

29. Коврижных О. Сущность и типология политического насилия. Гуманитарный вектор. 2010. № 4 (24). С. 45–54.

30. Колесов П. Ведение Соединенными Штатами информационных войн. Концепция «Стратегических коммуникаций». Зарубежное военное обозрение. 2010. № 6. С. 9-14.

31. Комунікативні тренди міжнародних відносин: монографія / Є. А. Макаренко, М. М. Рижков, Н. О. Піпченко, Т. В. Москаленко, І. І. Погорська; Київ. нац. ун-т ім. Т. Шевченка. К.: Центр вільної преси, 2016. 614 с.

32. Кугай А. И. Природа политического насилия и его роль в современном мире: автореф. дис… канд. филос. наук. М., 1993. 22 с.

33. Кузина С.И. Политическое насилие: природа, манифестирование и динамика в глобализирующемся мире. Автореф. дис. ... докт. полит. наук: 23.00.02. Ростов-на-Дону, 2010.

34. Кухта П. В. Кризи, їх причини та наслідки. URL: http://www.economy.nayka.com.ua/?op=1&z=1439

35. Левченко Л. Політичне насилля як різновид тиску у владних структурах. Наук. пр. Чорноморського держ. ун-ту імені Петра Могили. Серія : Політологія. 2008. Т. 79. Вип. 66. С. 18–21.

36. Лиддел-Гарт, Б.Г., 1954. Стратегия непрямых действий. URL: http://militera.lib.ru/science/liddel_hart1/index.html

37. Магда С. М. Гібридна війна: сутність та структура феномену. Міжнародні відносини. Серія «Політичні науки». URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/2489

38. Макаренко, Є.А., 2006. Міжнародна інформаційна безпека: сучасні виклики та загрози. К.: Центр вільної преси, 916 с.

39. Маритен Ж. Человек и государство. М.: Идея-Пресс, 2000. 196 с.

40. Методика організації оцінювання суспільно-політичної обстановки в районах дислокації військ (сил) та під час виконання ними завдань за призначенням: навчальний посібник / В. Безбах, Є. Гарькавий, С. Мотика та ін.]; за заг. ред. В. Безбаха. К.: ВІКНУ імені Тараса Шевченка, 2019. 94 с.

41. Навчальний посібник з воєнно-ідеологічної підготовки особового складу Збройних Сил України на 2016 навчальний рік / за заг. ред. І. С. Руснака. К.: НДЦ ГП ЗС України, 2016. 240 с.

42. Наумова Н. М., Наумов В. О. Інформація як комунікація та мотивація діяльності в сучасному інформаційному суспільстві. Управління проектами, системний аналіз і логістика. Технічна серія. 2012. Вип. 10. С. 178-186.

43. Нечитайло, Д.А., 2008. Джихад в информационном пространстве (киберджихад). URL: http://rodon.org/polit-081210114341

44. Олещук П. Теоретичні засади аналізу політичних наративів як засобу дослідження політичного дискурсу. Віче. URL: http://veche.kiev.ua/journal/2014/

45. Панченко В. Інформаційні операції в системі стратегічних комунікацій. URL: http://ippi.org.ua/sites/default/files/panchenko.pdf

46. Петров В. В. Культурна дипломатія як інструмент протидії гібридним загрозам. Вісник Національної академії керівних кадрів культури і мистецтв. Культурологія. 2019. № 1. С. 186-190.

47. Пиджаков А. Сущность и разновидности политического насилия. Москва : ЭКСМО-ПРЕСС, 2008. 136 с.

48. Піпченко Н. Соціальні медіа у структурі зовнішньої політики провідних міжнародних акторів: монографія. К.: Центр вільної преси, 2014. 332 с.

49. Побочий І.А. Політична боротьба як форма взаємовідносин соціальних сил в умовах утвердження державності сучасної України [Текст]: автореф. дис. … д-ра політ. наук: спец. 23.00.02 / І.А. Побочий. – К., 2008. – 35 с.

50. Почепцов Г. Інформаційна війна як інтелектуальна війна. URL: http://osvita.mediasapiens.ua/material/1330.

51. Почепцов Г., 2012. Контроль над розумом. К.: Вид. дім «Києво-Могилянська академія», 352 с.

52. Примуш М. Політичні конфлікти та їх типи. URL: https://ipiend.gov.ua/wp-content/uploads/2018/08/prymush_politychni.pdf.

53. Радченко Л. Політичні інтереси: поняття, функції, типологія. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/64445/108-Radchenko.pdf?sequence=1.

54. Різун В. В. Теорія масової комунікації. К.: Видав. центр «Просвіта», 2008. 260 с.

55. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. URL: http://nbuv.gov.ua/UJRN/vkp_2013_1_13

56. Сірук М. Про три головні проблеми комунікацій. URL: https://day.kyiv.ua/uk/article/podrobyci/pro-try-golovni-problemy-komunikaciy

57. Старостенко С. Политические интересы в контексте политического многообразия в Российской Федерации. URL: https://cyberleninka.ru/article/n/politicheskie-interesy-v-kontekste-politicheskogo-mnogoobraziya-v-rossiyskoy-federatsii/viewer.

58. Тарасюк В. М. Політико-правові засади застосування інформаційних технологій в умовах гібридної війни: дис. ... кан. політ. н.: 23.00.02 / Національна академія наук України. К., 2018. 235 с.

59. Федірко І. П. Соціально-політичні конфлікти як об’єкт дослідження. Філософія. Політологія. 2005. № 73–75, С. 63-65.

60. Фісун А. Теоретично-категоріальне осмислення поняття «інформаційна війна» в структурі інформаційно-політичного простору. Інформаційне суспільство: науковий журнал. К., 2011. 60 с.

61. Хилько М. І. Сепаратизм: походження, сутність, різновиди. Гілея: науковий вісник. URL: http://nbuv.gov.ua/UJRN/gileya_2019_144%283%29__28

62. Черненко Т. В. Пріоритети державної інформаційної політики в умовах гібридної війни. Стратегічні пріоритети: науково-аналітичний щоквартальний збірник. К.: НІСД, 2013. № 4 (29). С. 83-92.

63. Шейгал Е. И. Многоликий наратив. Политическая лингвистика. 2007. Выпуск (2) 22. С. 86-93.

64. Adie K. Television Presentation. Press Club, Australian Broadcasting Corporation, 13.00hr, 22 December, 2004.

65. Adorno, Th. W., Frenkel-Brunswik, E., Levinson, D. J. and Sanford R. N., 1950. The Authoritarian Personality. Norton: NY.

66. Apter, D. E., 1997. The Legitimization of Violence. New York: New York University Press.

67. Arquilla, J. & Ronfeldt, D., 1995. Network war and cyberwar, a copy of the study publication in "Comparative Strategy". RAND Corporation. Volume 12.

68. Barkan, S. E. and Snowden, L.L., 2001. Collective Violence. Boston: Allyn & Bacon.

69. Baudrillard J. The Gulf War Did Not Take Place. Sydney, Power Publications, 1995.

70. Blair, B.G., 2001. Strategic Command and Control. Washington, D.C., The Brookings Institution.

71. Błuszkowski, J., 2007. Paradoksy polityki [Paradoxes of politics]. Warsaw: Elipsa.

72. Boisot M. Knowledge Assets. Oxford, Oxford University Press, 1998.

73. Burgoon, B., 2006. On welfare and terror: Social welfare policies and political economic roots of terrorism. Journal of Conflict Resolution, issue 50, pp.176-203.

74. Campen A. The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. Fairfax, VA, AFCEA International Press, 1992.

75. Carpenter T. The Captive Press: Foreign Policy Crises and the First Amendment. Washington, DC, Cato Institute, 1995.

76. Carruthers S. The Media at War. Houndsville, MacMillan Press, 2000.

77. Cook, K. S. and Fine, G. A., 1995. Social Perspectives on Social Psychology. Boston: House J. S., Allyn & Bacon.

78. Coser, L. A., 1967. Continuities in the Study of Social Conflict. New York: The Free Press.

79. Czarnowski, S., 1982. Wybór pism socjologicznych [Choose of sociological writings]. Warsaw: Książka i Wiedza.

80. Dopfer, K., 2004. The Economic Agent as Rule Maker and Rule User: Homo Sapiens Economicus. Journal of Evolutionary Economics, issue 14, pp. 177-195.

81. Durkheim, E., 1992. Professional Ethics and Civic Morals. London: Routledge & Kegan Paul.

82. Elder-Vass, D., 2012. The Reality of Social Construction. Cambridge: Cambridge University Press.

83. Eriksson A. Viewpoint: Information Warfare: Hype or Reality? URL: https://www.nonproliferation.org/wp-content/uploads/npr/eriksss63.pdf.

84. Feuer, L. S., 1969. The Conflict of Generations. New York: Basic Books

85. Freud, Z., 1967. Group Psychology and the Analysis of the Ego. New York: Liverwright Publishing.

86. Fromm, E., 1963. War Within Man: A Psychological Enquiry Into the Roots of Destructiveness; a Study and Commentary. Peace Literature Service of the American Friends Service Committee.

87. Goode, E., 1992. Collective Behavior. Fort Worth: Harcourt Brace Jovanovich.

88. Guerra, N. and Huesmann, L. R., 2004. Une theorie cognitivo-ecologique du comportement agressif. [A cognitive-ecological model of aggression.] Revue Internationale de Psychologie Sociale.

89. Gurr, T. R., 1970. Why Men Rebel. Princeton: Princeton University Press.

90. Hartogs, R. and Artzt, E., 1970. Violence. Causes and Solutions. New York: Dell Publishing.

91. Herman E., Chomsky N. Manufacturing Consent: The Political Economy of the Mass Media. New York: Pantheon, 2002, 412 p.

92. Hughes, B., 2004. Political Violence and Democracy: Do Societal Identity Threats Matter? The Security and Politics of Identity, [online] Available at: http://www.adelaide.edu.au/apsa/docs_papers/Others/Hughes.pdf [Accessed 16 November 2020].

93. Huntington, S. P., 2007. The Clash of Civilizations and the Remaking of World Order. New York: Simon and Schuster.

94. Iyengar S., Simon A. News Coverage of the Gulf Crisis and Public Opinion. In The media, public opinion, and U.S. foreign policy in the Gulf War Chicago, University of Chicago Press, 1994, Ch. 8, p.167 - 185.

95. Kagan, R., 2003. Potęga i Raj. Ameryka i Europa w nowym porządku świata [Of Paradise and Power: America and Europe in the New World Order]. Warsaw: Emka.

96. Keane, J., 2004. Violence and Democracy. Cambridge: Cambridge University Press.

97. Knightley P. The First Casualty. Baltimore, John Hopkins University Press, 2000.

98. Król, M., 2008. Filozofia polityczna [Political philosophy]. Kraków: Znak.

99. Kukla, A., 2000. Social Constructivism and the Philosophy of Science. London and New York: Routledge.

100. Libicki M. What is Information Warfare? Washington, National Defense University, 1995.

101. Lloyd M. The Art of Military Deception. London, Leo Cooper, 1997.

102. Louw E. The Media and the Political Process. London, SAGE Publications, 2005.

103. Malešević, S., 2010. The Sociology of War and Violence. New York: Cambridge University Press.

104. Munro, N., 1995. The Pentagon's New Nightmare: An Electronic Pearl Harbor. Washington Post.

105. Pareto, V., 1935. The Mind and Society. Harcourt: Brace.

106. Peyrefitte, A. ed., 1982. Społeczeństwo wobec przemocy. Raport Komitetu Badań nad Przemocą, Zbrodnią i Występkiem [Society towards violence. Report of the Committee for Research on Violence, Crime and Misdemeanors]. Warsaw: Państwowe Wydawnictwo Naukowe.

107. Reisman, W.M. & Antoniou, C.T., 1994. The Laws of War: A Comprehensive Collection of Primary Documents on International Laws Governing Armed Conflict. New York, Vintage Books (Random House).

108. Schleher, C., 1999. Electronic Warfare in the information age. Artech House.

109. Schwartau W. Information Warfare, Chaos on the Electronic Superhighway. Thunder's Mouth Press, 1994.

110. Sederberg, P. C., 1994. Fires Within. Political Violence and Revolutionary Change. New York: HarperCollins College Publishers.

111. Shea T. Post-Soviet Maskirovka, Cold War Nostalgia, and Peacetime Engagement. Military Review, 2002. May/June, p.63-67.

112. Shibaev D. State Policy Against Information War. URL: file:///C:/Users/dell%2015z/Downloads/182-348-1-SM.pdf.

113. Skocpol, T., 1979. States and Social Revolutions: A Comparative Analysis of France, Russia, and China. New York: Cambridge University Press.

114. Stouffer, S. A., Cochran E., DeVinney L. C., Star S. A., and Williams, R. M., 1949. The American Soldier: Adjustment During Army Life. Princeton: Princeton University Press.

115. Street J. Mass Media, Politics and Democracy. Houndmills, Palgrave, 2001.

116. Sullivan G. War in the Information Age. URL: https://www.files.ethz.ch/isn/109690/War_Information_Age.pdf.

117. Szafranski, R., 1995. When waves collide, Essay contest on the Revolution in Military Affairs. Joint Force Quarterly.

118. Tarrow, S., 1998. Power in Movement: Social Movements and Contentious Politics. New York: Cambridge University Press.

119. Tilly, Ch., 1978. From Mobilization to Revolution. New York: McGraw-Hill Publishing Company.

РОЗДІЛ 2

ЗМІСТ І ЗАСОБИ ІНФОРМАЦІЙНОЇ ВІЙНИ ЯК СКЛАДОВОЇ ПОЛІТИЧНОГО НАСИЛЛЯ

2.1 Інструментарій інформаційної війни

Сучасний цифровий світ демонструє одночасно і звершення і вади суспільства. З одного боку, поглиблюється арсенал знань, удосконалюються технології, з іншого, - усі ці досягнення почасти використовуються для дестабілізації, пошкодження та руйнації. Стрімкими темпами розвивається інформаційно-комунікаційне поле глобалізованого світу, держави поринули у активне удосконалення інформаційно-комунікаційної інфраструктури. Інформаційна війна вийшла чи не на перше місце серед засобів нефізичного впливу на людину зокрема та спільноту загалом. Поза іншим, інформаційна війна широко застосовується у сучасних політичних протистояннях між політичними акторами різних рівнів та масштабів.

Як предмет наукового дослідження інформаційна війна комплексно вивчається як українськими науковцями, так і їх зарубіжними колегами через високий рівень прикладної значущості цієї тематики. Серед експертів найвищого гатунку доцільно згадати, зокрема А. Еріксона [24], А. Кампена [15], М. Лойда [31], Г. Салівана [40] тощо. Завдяки напрацюванням цих науковців та великої кількості інших на сьогоднішній час досліджені різні аспекти інформаційної війни: сутність, форми, наслідки тощо. Однак, інструментально-функціональний вимір, на нашу думку, висвітлений у недостатній мірі у науково-дослідній літературі.

Відповідно, мета цього підрозділу полягає у дослідженні інструментів політико-інформаційної війни і деталізується реалізацією таких завдань, як розкриття функціонального навантаження кожного інструменту, а також з’ясування ролі цих засобів за атакувальної та захисної стратегій.

Отже, інформаційна війна у політичній площині застосовується задля досягнення політичних цілей за рахунок використання інформаційного інструментарію. Комплексний аналіз інформаційної війни як засобу політичного насилля з необхідністю передбачає дослідження прикладних аспектів, зокрема інструментів, за допомогою яких відповідне протистояння може здійснюватися. Інструментальний арсенал інформаційної війни – це, по суті, інформаційна зброя.

«Інформаційна зброя – це сукупність засобів та методів, що дозволяють викрадати, спотворювати чи знищувати інформацію; обмежувати чи припиняти доступ до неї законних користувачів; порушувати роботу або виводити з ладу телекомунікаційні мережі та комп'ютерні системи, що використовуються у забезпеченні життєдіяльності суспільства та держави. А також інформаційна зброя здатна змінювати свідомість людей, змушує їх неадекватно сприймати реальність, жити у світі ілюзій та робити згубні для себе вчинки» [1].

«Інформаційну зброю від звичайної відрізняють: прихованість — можливість досягнення мети без видимої підготовки та оголошення війни; масштабність — можливість завдавати невиправні збитки, не визнаючи державних кордонів і суверенітетів, без обмеження простору в усіх середовищах; універсальність — можливість багатоваріантного використання країною, що нападає, проти як воєнних, так і цивільних об’єктів країни ураження», - стверджує група вітчизняних дослідників на чолі з І. Харченком [10].

А. Стадник вважає, що «Інформаційна зброя може характеризуватись такими показниками, як цілеспрямованість, вибірковість, масштабність впливу, досяжність, швидкість доставки, комплексність впливу на людей, технічні засоби і системи, можливість регулювання (дозування) «потужності» впливу, що визначає її як зброю масового впливу» [9, с. 114].

О. Рудаков визначає інформаційну зброю, як «єдину систему комплексного комбінованого, пучкового, цільового та ударного застосування

усіх сил і засобів технологічного, комунікативного, інформаційно-психологічного впливу на підсвідомість суб'єкта атаки. Ця зброя руйнує інтелект, військову інформаційну інфраструктуру, яка вирішує завдання управління військами, одночасно вражає інформаційні урядові комунікації та громадські системи супротивника» [8, с. 26].

С. Расторгуєв пропонує розглядати інформаційну зброю крізь алгоритмічну призму. Так, дослідник зазначає, що «інформаційна зброя – це насамперед алгоритм. Застосувати інформаційну зброю це означає так підібрати вхідні дані для системи, щоб активізувати у ній певні алгоритми, а в разі їх відсутності активізувати алгоритми генерації потрібних алгоритмів» [7, с. 76].

Тож, які інструменти можуть бути зараховані до арсеналу інформаційної зброї? На нашу думку, за найбільш узагальнюючого підходу можна виділити такі категорії, як збір, передача, захист, маніпулювання, порушення, деградація та заперечення. Деталізуємо їх зміст у подальшому аналізі.

Збір інформації є одним із інструментів інформаційної війни, оскільки та сторона протистояння, яка знає більше, у результаті матиме вирішальні переваги. Ідея полягає в тому, що чим більше у людини інформації, тим вище її обізнаність про ситуацію, що, у свою чергу, веде до кращого планування бою та кращих результатів. За словами А. Сіна, «… недавно знання свого положення та позиції дружніх сил саме по собі було величезним завданням. Технології точного визначення місцезнаходження, такі як навігація на основі глобальної системи позиціонування (GPS), значною мірою полегшили ці проблеми. Знання позиції противника також стало певною мірою можливим завдяки застосуванню технологій розвідки та спостереження» [37]. Далі він зазначає, що «функції розвідки та спостереження... рухаються до використання датчиків із спектрів, таких як інфрачервоний, ультрафіолетовий, нюховий, слуховий, зоровий, сейсмічний тощо, і об'єднання даних з них для формування всеосяжної картини» [37]. У інформаційній війні збір інформації набагато менш небезпечний і більш повний, оскільки ці технології можна

використовувати для проникнення в ситуації та збору точної інформації з мінімальною втратою достовірності.

Збір великої кількості вичерпної інформації, безумовно, є хорошою практикою, але він не має великої цінності, якщо інформація зберігається в сховищі й не використовується. Таким чином, здатність своєчасно передавати інформацію в руки тих, хто її потребує, є ще одним важливим аспектом інформаційної війни. Інструменти, які використовуються в цій області, - це не зовсім зброя, а скоріше цивільні технології, які використовуються у військових ситуаціях. Найважливішим з цих інструментів є комунікаційна інфраструктура, що складається з мереж комп'ютерів, маршрутизаторів, телефонних ліній, оптоволоконного кабелю, телефонів, телевізорів, радіоприймачів та інших технологій і протоколів транспортування даних. Без цих технологій можливість транспортування інформації в режимі реального часу, що вимагається за сучасними стандартами, була б неможливою.

У даному контексті хотілося б звернути увагу на аспект введення терміна «мережа» до військової лексики. Упродовж сотень років для поширення інформації військові покладалися на ієрархії, а не на мережі. Цивільні досягнення в комунікаційних технологіях дотримуються мережевої парадигми, що може серйозно змінити уявлення про командування і контроль у військових колах. Перехід до мережевих структур може вимагати децентралізації командування та контролю. Але децентралізація — це лише частина картини. Нова технологія також може забезпечити кращий «пригляд», центральне розуміння загальної картини, що покращує управління складністю. З цього стає очевидним, що навіть, здавалося б, базові зміни в технології транспортування інформації можуть зробити війну інформаційної епохи абсолютно відмінною від її аналога індустріальної епохи.

Одним із найбільш широко узгоджених аспектів інформаційної війни є необхідність мінімізувати обсяг інформації, до якої має доступ опонент. Значна частина цього завдання пов’язана з захистом інформації, яку ви маєте утримати від захоплення іншою стороною. Зброя, яка використовується для

захисту інформації, поділяється на два класи. По-перше, це ті технології, які фізично захищають життєво важливі засоби зберігання даних, комп'ютери та транспортні механізми, включаючи бомбо- та куленепробивні кожухи та механізми запобігання проникненню, такі як замки та сканування відбитків пальців. По-друге, і, можливо, важливіше, це технології, які запобігають видимості та перехопленню фрагментів ворогом. Це, безумовно, стосується основних технологій комп'ютерної безпеки, таких як паролі, а також більш складні технології, як-от шифрування. За словами М. Лібіцкі, «заплутуючи власні повідомлення та розшифровуючи повідомлення іншої сторони, кожна сторона виконує квінтесенцію інформаційної війни, захищаючи свій власний погляд на реальність, одночасно принижуючи погляд іншої сторони» [29].

Наступний широко уживаний інструмент – це інформаційні маніпуляції. У контексті інформаційної війни – це зміна інформації з метою спотворити картину реальності опонента. Це можна зробити за допомогою ряду технологій, зокрема комп'ютерного програмного забезпечення для редагування тексту, графіки, відео, аудіо та інших форм передачі інформації. Розробка маніпульованих даних, зазвичай, виконується вручну, щоб ті, хто командує, мали контроль над тим, яке зображення представляється ворогу, але вищезгадані технології переважно використовуються для пришвидшення процесу фізичного маніпулювання після визначення вмісту.

Кінцевими аспектами інформаційної війни є порушення, деградація та заперечення. Усі три прийоми є засобами для досягнення однієї і тієї ж загальної мети – запобігання отриманню ворогом повної правильної інформації. Через їхню схожість багато однакових видів зброї використовуються для досягнення однієї або кількох цілей. Тому має сенс обговорити їх разом. Деякі з найбільш популярних видів зброї, які використовуються для ведення цих видів інформаційної війни, — це підробка, введення шуму, заглушення та перевантаження [29].

Підробка – це техніка, яка використовується для погіршення якості інформації, що надсилається ворогу. Потік інформації ворога порушується

введенням у цей потік «підробки» або підробленого повідомлення. Ця техніка працює, оскільки дозволяє надавати неправдиву інформацію системам збору цільових конкурентів, щоб спонукати цю організацію приймати погані рішення на основі цієї помилкової інформації.

Інший спосіб порушити інформацію, яку отримує опонент, - це ввести шум на частоту, яку він використовує. Фоновий шум заважає противнику відокремити фактичне повідомлення від шуму. Це особливо корисна техніка, якщо ворог використовує бездротовий зв'язок, оскільки ці частоти можна використовувати без необхідності під'єднання до фізичної мережі кабелів.

Заглушення – це техніка, яка використовується для досягнення заперечення, яка включає перехоплення сигналів, надісланих між двома каналами зв'язку або між датчиком і каналом. Сигнал перехоплюється, потім «заглушається» або зупиняється від подальшого просування до цільового призначення. У більшості випадків той самий сигнал зберігається захоплюючим як розвідувальна інформація і використовується для визначення погляду противника на його власну позицію в змаганні.

Нарешті, перевантаження – це техніка, яка використовується для відмови ворогу в інформації як у військових, так і в цивільних умовах. Надсилаючи в комунікаційну систему противника об'єм даних, який є занадто великим для того, щоб він міг обробити, спричиняється збій або серйозне погіршення здатності системи передавати інформацію. Система настільки зайнята боротьбою з перевантаженням, що не в змозі надати важливу інформацію тим, хто її потребує. Цю тактику називають атакою «відмова в обслуговуванні», і вона виявилася легкою та ефективною.

Таким чином, «Інформаційно-технічний вплив є цілеспрямованим виробництвом і поширенням спеціальної інформації, яка справляє безпосередній вплив на функціонування та розвиток інформаційно-технічного середовища суспільства, тобто комп'ютери, засоби зв'язку і програмне забезпечення відіграють роль зброї масового збою, за допомогою якої можна проникати до комп'ютерних систем і порушувати їх роботу» [3].

Перераховані вище методи та зброя, безумовно, можуть завдати серйозної шкоди воєнно-політичним операціям, що залежать від інформації. Сучасний контекст інформаційного суспільства робить держави та інших політичних акторів особливо у країнах з високорозвиненою інформаційно-комунікаційної інфраструктурою, з одного боку, найбільш дієвими, а з іншого, - найбільш уразливими. Як же тоді захищатися? Існує кілька способів, багато з яких використовують ті самі прийоми, які задіяні за атакувальної стратегії. Тож, розглянемо також доступні контрзаходи для кожного з вище озвучених інструментів інформаційної війни.

Захищатися від атак збору інформації означає не дати ворогам можливості зібрати інформацію про себе та/або про конфліктну ситуацію. Це передбачає захист власної інформації від перехоплення та запобігання потраплянню інформації до об’єктів збору ворога. Таким чином, доступними контрзаходами для захисту від збору інформації є та сама зброя, яка була визначена раніше для використання для захисту, підробки, заглушення та перевантаження. Зокрема, використання шифрування, підробки, введення шуму, заглушення та перевантаження є особливо корисними для зведення до мінімуму збору інформації ворогом.

Оскільки транспортування інформації сильно залежить від інфраструктури, найефективнішим контрзаходом для запобігання передачі-тримання є знищення інфраструктури противника. Цей конкретний контрзахід, «потребує знання того, як спілкується інша сторона» [29]. Із цими знаннями захист може бути відносно легким. Якщо архітектура транспортування інформації будується на дротах та вузлах, останні легко ідентифікуються та виводяться з ладу. Як і командні центри, системи зв’язку можуть бути пошкоджені внаслідок атак на генератори, підстанції та трубопроводи подачі палива. Якщо архітектура є електромагнітною, часто ключові вузли видно. Якщо супутники використовуються для передачі та сигналізації, то лінії зв'язку можуть бути заглушені або збиті.

Атака на інфраструктуру противника як протидія транспортуванню інформації може бути не тільки особливо легкою, але також може мати далекосяжні наслідки для всієї їхньої інформаційної системи. У своїй книзі «Захисна інформаційна війна» Д. Альбертс зауважує про це явище: «Два різні сценарії служать для ілюстрації хаотичного характеру атак на інфраструктуру. У першому випадку конкретна атака на інфраструктуру може викликати низку приблизних наслідків, які важко передбачити, і які значно посилюють наслідки атаки. У другому випадку серія атак демонструватиме хаотичну поведінку, коли сума їх кумулятивного ефекту значно перевищує суму індивідуальних впливів серії незалежних подій. Це не рідкісні моделі» [11].

Щоб протидіяти спробам ворога захистити власну інформацію, треба мати можливість обійти їхні механізми захисту. Як зазначалося раніше, основною технологічною зброєю для захисту власної інформації є шифрування. На жаль, нещодавнє зростання складності криптографії дуже ускладнило контрзаходи. "Декодування повідомлень, створених комп'ютером, усе більше ускладнюється. Комбінація таких технологій, як стандарт потрійного цифрового шифрування для передачі повідомлень за допомогою закритих ключів, і шифрування з відкритим ключем для передачі приватних ключів за допомогою відкритих ключів, ймовірно, буде переможена найкращими комп’ютерами, що розшифровують код» [29]. Що це означає для тих, хто бажає протидіяти захисту інформації, так це те, що їхні зусилля згодом стануть марними. А ось спроби зламати коди за допомогою потужних комп’ютерів, швидше за все, принесуть найкращі результати.

Хоча криптографія є найефективнішою, вона не є єдиним інструментом захисту інформації. Насправді, паролі є набагато більш поширеною технікою для захисту інформаційних систем від несанкціонованого доступу. Однак, на жаль, системи паролів залежать від людей, які відстежують і вводять коди, що створює для них значну вразливість. Якщо є можливість фізичного доступу до системи або тих, хто її використовує, отримання або вгадування паролів може

бути неймовірно простим і є дуже ефективним засобом для отримання доступу до захищеної інформації.

Як тільки ворог отримає інформацію, запобігти маніпулюванню нею буде надзвичайно складно. З огляду на це, насправді існує лише два контрзаходи для захисту від такого роду атак. По-перше, можна працювати над тим, щоб не допустити перехоплення інформації ворогом. Найефективнішими тут є методи захисту інформації, оскільки вони не дозволяють ворогу отримати доступ до інформації або зрозуміти її у початковій формі.

Другий, і, можливо, більш важливий ключ у захисті від маніпуляцій з даними — запобігти повторному введенню змінених даних у потік реальної інформації. На щастя, для цього існує кілька методів, найпоширенішим з яких є резервування.

М. Лібіцкі називає маніпуляцію інформацією «семантичною атакою» і зазначає, що «система під семантичною атакою функціонує і буде сприйматися як така, що працює правильно... але вона генеруватиме відповіді, що відрізняються від реальності...» [29]. Це відбувається, тому що ці системи залежать від якогось джерела інформації, яке дослідник називає датчиком для отримання інформації про реальний світ. Якщо датчики можна обдурити, системи можна обдурити. Щоб протидіяти семантичній атаці, захист від збою може полягати, скажімо, у датчиках, надлишкових за типами та розподілами, за допомогою мудрого розподілу влади на прийняття рішень між людьми та машинами. Збираючи ту саму інформацію з кількох зайвих джерел, збільшується ймовірність того, що правильна інформація пройде. Навіть якщо ворогу вдасться зіпсувати ці дані на одній лінії зв’язку, можна легко виявити погані дані, оскільки вони відрізнятимуться від картини, намальованої рештою ваших джерел.

Захист від порушення інформації, деградації та заперечення вимагає застосування багатьох із згаданих контрзаходів. Будь-який з видів зброї для здійснення цих типів атак вимагає доступу до каналів зв’язку противника, тому механізми захисту інформації та резервні канали можуть бути

ефективними для підтримки деяких ліній зв’язку, на які потенційні зловмисники не впливають. «Наша колекція застарілих систем забезпечує певну частку притаманної надійності та стійкості. Вони вказують на перекриття та дублювання в цих системах і стверджують, що комусь було б дуже важко повністю порушити певний набір послуг» [11].

Існує також кілька доступних методів, спеціально розроблених для протидії описаній зброї для виконання атак порушення, деградації та заперечення. «Комунікатори рухаються до технологій стрибкоподібної зміни частоти, широкого спектру та множинного доступу з кодовим поділом (CDMA), які важко заглушити та перехопити. Зв’язок із відомих місць... може використовувати цифрові технології для фокусування на фронтальних сигналах та відкидання глушіння, яке виникає з боків. Методи цифрового стиснення разом із надлишковістю сигналу означають, що бітові потоки можна відновити неушкодженими, навіть якщо великі частини знищені» [29]. Ці методи, а також тисячі інших, які зараз розробляються в дослідницьких центрах по всьому світу, полегшують кожен день відновлення після спроб знищити та заблокувати інформацію, коли вона потрапляє до цільового призначення.

Існують і менш розгалужені підходи до деталізації інструментарію інформаційної війни. Зокрема О. Левін виділяє такі найпоширеніші види інформаційної зброї:

- засоби розкрадання інформації;
- засоби подолання систем захисту;
- засоби обмеження допуску законних користувачів;
- засоби порушення роботи комп'ютерних систем [5, с. 65].

Авторський колектив на чолі з Ф. Акелло запропонували власну систему інформаційно-воєнної зброї, виділивши такі кластерні підрозділи (функції) останньої, як огляд, оцінка, командування, контроль та виконання [25]. Усі ці інструменти взаємопов’язані і подані вище у їх логічному порядку використання. Розглянемо кожну групу більш детально.

Огляд є першою підфункцією. Цей крок включає накопичення даних, що охоплюють інформаційну систему опонента, щоб планувальники могли використовувати модель операційної архітектури. Активи, які планувальник може використовувати, щоб зібрати цю інформацію у складному діапазоні від багатомільйонних супутників до агента, який працює під прикриттям, щоб отримати інформацію з відкритих джерел з Інтернету або місцевої бібліотеки. Збір інформації здійснюється за допомогою семи основних засобів. Це розвідка зображень, людський інтелект, розвідка сигналів, розвідка вимірювань і підписів, технічна розвідка, контррозвідка та розвідка з відкритим кодом.

Залежно від потреб та рівня конфлікту, огляд може варіюватися від тактичного до стратегічного. Для дослідження на стратегічному рівні область інтересів може охоплювати цілі країни або регіони. В оперативному або тактичному середовищі зони інтересу можуть бути обмежені країною, містом або навіть полем бою. Наприклад, під час «Бурі в пустелі» силам коаліції була потрібна як стратегічна, так і оперативна розвідка, яка охоплює електромагнітний спектр. Вони отримали цю інформацію за допомогою космічних засобів, до яких вони мали різний ступінь доступу.

Наземні можливості для отримання інформації, необхідної на етапі огляду, передбачають традиційні та менш традиційні методи. Традиційні методи включають людський інтелект, технологічний інтелект, розвідку з відкритим кодом, електронне підслуховування тощо. Нетрадиційне джерело зараз викликає дедалі більше занепокоєння не лише з боку урядів, а й у приватному секторі. Це несанкціоноване проникнення в електронні системи даних — іншими словами «злом».

За допомогою комп’ютерного злому можна дістатися до комп’ютерних файлів супротивника і отримати детальну інформацію про його чи її можливості, готовність і навіть фінансовий стан уряду. Інструменти для злому недорогі: персональний комп’ютер і модем – це все, що потрібно. За допомогою цих простих інструментів хакер може отримати доступ до будь-

якого іншого комп’ютера, який має модем. Справді унікальним є те, що це може зробити людина на персональному комп’ютері, розташованому за тисячі миль від цілі.

Друга підфункція, яку повинен виконати учасник інформаційної війни, — оцінити інформацію, зібрану на попередньому етапі. Зараз дані опитування обробляються та аналізуються. Термін, що використовується для опису цього процесу, — «злиття інформації», поєднання інформації в картину простору бою, яку може використовувати інформаційно-воєнний актор.

Щоб здійснити оцінку треба почати з переміщення інформації від функції огляду до функції оцінки. Ось деякі шляхи переміщення інформації до функції оцінки та виходу з неї: радіо, мікрохвилі, низхідні лінії супутникового зв’язку, комерційні та військові телефонні системи (захищені та незахищені), волоконна оптика, факсиміле, трафік повідомлень, і кур'єр. У інформаційну епоху засобом, яким переважно володіють ті, хто володіє здібностями, є електронна передача даних.

Зі збільшенням відстані між відправником і одержувачем зростає ймовірність того, що супутники будуть переважаючим способом передачі даних. У період високого попиту використовуються як комерційні, так і військові супутники. Наприклад, під час «Бурі в пустелі» 22% військового трафіку проходило через комерційні супутники. Супутники можна навіть використовувати для передачі даних на інші супутники, такі як супутникова система відстеження та ретрансляції даних, для того щоб досягти всесвітнього охоплення. У разі супутників спостереження ці системи обмежені їх здатністю або відсутністю обробляти дані. Для виробництва значущих даних або зображень з необроблених даних, які надходять від їхніх датчиків, потрібні величезні обчислювальні можливості. Такий обсяг комп’ютерних можливостей займає простір, а в супутниках простір є надзвичайно важливим. Таким чином, вихідні дані передаються через наземний вузол низхідного зв’язку в центри аналізу для обробки.

Потім оброблені дані надходять у функцію оцінки, щоб проаналізувати їх за допомогою методів інтерпретації на основі людини та комп'ютера. Після завершення аналізу про це повідомляється командно-контрольній службі за тими ж лініями зв'язку, які були описані раніше. Після отримання даних аналітики розвідки оцінюють їх значення. Активи, які беруть участь у цьому процесі, включають такі речі, як спеціалізоване програмне забезпечення, комп'ютерні бази даних та засоби перегляду зображень.

Командна функція отримує картину поля бою від функції оцінки, проводить планування та визначає курси дій. На цьому етапі актори інформаційних війн використовують ручні або автоматизовані системи планування та цільові бази даних для створення загальної кампанії інформаційної війни. Вони також розробляють кроки кампанії (щоденні, погодинні тощо), що передбачають узгодження конкретних інструментів інформаційної війни з центрами тяжіння, визначеними на етапі оцінки. План інформаційної кампанії тепер передано до контрольної функції, яка контролює його виконання.

Функція контролю аналізує отримані накази, готує активи, реагує на загрози та зміни ситуації та повідомляє про результати через ланцюг командування. Існує дуже мало активів, призначених безпосередньо для ведення інформаційної війни. Натомість використовувані активи будуть залучені з тих, що належать до сухопутних, повітряних та морських компонентів. Таким чином, функція управління, зазвичай, буде виконуватися через механізми управління компонентами. Відповідно, інструменти, які учасники інформаційних війн використовують для контролю виконання кампанії, будуть включати комплекс засобів, таких як авіаційний комплекс радіолокаційного виявлення і наведення, а також центри управління повітряно-десантними, наземними та наплавними комплексами.

Виконання в інформаційній війні включає два аспекти: інформаційну атаку та інформаційний захист. Засоби для виконання як наступальних, так і оборонних дій розбиті на шість підкатегорій, кожна з яких буде розглянута

далі. Незалежно від використаного методу, бажаний ефект полягає в тому, щоб створити комбінацію «перевантаження даними» та «недостатності даних» в інформаційній системі супротивника, яка погіршить картину його поля бою, і захистити власну систему від цих ефектів. Перевантаження даними виникає, коли система не може впоратися з інформацією, що надходить до неї або протікає через неї. І навпаки, нестача даних – це коли припиняється надходження адекватних даних до інформаційної системи. Цього можна швидко й ефективно досягти за допомогою одночасних операцій проти різних інформаційних точок, концепція, відома як «паралельна війна» [20, с. 3].

Коли безліч інформаційних точок атакується паралельно, в інформаційній системі виникають два результати. По-перше, пошкоджені точки більше не надають інформацію нижчестоящим функціям і, таким чином, «голодують» частини системи, до яких вони підключені. По-друге, сегменти інформаційної системи, які зараз не порушені, повинні нести існуюче навантаження всієї системи, а також збільшений потік трафіку від реальних або штучно викликаних звітів про порушення. Один-два відповідних ударів може призвести до катастрофи для непідготовленого супротивника. Але як актору інформаційної війни досягти бажаного ефекту?

Можна виділити шість ключових категорій операцій, які слід використовувати для атаки або захисту інформації:

1. Психологічні операції — використання інформації для впливу на міркування противника;

2. Електронна боротьба — заперечує ворогу точну інформацію;

3. Військовий обман — вводить противника в оману щодо його можливостей або намірів;

4. Фізичне знищення — перетворює накопичену енергію в руйнівну силу;

5. Заходи безпеки — заперечує інформацію про військові можливості та наміри;

6. Інформаційна атака — прямо пошкоджує інформацію, не змінюючи помітно фізичної одиниці, в якій вона знаходиться.

Інформаційна війна – це як дуже старий, так і дуже новий стиль ведення боротьби. Бажаний ефект залишається незмінним — модернізувалися лише форми обробки інформації та інструменти її атаки. Метою цього підрозділу було надати короткий огляд репрезентативних систем і методів, які актори інформаційних війн можуть використовувати для проведення кампанії інформаційної війни. Плануючи кампанію інформаційної війни, планувальник, ймовірно, матиме більше ресурсів, ніж описано тут. Зважаючи на те, що кожна система і ситуація відрізняються, учасник інформаційної війни повинен зіставити доступні ресурси з вразливими місцями, визначеними моделлю операційної архітектури, щоб розробити успішну кампанію.

Будь-яка війна, якщо вона націлена на перемогу, у тому числі й інформаційна, має спиратися на виважену стратегію. Чіткий план дій інформаційного протистояння передбачає визначення мети, завдань, цільової групи, інструментів, змісту меседжів тощо. Без стратегічного підходу усі активності в межах інформаційного протиборства матимуть несистемний характер, алогічний зміст, сумбурну динаміку. А окремі успішні операції будуть радше випадковим везінням, які у фіналі не матимуть вирішального значення. Високоякісна інформаційна інфраструктура, досвідчені фахівці та належний збройний арсенал без продуманої і перманентно оновлюваної стратегії може стати виразною мішенню, вразливою для швидких та ефективних атак.

Поняття «стратегія» походить з давньогрецької мови. «Stratos» означає «армія», а «agos» - «я керую». З. Бурик зазначає, що найперше цей термін розумівся, як «мистецтво або наука ведення воєнних дій» [2, с. 2]. Авторство поняття дослідники приписують різним видатним історичним особистостям, як то О. Македонський або ж Чингісхан [22].

Стратегія — це загальний план, що охоплює довготривалий проміжок часу, спосіб досягнення важливої мети. Завданням стратегії є ефективне використання наявних ресурсів для досягнення основної мети (стратегія

набуває особливого значення, коли наявних ресурсів недостатньо для досягнення визначеної мети).

В. Квінт визначає стратегію, як систему пошуку, формулювання і розвитку доктрини, яка забезпечить довгостроковий успіх при послідовній і повній реалізації [4].

І. Ансофф переконаний у тому, що вибір стратегії та формування політики, насамперед, є процесом прийняття рішення. Це встановлення цілей, після чого із застосуванням серії аналітичних методів визначаються альтернативи та здійснюється вибір між ними [12, с. 8].

Сьогодні стратегічний підхід перестав бути виключно прерогативою військової царини, він активно використовується у підприємницькій діяльності, в межах публічного та політичного управління. Однак, попри більш широкі масштаби використання, стратегія не втратила своєї значущості для воєнної справи. І наразі є неодмінною умовою провадження ефективної інформаційної війни.

Отже, стратегія розробляється для того, щоб пояснити, як перемогти у інформаційній війні. К. Коп виділяє чотири основні стратегії:

- відмова в інформації;
- обман і мімікрія;
- порушення та знищення;
- підривна діяльність [26].

«Жоден користувач не хотів би, щоб інша сторона мала доступ до його важливої інформації. Використання брандмауера, системи виявлення вторгнень, віртуальної приватної мережі, шифрування та, останнім часом, стеганографія є проявом спроби не допустити зусиль ворога щодо доступу до власної інформації.

У той же час хакери, терористи та іноземні країни щодня розробляють нові інструменти, щоб проникнути в суть ворожих інформаційних систем з наміром вставити оманливу інформацію або програму для створення дисфункції, по черзі для повного знищення. Будь-яка атака на відмову в

обслуговуванні, від «пінгу смерті» до електромагнітної бомби, може бути реалізована для досягнення бажаного цілі. Підривна діяльність - це стратегія, при якій інформація вставляється в систему супротивника, яка запускає процес саморуйнування, такий як логічна бомба, віруси та інші руйнівні програми, які використовують системні ресурси для пошкодження самої системи» [39, с. 9].

Стратегічна інформаційна війна вимагає особливого визнання та уваги, як законний новий аспект війни з глибокими наслідками як для військової стратегії, так і для національної стратегії безпеки будь-якої держави, яка прагне зберегти свій суверенітет, незалежність та цілісність.

Нова інфраструктура та культура кіберпростору останніми роками розвивалися майже виключно за межами військового контексту. Відповідно, нові елементи та характеристики кіберпростору за своєю природою відкривають нові можливості для інформаційної війни.

Паралельно відбувається еволюція міжнародної політики, і в цьому контексті неминуча еволюція війни К. фон Клаузевіца як інструменту політики. У цьому контексті у всіх країн з’являються нові стратегічні інтереси, що дають нові стратегічні дилеми та нові стратегічні цілі, проти яких можна використовувати важелі впливу, включаючи загрозу використання нових видів стратегічної сили. Таким чином, з’являються нові стратегічні загрози та нові стратегічні вразливості. Стає все більш зрозумілим, що еволюція стратегічної війни з часом включатиме все більше загроз і вразливостей кіберпростору, гідних ярлика «стратегічна інформаційна війна».

Національна стратегія — це мистецтво і наука розвитку та використання політичних, економічних і психологічних сил нації разом із її збройними силами під час миру та війни для забезпечення національних цілей. Національна військова стратегія поширює це на застосування збройних сил для надання максимальної підтримки політиці, щоб збільшити ймовірність і сприятливі наслідки перемоги та зменшити шанси на поразку [19].

Стратеги, як військові, так і бізнесмени, обговорюють точний зміст, розробку та впровадження стратегії, але всі визнають, що це має бути

динамічний процес, який постійно змінюється, щоб адаптуватися до зовнішнього середовища, щоб відповідати навіть статичній політичній позиції [42].

Стратегія формулюється в плані, що визначає засоби реалізації політики. Стратегічний процес включає як діяльність з розробки стратегії, так і додатковий процес оцінки, який постійно контролює ефективність стратегії.

Діяльність з розробки стратегії проходить наступними етапами:

1. Проводиться ситуаційний аналіз для оцінки поточної та прогнозованої загрози, а також технологічних факторів, що впливають на вразливість та летальність загроз;

2. Встановлюються стратегічні цілі на основі політики національної безпеки. Цілі кваліфікують і кількісно визначають рівні безпеки (захист і стримування), які необхідно досягти, і дати досягнення;

3. Розробляються та обґрунтовуються альтернативні підходи для досягнення цілей через недоліки безпеки та невизначеність щодо загроз;

4. Альтернативи обмірковуються, і конкретні елементи плану (наприклад, стратегія захисту, показання та стратегія попередження, стратегія реагування) вибираються на основі ефективності, доцільності, витрат, вигод та ризику. Елементи плану інтегровані в узгоджений стратегічний план;

5. Також розробляється підхід до вимірювання та управління ризиками щодо плану реалізації стратегії з кількісною оцінкою ризиків, ймовірності їх виникнення та наслідків;

6. На основі стратегічного плану виводяться оперативні вимоги для реалізації плану, що включають такі компоненти:

- організаційна структура, ролі та місії;

- необхідна діяльність з досліджень і розробок, тестування та оцінки;

- розробка операційних концепцій, доктрини та навчання.

7. Упродовж виконання плану здійснюється моніторинг виконання впроваджувальних заходів, і відповідний прогрес може використовуватися для перегляду елементів плану.

Оцінка ефективності включає в себе наступні етапи впродовж усієї реалізації стратегії:

1. На основі стратегічних цілей встановлюються показники ефективності та часові межі для моніторингу прогресу в процесі впровадження стратегії;

2. Поточну оцінку проводить незалежна організація (наприклад, групи реагування на надзвичайні ситуації з комп'ютерними системами, центри передового досвіду тощо) для виконання моделювання та аналізу операційних тестів, розвідувальних даних та інших даних про загрози. Оцінки регулярно повідомляються органу, що розробляє політику;

3. Недоліки, визначені в процесі оцінки, використовуються для покращення процесу оперативного впровадження та, у разі необхідності, для перегляду підходу до стратегічного плану.

Складові стратегічного плану включають, як мінімум, такі компоненти:

- визначення завдань інформаційних операцій (державних і приватних, військових і невійськових);

- Визначення всіх застосовуваних політик, конвенцій та договорів національної безпеки;

- постановка цілей та завдань реалізації;

- організації, обов'язки та ролі;

- елементи стратегічного плану:

1. Загрози, можливості та прогнози загроз;

2. Структура, власники та недоліки;

3. Функціональні (експлуатаційні) вимоги до можливостей;

4. Прогнозовані прогалини у спроможності досягти цілей національної безпеки та плани ліквідувати прогалини та пом'якшити ризики;

5. Організаційний план;

6. Оперативний план (концепції операцій);

7. Стратегічний технологічний план;

8. План управління ризиками;

- план оцінки продуктивності та ефективності.

І. Нежданов, який переважно займається вивченням технологій інформаційних війн в інтернеті, при розробці стратегії протидії виділяє наступні ключові етапи:

- моніторинг;
- визначення агресора;
- ідентифікація сил супротивника;
- розробка плану дій;
- офіційні звернення [6, с. 49-52].

Авторський колектив на чолі з Р. Моландером у спільній роботі «Стратегічна інформаційна війна: нове обличчя війни» виділяє сім визначальних особливостей стратегічної інформаційної війни, які відрізняють її від інших форм конфлікту та створюють нові виклики для урядів та суспільств [33]. Ці особливості, які є високоефективними шляхами для вивчення стратегічної проблеми інформаційної війни, заслуговують на особливу увагу.

Перша особливість - низька вартість входу. Ціна на розробку високопродуктивних можливостей інформаційної війна низька і доступна для широкого кола учасників. На відміну від попередніх високоефективних збройних технологій, нова потенційна зброя інформаційної війни може бути розроблена кваліфікованими особами або групами, які проживають у будь-якій точці світу.

Найважливішим явищем для виникнення інформаційної війни є злиття недорогих мікрокомп'ютерів і використання все більш складних комунікаційних мереж для досягнення, наприклад, підвищення ефективності в управлінні потоком даних, матеріалів та інших «товарів» та супутньої інформації від різних виробників і споживачів. Ця обставина безпосередньо призводить до значного збільшення кількості, видів і можливостей потенційних супротивників інформаційної війни. Іншим аспектом функції низької вартості входу є швидко зростаюча складність інформаційної інфраструктури та, як наслідок, вплив цієї складності на інші функції, такі як

розмиті кордони, стратегічна розвідка та тактичне попередження/оцінка нападу.

Існує потужний комерційний імператив для забезпечення того, щоб нова система мереж кіберпростору працювала з підвищеною ефективністю, щоб можна було використовувати запаси будь-яких даних та/або матеріальних товарів з меншою потребою в підтримці великих запасів, які компенсують невизначеність попиту та пропозиції. Ця заміна «ефективності на масу» у багатьох випадках, на жаль, призводить до нових типів уразливості для атак — особливо на ранніх (та під час будь-яких інших) динамічних етапах еволюції мережі (скоріше правило, ніж виняток у більшій частині кіберпростору). Це явище, що швидко розвивається, надає зловмисному та компетентному суб’єкту кіберпростору потенційний майже швидкісний доступ до широкого кола національних «стратегічних цілей» у глобальних межах.

У цій ситуації багато розвинених і взаємопов’язаних мереж можуть бути піддані атаці з боку низки організацій, включаючи кваліфікованих осіб, суб'єктів, які не представляють державу, наприклад, транснаціональні злочинні організації, держави з добре підготовленим кадром «воїнів кіберпростору». Ключовими інгредієнтами є доступ і володіння, наприклад, певним файлом даних, системою керування даними або системою контролю потоків у контексті, коли бази даних ключової інформаційної інфраструктури та системи управління та контролю все більше взаємопов’язані.

Найбільш драматичним прикладом цього явища є вибухове зростання Інтернету, в якому десятки мільйонів користувачів експлуатують глобальну комунікаційну мережу з доступом до десятків тисяч баз даних, які майже не захищені від «несанкціонованого» проникнення.

Шифрування на точках входу до різних баз даних і виконання функції аутентифікаторів повідомлень відповідних користувачів системи є вірогідним засобом підвищення ціни входу для певних класів «любителів» і низькотехнологічних зловмисників кіберпростору («шахраїв»). Можна

передбачити, що з часом низька вхідна ціна спричинить дуже високу «ціну» для внутрішніх правоохоронних органів/іноземної національної безпеки. Принаймні, одним із можливих наслідків швидкого поширення технології шифрування буде подальше посилення складності вітчизняних та іноземних установ збору розвідувальних даних у моніторингу, а тим більше - виявлення джерела майбутніх зловмисників у кіберпросторі.

Друга риса - розмиті традиційні кордони. Традиційні кордони між націями та сегментами суспільства та уряду — і навіть концептуальні визначення, такі як національна держава — сьогодні розмиті. Розмежування між державними та приватними інтересами скомпрометовано зростаючою взаємодією в інформаційній інфраструктурі. Вибуховий глобальний ріст та експлуатація Інтернету демонструють широко відкриті, нерегульовані кордони, характерні для цієї інфраструктури. У межах цього нового кордону, який характеризується плюралізмом і зростаючою кількістю фракцій, є широкі можливості для злочинної діяльності та/або бойової діяльності.

Отже, однією з найважливіших особливостей розвитку глобальної інформаційної інфраструктури (і підпорядкованих їй національних інфраструктур) є розмивання чітких географічних, бюрократичних, юрисдикційних і навіть концептуальних кордонів, пов’язаних із традиційними проблемами національної безпеки. Наприклад, кордони, що визначають суверенну державу, будуть все більше розмиватися. На відміну від втрати національними державами контролю над поточними глобальними фінансовими та валютними ринками, посилення взаємозв’язку національної інформаційної інфраструктури з глобальним кіберпростором неминуче зменшує національний суверенітет.

Серед найяскравіших аспектів цього явища розмиття кордонів є зникнення можливості чітко розмежовувати зовнішні та внутрішні джерела загроз безпеці держави. Це розмивання кордонів значно посилює інституційну напруженість між національною безпекою та правоохоронними органами.

Іншим розмитим явищем є фактичне зникнення за численних обставин чітких відмінностей між різними рівнями антидержавної діяльності у спектрі від злочинності до військового конфлікту. Без чіткого географічного розмежування між іноземними та внутрішніми джерелами збільшується ймовірність того, що діяльність, пов'язану з традиційним шпигунством, злочинністю та «діями війни», буде дуже важко ідентифікувати. З перспективою того, що інфраструктура може бути атакована через кіберпростір, існує підвищена ймовірність того, що національні держави, слабші в традиційних інструментах військової та економічної влади, наймуть окремих осіб для проведення «стратегічних злочинних операцій», фактичне походження яких буде дуже важко визначити.

Інші приклади розмитих традиційних відмінностей включають ті, що виникають між державним і приватним, військовим і комерційним, а також стратегічним і тактичним вимірами. Останнім прикладом є розмивання численних обставин «ефектів зброї» —значна невизначеність щодо фактичних і передбачуваних «ефектів зброї», особливо проблеми невідомої побічної шкоди всередині інфраструктури та між ними від будь-яких конкретних дій.

Наслідком розмиття кордонів є цілком реальна ймовірність того, що в разі нападу країна може навіть не відчути, що зазнає нападу. Аналогічно, не відразу буде зрозуміло, яка агенція або сегмент суспільства повинні відповідати за будь-яку відповідь на напад.

Наступна особливість - управління сприйняттям. Управління сприйняттям може відігравати більшу роль. Хоча організоване та систематичне використання методів обману має потужні історичні передумови, нові методики, засновані на інформації, можуть надати маніпуляторам потужний набір нових інструментів.

Оскільки кіберпростір розвивається, вартість входу зменшується, а кордони національного суверенітету розмиваються, у досвідчених недержавних і державних суб'єктів з'являється більше можливостей маніпулювати інформацією, яка є ключовою для сприйняття. Почнемо з того,

що Інтернет та його ймовірні комерційні конкуренти забезпечують мережу розповсюдження «пропаганди», створеної широким колом акторів. Групи політичних дій та неурядові організації зможуть використовувати Інтернет для мобілізації політичної підтримки, приміром, проти уряду, який може вирішити застосувати військову силу в умовах кризи, сповненої невизначеністю та потенційними внутрішніми суперечками.

Крім того, існує ймовірність того, що «фактами» події можна сильно маніпулювати за допомогою тексту, аудіо та відео (наприклад, використання передових відеотехнологій для маніпулювання зображеннями). Зокрема, такі методи можуть дозволити широкому спектру акторів проводити витончене управління сприйняттям або кампанії публічної дипломатії, покликаними підірвати внутрішню підтримку певного курсу дій держави. Такі кампанії створюють проблеми не лише для уряду, а й для ЗМІ як інституції у пошуках «точного висвітлення». Прямим наслідком цієї функції є те, що особи, які приймають рішення у державі та/або широка громадськість можуть не знати, що є справжнім.

Далі автори виділяють стратегічний інтелект. Останній являє собою новий фундаментальний виклик. Нещодавно виявлені загрози та вразливості інформаційної війни потребуватимуть ретельного перегляду класичних методів збору та аналізу розвідувальних даних. Можливо, знадобиться розробити новий тип аналітичного поля стратегічної розвідки.

Через особливості низької вхідної ціни та розмитих кордонів розвідувальне співтовариство може зіткнутися з великими труднощами у наданні своєчасної та надійної стратегічної розвідки виконавчій владі про поточні та майбутні загрози інформаційної війни.

Очевидно, що цілі для збору розвідувальних даних буде набагато складніше визначити. Класичний геостратегічний підхід фокусування на конкретних національних державах як «загрозах» застарів. Цілі збору розвідувальних даних тепер охоплюватимуть неурядові організації, суб’єктів, які не є національними державами. Вага та значення конкретної загрози

залежатимуть від оцінки як можливостей потенційних зловмисників у кіберпросторі, їхніх намірів та вразливості певного набору цілей. Можливості конкретного зловмисника можуть бути обмежені дуже динамічною природою телекомунікацій кіберпростору, мікропроцесорного апаратного/програмного забезпечення та захисних методів, наприклад, шифрування. Ця інфраструктура включатиме широкий спектр елементів технологічно та економічно розвиненого суспільства сучасного. Ці елементи інфраструктури включають: нафто- та газопроводи; електричні мережі; системи керування транспортом; систему переказу коштів; різні системи банківських переказів; систему охорони здоров'я тощо. Хоча деякі вразливі місця цих елементів інфраструктури добре зрозумілі, багато - ні.

Розвідувальній спільноті буде надзвичайно важко розробити та підтримувати стабільний список потенційних загроз. Загальне глобальне середовище перейшло до набагато більш динамічної багатополярної, а не статичної біполярної структури. Залежно від конкретних геостратегічних та економічних обставин кожна країна може знайти одного або кількох традиційних союзників, які виступають як економічні суперники. Далі, розвідувальні центри можуть зіткнутися з важким завданням відсортувати конкуруючі політичні цілі з військовими аналогами, які мають націоналістичні амбіції, що суперечать стратегічним цілям країни. У меншому масштабі держави можуть зіткнутися з меншими державними акторами, транснаціональними корпораціями, які здатні та готові кинути виклик стратегічним інтересам країни. Встановлення пріоритетів збору й аналітичних ресурсів та інвестицій буде дуже складним для керівництва національної розвідувальної спільноти. Наслідки проблеми стратегічної розвідки включають можливість того, що уряди можуть не знати, ким будуть їхні супротивники або які будуть їхні наміри та можливості.

Тактичне попередження та оцінка атаки постають ще одним новим викликом. Враховуючи різноманітність і тонкість різних методів захисту та атаки в інформаційній інфраструктурі, потрібно буде розробити новий тип

тактичного попередження та оцінки атаки, щоб виявляти та розрізняти помилку, нещасний випадок, розгортання програмних агентів, призначених для шпигунства, та попереднє розгортання зброї програмного забезпечення. Тактичне попередження та оцінка атаки вимагатимуть моніторингу всіх елементів у глобальному вимірі, національної інформаційної інфраструктури та оборонної інформаційної інфраструктури для виявлення заходів спостереження, проникнення та зриву тощо.

Випливаючи з притаманної складності ведення стратегічної розвідки, тимчасовий тиск кризи робить виклик тактичного попередження та оцінки атаки ще більш складним. Існує реальна перспектива того, що для певної атаки чи ситуації національним командним органам будуть представлені різко суперечливі оцінки різних правоохоронних та розвідувальних організацій.

Зловмисник із застосуванням кіберпросторової зброї здатний проводити стратегічні операції з безпрецедентною швидкістю та виходити за межі кіберпростору. Своєчасно знайти «пістолет, від якого іде дим» буде дуже важко, якщо взагалі не неможливо, особливо в контексті серйозної кризи, коли залишається мало часу для більш традиційного розслідування, яке стосуватиметься правоохоронних органів.

З огляду на збільшення складності різноманітних комунікаційних мереж, систем керування базами даних та систем контролю, деякі події будуть результатом невдачі або поганого дизайну. Крім того, імовірно, будуть стратегічні наступальні заходи, під час яких в системи проникають і їх компрометують протягом багаторічної «підготовки поля бою». Значна частина цієї діяльності може бути діагностована неправильно. Результатом цієї функції є те, що держави можуть не знати про те, що відбувається атака, хто атакує або як здійснюється атака.

Створення та підтримка коаліцій. Збільшення опори на союзників по коаліції призводить до зростання вразливості. Майбутні основні регіональні надзвичайні події залучатимуть важливих у військовому та географічному відношенні партнерів по коаліції. Ці союзники можуть мати особливу

вразливість до нових методів атаки інформаційної війни, яку противник може використати, щоб підірвати участь коаліції.

Сьогодні уряди більшості розвинених держав усвідомлюють, що створення та підтримка іноземних коаліцій для підтримки силових дій проти майбутніх міжнародних військових дій буде дуже складним, і ситуація може ще більше погіршитися через проблеми інформаційної війни. Багато союзників можуть самі мати високий ступінь вразливості до атак на свою основну інформаційну інфраструктуру. Цю складність посилюють декілька факторів. По-перше, важливі союзники можуть зіткнуться з такою ж складною проблемою підтримки надійної стратегічної розвідки та можливості тактичного попередження та оцінки нападу. Після серйозного інформаційного конфлікту утримання коаліції стає дедалі складнішим, оскільки союзники охоплені туманом інформаційної війни. Гострі проблеми з виконанням плану коаліції також можуть виникнути, якщо один із партнерів виявиться «слабкою ланкою ланцюга» через вразливість до інформаційно-воєнних атак.

По-друге, багато країн можуть мати гостру вразливість у ключових секторах (наприклад, комунікації, енергетика, транспорт та фінанси тощо), які противник може атакувати, щоб підірвати участь коаліції. Такі вразливості, ймовірно, будуть особливо гострими на ранньому етапі використання цими країнами революції в галузі інформаційних технологій, коли увага буде зосереджена більше на придбанні можливостей, ніж на забезпеченні безпеки системи. Нові системи, придбані за межами країни (в ім’я раннього та економічно ефективного комерційного впровадження), можуть виявитися особливо вразливими. Показовим прикладом є швидке поширення систем стільникового телефонного зв’язку в країнах, де немає традиційної інфраструктури наземних мереж. Мобільні телефони поточного покоління потенційно дуже вразливі до моніторингу, перешкод і крадіжки ідентифікаційних номерів абонентів. Мобільні телефони нового покоління будуть менш уразливими, але вартість зміни покоління може стримувати швидкі зміни в країнах з нижчим рівнем доходу.

І навпаки, інше занепокоєння полягає в тому, що попередні партнери по коаліції, яким знадобиться військова допомога, перш ніж вони візьмуть на себе згоду на участь у коаліції, можуть вимагати гарантії того, що план розгортання в їхньому регіоні не є вразливим до зриву інформаційної війни.

Майбутня залежність держави у конфлікті від союзників і партнерів по коаліції, які потенційно (можливо, унікальними способами) є вразливими до стратегічної інформаційної війни, є наслідком, що має значний вплив на стратегію національної безпеки, що неявно передбачає їхню своєчасну та стійку підтримку.

Уразливість. Сьогодні будь-яка країна може виявитися вразливою перед новою стратегічною загрозою. Враховуючи зростаючу залежність економіки та суспільства від високопродуктивних комп'ютерних мереж, інфраструктури представляють собою новий набір «стратегічних» цілей. Загрози проти ключових цілей на національному рівні можуть мати надзвичайно примусове значення, тоді як прямі атаки можуть мати потужний руйнівний вплив на національний орган, що приймає рішення. Кордони держави не забезпечать притулок від такого роду конфліктів.

Щоб підвищити загальну ефективність економіки, різні ключові інфраструктурні мережі будуть все більше залежати від все більш складних систем управління мережами. Як наслідок, ці елементи інфраструктури стануть стратегічно дуже прибутковими цілями. У цьому контексті захист інфраструктури від атак зброєю в кіберпросторі шляхом погрози відплатою виглядає надзвичайно проблематично. Як зазначалося раніше, існує велика неясність щодо джерела багатьох подій стратегічної інформаційної війни. Противники можуть скористатися нагодою для проведення шкідливої кампанії, яка не передбачає «негайної та масованої помсти».

Крім того, стратегам доведеться розробити узгоджену концепцію ескалації та контролю ескалації. Це може виявитися складним, якщо існує значна невизначеність щодо фактичного «смертоносного радіусу» конкретної

зброї кіберпростору, а тим більше побічної шкоди, завданої успішною атакою на певну національну інформаційну інфраструктуру.

Окрім імовірності того, що майбутні противники атакуватимуть інфраструктуру у відповідь на військові дії, існує також ймовірність того, що цей супротивник зможе використовувати кіберпростір для маніпулювання внутрішніми військами у сприйнятті конфлікту.

Таким чином, «зона внутрішніх справ» потенційно дуже вразлива для інформаційно-воєнної атаки, і в доступному для огляду майбутньому буде дуже важко довести протилежне. Наслідок цієї особливості є неминучим: держава як гарант прихистку втрачає цей статус у контексті нового обличчя стратегічного конфлікту.

У результаті посилення усіх цих особливостей сучасної стратегічної інформаційної війни, їх попереміннього або одночасного функціонування, може постати низка наслідків, з якими складно взаємодіяти. Зокрема, виникають наступні проблеми: напасти може будь-хто; ви можете не знати, хто нападає і хто піддається нападу або хто керує цими процесами; ви можете не знати, що є справжнім; ви можете не знати, хто буде вашими супротивниками або якими будуть їхні наміри чи можливості; ви можете не знати, що на вас нападають, хто цей нападаючий або як він це робитиме; ви можете залежати від інших вразливих; ви втрачаєте власну країну, як надійний прихисток.

Вище окреслені результати цього процесу, переконують у тому, що сьогодні варто враховувати ті аспекти стратегічної інформаційної війни, які відрізняють її від інших нових форм конфлікту.

Підсумовуючи весь опрацьований вище матеріал, наведемо цитату з роботи С. Расторгуєва «Формула інформаційної війни». «Грамотне поєднання всіх допустимих видів впливу на противника є комплексною стратегію впливу. Під допустимими видами дії тут розуміються такі дії, які «грубо» не порушують прийняті у суспільстві на поточний час норми та правила поведінки. Дотримання принципу комплексності при формуванні загальної

стратегії впливу на противника дозволяє посилити ефект від застосування інформаційної зброї…» [7, с. 77].

Отже, у цьому підрозділі наголошується на переході від політики до стратегії і від стратегії до операцій як логічного процесу, який можна простежити. Теоретично, це пов’язано з розвитком комплексних оперативних можливостей на виваженому ґрунті. У реальному світі такі чинники, як темпи розвитку технологій, загрозливий глобальний ландшафт та динамічні національні цілі, змушують планувальників працювати в цих областях одночасно, часто маючи повністю розвинуті можливості (або загрози) без підтримки політики, стратегії чи доктрини, спроможної уможливити їх використання (або захист від загрози). Технологічні розробки забезпечують інструменти та прийоми, які можуть бути зброєю для проведення інформаційної роботи. Політики, стратеги та творці доктрини повинні паралельно розробляти та постійно вдосконалювати межі шарів, які погано формулюють, що таке інформаційний ресурс, хто відповідає за його проведення та як він буде проводитися.

2.2 Основні тенденції інформаційної війни у кіберпросторі

Інформаційна війна, яка ведеться у кібернетичному просторі, - це кібервійна. Одна з форм інформаційної боротьби, що набуває все більшого поширення та актуальності, що насамперед, пов’язано з динамічним розвитком інформаційно-комунікаційних технологій. Враховуючи тенденцію активізації кібернетичних війн, вважаємо доцільним більш ґрунтовно розкрити зміст інформаційної війни у кібернетичному просторі, адже найближчим часом ця форма протистояння може стати домінуючою у інформаційному суспільстві.

Цифровий світ приніс новий тип явної актуальної небезпеки: кібервійну. Оскільки інформаційні технології та Інтернет розвинулися до такої міри, що стали основним елементом національної могутності, кібервійна стала

барабанним ударом дня, оскільки національні держави озброюються для битви у кіберпросторі.

Багато держав здійснюють не лише кібершпигунство, кіберрозвідку та зондування; вони створюють наступальні засоби кібервійни, розробляють національні стратегії та здійснюють кібератаки з тривожною частотою. Усе частіше з'являються повідомлення про кібератаки та проникнення в мережі, які можуть бути пов'язані з національними державами та політичними цілями. Очевидно, що більше фінансового та інтелектуального капіталу витрачається на те, щоб з'ясувати, як вести кібервійну, ніж на спроби запобігти їй.

Насправді, вражає відсутність міжнародного діалогу та активності щодо стримування кібервійни. Це прикро, оскільки кіберсфера — це область, у якій технологічні інновації та операційне мистецтво значно випередили політику та стратегію. Саме тому кібервійна як явище зрештою має бути політично обмежена.

Комплексний підхід до розуміння теми кібервійни вимагає, на нашу думку, ознайомлення з чотирма основними будівельними блоками: кіберпростір, кіберсила, кіберстратегія та кібервійна. Тож, деталізуємо кожне з цих явищ.

Кіберпростір, новий п'ятий простір війни після землі, моря, повітря та космосу, — це всі комп'ютерні мережі у світі та все, що вони об'єднують та контролюють за допомогою кабелю, волоконно-оптичного або бездротового зв'язку. Це не просто Інтернет – відкрита мережа мереж.

З будь-якої мережі в Інтернеті можна спілкуватися з будь-яким комп'ютером, підключеним до будь-якої з мереж Інтернету. Таким чином, кіберпростір включає Інтернет плюс безліч інших комп'ютерних мереж, враховуючи ті, які не повинні бути доступні з Інтернету. Деякі з цих приватних мереж виглядають так само, як Інтернет, але вони, принаймні теоретично, окремі.

Інші частини кіберпростору — це трансакційні мережі, які виконують такі дії, як надсилання даних про грошові потоки, операції на фондовому ринку та

операції з кредитними картками. Крім того, існують мережі, які є системами контролю та збору даних, які просто дозволяють машинам спілкуватися з іншими машинами: панелі керування, які спілкуються з насосами, ліфтами, генераторами тощо. Таким чином, кіберпростір складається з двох мільярдів наявних на сьогодні комп'ютерів, а також серверів, маршрутизаторів, комутаторів, волоконно-оптичних кабелів та бездротових комунікацій, які дозволяють працювати критично важливим інфраструктурам.

Існує безліч визначень кіберпростору. Згідно з одним із таких визначень, «кіберпростір не є фізичним місцем – він не піддається вимірюванню в будь-якому фізичному чи часовому просторі. Це скорочений термін, який відноситься до середовища, створеного в результаті злиття спільних мереж комп'ютерів, ІТ-систем та телекомунікаційних інфраструктур, які зазвичай називають всесвітньою павутиною» [43, с. 17].

Один з добре обізнаних експертів вважає, що кіберпростір — це операційна область, відмітний та унікальний характер якої обумовлений використанням електроніки та електромагнітного спектру для створення, зберігання, модифікації, обміну та використання інформації за допомогою взаємопов'язаних інформаційно-комунікаційних технологічних систем та пов'язаних із ними інфраструктур [27].

Вже ці кілька прикладів ілюструють труднощі у визначенні терміну, що може бути однією з проблем у створенні будь-якого типу спільної згоди між державами щодо того, як міжнародне право має застосовуватися до війни, що ведеться у кіберпросторі.

Ці мережеві та взаємопов'язані інформаційні системи одночасно знаходяться як у фізичному, так і у віртуальному просторі, а також всередині та за межами географічних кордонів. Їхні користувачі варіюються від національних держав та їх складових організаційних елементів і громад до окремих осіб та аморфних транснаціональних груп, які можуть не сповідувати відданість жодній традиційній організації чи національному утворенню. Вони спираються на три різні, але взаємопов'язані ефекти: фізичний, інформаційний

та когнітивний. У сукупності вони включають глобальне інформаційне середовище: фізичні платформи, системи та інфраструктури, які забезпечують глобальне підключення до взаємозв'язкових інформаційних систем, мереж і людей-користувачів; величезні обсяги інформаційного вмісту, які можна надіслати в цифровому та електронному вигляді будь-куди в будь-який час практично будь-кому; і людське пізнання, яке є результатом значного розширення доступу до вмісту, що може мати драматичний вплив на людську поведінку та прийняття рішень [27].

Однією з характеристик кіберпростору є те, що він не може існувати без можливості використання природно існуючого електромагнітного спектру. Без нього мільйони інформаційно-комунікаційних технологій (ІКТ) не тільки не могли б зв'язуватися одна з іншою, але й самі ІКТ не змогли б функціонувати. Функціонування інтегральних схем та інших мікроелектронних пристроїв залежить від електронів. Волоконно-оптичні кабелі ніщо, якщо вони не здатні поширювати світло. Крім того, ІКТ-мережі також залежать від безлічі властивостей електромагнітного спектру для їх суттєвого підключення через радіочастоту та мікрохвилі [32].

Друга характеристика полягає в тому, що для кіберпростору потрібні створені людиною об'єкти, що, знову ж таки, робить кіберпростір унікальним у порівнянні з наземним, морським, повітряним і космічним доменами. Кіберпростір не існував би, якби не здатність людей впроваджувати інновації та виробляти технології, спроможні використовувати різноманітні властивості електромагнітного спектру.

Третя характеристика полягає в тому, що кіберпростір можна постійно тиражувати. Кіберпросторів може бути стільки, скільки можна створити. Але є одна частина повітряного, морського чи сухопутного простору, яка є важливою: частина, яка оскаржується. Однак, у кіберпросторі їх може існувати багато в будь-який момент – деякі суперечливі, інші – ні. Крім того, здебільшого в кіберпросторі ніщо не є остаточним. І через відносно недороге

та легкодоступне обладнання ІТ-системи та мережі, якщо вони пошкоджені, можна швидко відремонтувати та відновити [30].

Четверта характеристика полягає в тому, що вартість входу в кіберпростір є відносно низькою. Ресурси та досвід, необхідні для проникнення, існування та використання кіберпростору, є скромними в порівнянні з тими, які необхідні для експлуатації наземних, морських, повітряних та космічних доменів. Створення стратегічних ефектів у кіберпросторі не вимагає мільярдного бюджету, великої кількості живої сили та зброї. Швидше, скромні фінансові витрати, невелика група мотивованих людей і доступ до мережевих комп'ютерів можуть забезпечити доступ до кіберпростору. Однак, характер кіберпростору такий, що кількість акторів, здатних діяти в цій області та потенційно створювати стратегічний ефект, є експоненційною в порівнянні з іншими доменами.

Ще одна характеристика полягає в тому, що на даний момент у кіберпросторі з ряду причин домінує напад, а не захист. По-перше, захист ІТ-систем і мереж покладається на вразливі протоколи та відкриту архітектуру, а панівна філософія захисту робить акцент на виявленні загроз, а не на ліквідації вразливості [16]. По-друге, атаки в кіберпросторі відбуваються з великою швидкістю, створюючи оборону під великим тиском, оскільки зловмисник має бути успішним лише один раз, тоді як захисник має бути успішним увесь час. По-третє, відтоді як дальність більше не є проблемою у кіберпросторі, атаки можуть відбуватися з будь-якої точки світу [36]. По-четверте, атрибуція атак є особливо важкою, що ускладнює можливі відповіді [14]. І, по-п'яте, переважна залежність сучасного суспільства від кіберпростору забезпечує будь-якому зловмиснику багате на цілі середовище, що призводить до великого навантаження на захисника, щоб успішно захистити домен [16].

Багато хто вважає кіберпростір найновішим і найважливішим доповненням до всесвітнього надбання, яке складається з чотирьох доменів: морського, повітряного, космічного, а тепер і кібернетичного. Морський і повітряний — це міжнародні океани і небо, які не підпадають під юрисдикцію

жодної країни. Космічний простір починається в точці над землею, де об'єкти залишаються на орбіті. А кіберпростір — це електромагнітний спектр, який забезпечує цифрову обробку та комунікації. Морський домен використовувався людьми тисячоліттями, повітря — століттям, а космос — шість десятиліть. Кіберпростір, як найновіше і найважливіше з глобальних надбань, широко доступний біля тридцяти років, проте більше чверті населення світу користується ним щодня, і ця кількість продовжує збільшуватися. Таким чином, кіберпростір став центром ваги глобалізованого світу, а для націй — центром ваги не лише військових операцій, а й усіх аспектів національної діяльності, включаючи економічні, фінансові, дипломатичні та інші операції.

Кіберпростір також можна розглядати як «терени» комунікації, опосередкованої технологіями. Зведений до основ, кіберпростір — це відомий ефір, усередині якого і через який поширюється електромагнітне випромінювання у зв’язку з роботою та керуванням механічними та електронними системами передачі. Більше того, це засіб, в якому інформація може створюватися та задіюватися в будь-який час, у будь-якому місці і практично будь-ким.

Кіберпростір якісно відрізняється від морського, повітряного та космічного простору, але він одночасно перекривається та постійно діє у всіх з них. Що ще важливіше, це єдина сфера, в якій усі інструменти державної влади – дипломатичні, інформаційні, військові та економічні – можуть одночасно використовуватися за допомогою маніпуляції з даними. Так само, як і інші звичайні надбання, це те, в якому тривалий безперешкодний доступ ніколи не може сприйматися як належне природне та гарантоване право. Якщо безперешкодний доступ до електромагнітного спектру буде заблокований через ворожі дії, боєприпаси за допомогою супутників стануть марними, механізми командування та управління будуть порушені, а наслідки можуть бути паралізуючими.

Відповідно, кіберпростір став новим театром військових дій, який, безсумнівно, буде активно фігурувати у майбутніх конфліктах. Успішна експлуатація цього домену за допомогою операцій мережевої війни може дозволити супротивнику домінувати або тримати під загрозою будь-який вияв або все глобальне надбання. І все ж, серед інших трьох, кіберпростір є унікальною сферою, в якій класичні обмеження відстані, простору, часу та інвестицій зменшуються, іноді різко, як для нас, так і для потенційних ворогів.

Влада, заснована на інформаційних ресурсах, - це кіберсила [35]. У той час як кіберпростір — це сфера, в якій відбуваються кібероперації, кіберсила — це сума стратегічних ефектів, які генеруються кіберопераціями в кіберпросторі та з нього. Згідно з одним широко вживаним визначенням, «кіберсила – це здатність використовувати кіберпростір для створення переваг та впливу на події в інших операційних середовищах та за допомогою інструментів влади» [27, с. 38]. Її стратегічна мета зводиться до здатності в умовах миру та війни маніпулювати уявленням про стратегічне середовище на свою користь, водночас принижуючи здатність супротивника усвідомлювати те саме середовище. Перетворення ефектів кібервлади в цілі політики — це мистецтво і наука про стратегію, яка визначається як «управління контекстом для постійної переваги відповідно до політики» [21, с. 6]. Переважно, кіберсила — це здатність керувати ІТ-системами і мережами в кіберпросторі та через нього. Влада залежить від контексту, а кіберсила залежить від ресурсів, які характеризують домен кіберпростору. А серед інших елементів та інструментів влади кіберсила створює синергію між цими елементами та з’єднує їх у спосіб, який покращує їх усі.

Кіберсила формується під впливом багатьох факторів. Хоча кіберпростір існує лише як середовище, кіберсила завжди є мірою здатності використовувати це середовище. Технологія є одним із факторів, тому що можливість «увійти» у кіберпростір – це те, що робить його можливим. Ця технологія постійно змінюється, і деякі користувачі – країни, суспільства, недержавні суб’єкти тощо – можуть перестрибнути через старі технології, щоб

розгорнути та використати нові з величезною перевагою. Організаційні фактори також відіграють певну роль, оскільки організації відображають людські цілі та завдання, а їхні погляди на створення та використання кіберсили формуються їхньою організаційною місією, будь то військова, економічна чи політична. Але елементом, найбільш тісно пов'язаним з кіберсилою, є інформація. Кіберпростір і кіберсила — це виміри інформаційного інструменту влади, і існує безліч способів, якими кіберсила пов'язується з іншими інструментами влади, підтримує й дає змогу використовувати їх [27]. Таким чином, інформація є валютою або ДНК кіберсили.

Кіберпростір також змінює те, як створюється інформація: сировина, яка живить економіку та суспільство. А нові форми вмісту – зображення, звуки, інформація та дані в різних формах – і зв'язок, що використовується для передачі й обміну цим вмістом, змінюють способи впливу. Оскільки протягом останніх двох десятиліть кіберсила справляла все більш широкий вплив на суспільство, держави змушені адаптуватися до цих впливів по-новому. Мабуть, найбільш значний і трансформуючий вплив, який надають кіберпростір і кіберсила, полягає в тому, щоб по-новому зв'язувати людей та організації у все більш залежному світі, в якому змінюються традиційні кордони та формуються нові стосунки між людьми, тепер дедалі частіше також з урядами, а також особами через національні кордони.

Кіберсила може використовуватися для досягнення бажаних результатів у кіберпросторі, або вона може використовувати кібер-інструменти для отримання бажаних результатів в інших областях за межами кіберпростору. Ключовими елементами кіберсили є наука про електромагнітний спектр, технології електроніки та інтегровану штучну інфраструктуру. Ключовим аспектом кіберсили є її здатність маніпулювати або отримати доступ до цілі кіберінфраструктури за допомогою експлуатації та атаки.

Кіберсила покладається на апаратне та програмне забезпечення. Апаратне забезпечення — це механічні, магнітні, електронні та електричні пристрої, що

містять комп’ютерну систему, наприклад, центральний процесор, дисководи, клавіатуру або екран. Кабелі, супутники, маршрутизатори, комп’ютерні мікросхеми тощо також вважаються апаратними засобами. Програмне забезпечення складається з програм, які використовуються для керування операціями та використання комп’ютера. Шкідливе програмне забезпечення – це шкідливе програмне забезпечення, яке заважає звичайним функціям комп’ютера та Інтернет-додатків і є ключовою зброєю в кібервійні.

Кіберсила має три основні характеристики: вона усюдисуща, вона взаємодоповнює і може бути прихованою. Наземна, морська, повітряна та космічна енергетика здатна генерувати стратегічний вплив на кожну з інших областей. Але ніщо так абсолютно і одночасно не створює стратегічного ефекту у всіх сферах, як кіберсила [32], оскільки кіберсила є усюдисущою.

Прихованість кіберсили робить її привабливою для багатьох користувачів. Вони можуть використати цю здатність, щоб таємно володіти нею в глобальному масштабі. Бази даних можуть бути облаштовані на предмет секретної або конфіденційної інформації, при цьому власники не стануть розумнішими після викрадення терабітів даних. Шкідливе програмне забезпечення може бути запроваджено в ІТ-системи та мережі супротивника без відома, доки ця зброя не буде активована і не завдасть шкоди. Таке приховане використання кіберсили, якому сприяють притаманні труднощі визначення особистості та мотивації більшості зловмисників, робить її привабливим інструментом для урядів та інших суб’єктів [14].

Кіберсила технічно, тактично та оперативно відрізняється від інших інструментів військової сили. Але це не виходить за рамки стратегії. Це також не підриває стійкий характер війни, який є незмінним. Ключовим стратегічним атрибутом кібервлади є здатність у мирі та війні маніпулювати стратегічним середовищем на свою користь, водночас принижуючи здатність супротивника усвідомлювати те саме середовище. Ця стратегічна корисність поширюється на всі інші стратегічні сфери, враховуючи їх повсюдну залежність від кіберпростору. Маніпуляція створює стратегічний ефект невірного

спрямування та обману, що, у свою чергу, дозволяє іншим військовим та національним інструментам влади безпосередньо досягати політичних цілей. Кіберсила підпорядковується потребам політики, а стратегія — це процес втілення цих потреб у дії. Кібероперації відбуваються у кіберпросторі та генерують кіберсилу, але вони не служать власним цілям: вони служать цілям політики. Стратегія є мостом між політикою та використанням кіберінструменту.

Кіберсила виступає як ключовий важіль у розробці та здійсненні національної політики. Його можливості ставлять перед стратегом виклик інтегрувати ці можливості з іншими елементами та інструментами влади. А це вимагає розробки кіберстратегії, яка полягає в розвитку та застосуванні можливостей для роботи у кіберпросторі, інтегрованих та координованих з іншими оперативними сферами, для досягнення або підтримки досягнення цілей за допомогою елементів національної влади [27].

Кіберстратегія ґрунтується на систематичному і структурованому поєднанні цілей (цілей і завдань), засобів (ресурсів і можливостей) і способів (як засоби використовуються для досягнення цілей) з дотриманням належного аналізу та врахуванням ризиків і витрат. Таким чином, розробка національної стратегії щодо кіберпростору означає одночасне створення кіберресурсів і процедур, які можуть сприяти досягненню конкретних цілей національної безпеки. Найважливіша частина кіберстратегії стосується цілей, для яких можуть бути використані кіберспроможності. Ці цілі є частиною більш масштабних військових, політичних, економічних, дипломатичних цілей і цілей національної безпеки. Кіберсила створена для підтримки досягнення ширших цілей: стратегічних цілей за елементами національної влади як засобу задоволення життєво важливих національних потреб та інтересів Стратегії національної безпеки. Ключовий внесок національної стратегії щодо кіберпростору полягатиме в тому, щоб чітко продемонструвати, як вона робить можливим досягнення всіх інших стратегій, особливо Стратегії національної безпеки [27]. Хоча національна стратегія повинна охоплювати й

розуміти кібервійну, у цьому процесі національну стратегію необхідно переглянути й адаптувати.

У військовому плані кіберсила була найвпливовішим інструментом останніх двох десятиліть. І кіберсила, і кіберпростір посіли центральне місце у нових концепціях і доктринах війни. На різних рівнях конфлікту, від повстанців до звичайних військових дій основних сил, кібервлада стала незамінним елементом сучасного військового потенціалу, заснованого на технології.

Як і у випадку з терміном кіберпростір, не існує загальновизнаного визначення кібервійни. Кібервійна — це масова скоординована цифрова атака на уряд з боку іншого або великих груп громадян. Це дії національної держави, спрямовані на проникнення в комп'ютери та мережі іншої країни з метою заподіяння шкоди чи збою». Окрім цього, додається, що «термін кібервійна також може використовуватися для опису атак між корпораціями, терористичними організаціями або просто атаки осіб, які називаються хакерами, які вважаються войовничими у своїх намірах.

Інше визначення: «Кібервійна є симетричною або асиметричною наступальною та оборонною цифровою мережевою діяльністю держав або подібних до держав акторів, що охоплює небезпеку для критичної національної інфраструктури та військових систем. Вона вимагає високого ступеня взаємозалежності між цифровими мережами та інфраструктурою з боку захисника, а також технологічним прогресом з боку нападника. Її можна розуміти як майбутню загрозу, а не як нинішню, і вона чітко вписується в парадигму інформаційної війни» [18, с. 2].

Ще одне розуміння кібервійни пропонує сприймати її, як конфлікт, який використовує ворожі, незаконні транзакції або атаки на комп'ютери та мережі з метою порушити комунікації та інші частини інфраструктури як механізм для нанесення економічної шкоди чи порушення захисту [17].

Згідно резолюції Ради Безпеки ООН, кібервійна – це використання комп'ютерів або цифрових засобів урядом або з явним знанням чи схваленням

цього уряду проти іншої держави або приватної власності в іншій державі, включаючи: навмисний доступ, перехоплення даних або пошкодження цифрової та керованої у цифровий спосіб інфраструктури. А також виробництво та розповсюдження пристроїв, які можуть бути використані для підриву внутрішньої діяльності [41].

Успішна кібервійна залежить від двох речей: засобів і вразливості. «Засоби» — це люди, інструменти та кіберзброя, доступні зловмиснику. Уразливість — це ступінь, до якої ворожа економіка та військові використовують Інтернет та мережі загалом [23]. Ми не знаємо, хто має які можливості кібервійни напевно, але дедалі більше держав організовують підрозділи кібервійни та все більш кваліфікованих експертів з Інтернету для боротьби в цій сфері [28].

Отже, кібервійна існує у сфері військових і розвідувальних служб і відноситься до проведення військових операцій відповідно до інформаційних принципів. Це означає порушення або знищення інформаційно-комунікаційних систем, а також пов’язано зі спробами знати все про супротивника, не даючи йому знати багато про себе [13]. Кібервійна — це войовничий конфлікт у віртуальному просторі із використанням засобів інформаційно-комунікаційних технологій (ІКТ) та мереж. Як і інші форми інформаційної війни, кібервійна має на меті впливати на волю та здатність приймати рішення політичного керівництва і збройних сил противника на арені операцій комп’ютерної мережі [34].

Можна виділити три форми операцій в комп’ютерній мережі:

1) атака комп’ютерної мережі – операції, призначені для порушення, заперечення, деградації або знищення інформації, що знаходиться в комп’ютерах і комп’ютерних мережах, або самих комп’ютерів чи мереж;

2) експлуатація комп'ютерної мережі, що означає отримання даних та інформації розвідувального рівня з комп'ютерів противника за допомогою ІКТ;

3) захист комп’ютерної мережі, який складається з усіх заходів, необхідних для захисту власних засобів ІКТ та інфраструктури від ворожих атак на комп’ютерну мережу та експлуатації комп’ютерної мережі [34].

Атака на комп’ютерну мережу, або навмисне паралізування чи знищення можливостей мережі противника, є лише одним із багатьох інструментів у рамках військових завдань. Важливість атаки на комп’ютерну мережу, безсумнівно, зростатиме в найближчі роки, з огляду на стан розвитку наступальних засобів кібервійни. Однак, існує дуже мало тематичних досліджень, і більшість інформації знаходиться за межами публічного доступу. Велика кількість організацій досі не впевнені у стані власної кібербезпеки.

Одним із важливих аспектів кібернетичних протистоянь є те, що неконтрольовані ефекти зворотного ефекту у високо мережевому віртуальному просторі становлять значні ризики для атакуючої держави. Цей фактор є тим більш актуальним, оскільки держави, які найімовірніше розробляють технологічні ноу-хау для стратегічної кібервійни, також найбільше залежать від власної інфраструктури, тому дуже вразливі в кібервійні.

Через неконтрольовані побічні ефекти кібервійна також підірве довіру до кіберпростору в довгостроковій перспективі, що може мати згубні наслідки для глобальної економіки, а отже, і для всіх залучених сторін. Стратегічна кібервійна сама по собі, ймовірно, дратує, але не роззброює супротивника. І будь-який супротивник, який заслуговує стратегічної кампанії кібервійни, щоб бути втихомиреним, також, ймовірно, має здатність завдати відповідного удару способами, які можуть бути більш ніж дратівливими.

Можливості кібервійни на оперативному рівні для дій проти військових цілей можуть сприяти веденню реальної традиційної війни. Оскільки руйнівна кібератака може полегшити або посилити військові операції, а оперативний потенціал кібервійни здається відносно недорогим, його й надалі будуть

розвивати. Але для того, щоб оперативна кібервійна спрацювала, її цілі мають бути доступними та мати певні вразливості.

При всьому цьому кіберзахист залишається найважливішою діяльністю збройних сил у кіберпросторі. Переважна більшість атак, щодо яких було висловлено занепокоєння, стосується лише комп'ютерів, підключених до Інтернету. Як наслідок, системи, які є автономними або зв'язуються через власні мережі або не мають доступу до Інтернету, повинні бути захищені від них. Жертвами збоїв у кібербезпеці та кібератак є багато цивільних систем, і з цієї причини цінність суто військового підходу до захисту кібербезпеки обмежена. Збройні сили відіграють важливу роль у захисті власних систем і розвитку потенційних наступальних можливостей. Хоча більшість того, що потрібно для захисту військових мереж, можна дізнатися з того, що потрібно для захисту цивільних мереж, перші відрізняються від останніх важливими аспектами. Отже, збройні сили повинні добре подумати, створюючи цілі, архітектуру, політику, стратегію та операції з кіберзахисту.

Наразі мало б стати очевидним, що дебати про кібервійну схильні до спекуляцій. Деякі прихильники вважають, що кібервійна рано чи пізно замінить кінетичну війну. Частіше кібервійна представляється як новий вид війни, який є дешевшим, чистішим, з меншим кровопроливттям або без нього, і менш ризикованим для зловмисника, ніж інші форми збройних конфліктів. Таким чином, кібервійна видається привабливою.

Тож, які елементи роблять кібервійну привабливою? На нашу думку, можна виділити наступні аргументи:

- кібервійна дешевша, оскільки не вимагає великої кількості військ і зброї;
- витрати на вхід низькі: маючи комп'ютер та доступ до Інтернету, кожен може брати участь у кібервійні;
- кібервійну легко провадити приховано через глобальне підключення з будь-якого місця;
- інструменти для атаки дешеві та відкрито доступні в Інтернеті;
- поширення таких засобів відбувається без будь-якого контролю;

- немає технологічних, фінансових чи юридичних перешкод для подолання цього розповсюдження;

- є перевага для зловмисника, який може отримати прибуток від останніх і найновіших інновацій;

- кіберпростір надає зловмиснику анонімність, оскільки досить важко відстежити походження атаки;

- кіберпростір надає непропорційну владу маленьким та іншим відносно незначним акторам;

- працюючи за фальшивими IP-адресами, іноземними серверами та псевдонімами, зловмисники можуть діяти майже повністю анонімно та відносно безкарно, принаймні в короткостроковій перспективі;

- кібервійна може допомогти уникнути необхідності брати участь у бойових операціях і таким чином рятує життя;

- кібервійна веде до здатності вивести з ладу супротивника, а не знищити його сили;

- розмиті традиційні кордони: кібервійна створює власний «туман і тертя війни»;

- кібервійні притаманні труднощі з тактичним попередженням та оцінкою атаки чи збитку;

- кібервійна дозволяє акторам досягати політичних і стратегічних цілей без необхідності збройного конфлікту;

- кібервійна пропускає поле битви. Системи, на які люди покладаються, від банків, електромережі до радарів протиповітряної оборони, доступні в усьому світі з кіберпростору, і ними можна швидко заволодіти або знищити без попереднього ураження традиційної оборони країни;

- кібервійна відбувається майже зі швидкістю світла. Оскільки фотони пакетів атаки стікають по волоконно-оптичних кабелях, час між запуском атаки та її наслідками ледве вимірюється, що створює більше ризиків для осіб, які приймають рішення, особливо в умовах кризи;

- жертва атаки повинна інвестувати значні ресурси для нейтралізації загрози, для чого потрібні команди спеціалізованих експертів з програмного та апаратного забезпечення з певними навичками. Таких людей важко найняти та утримати, оскільки приватна промисловість пропонує більш привабливі умови для їх таланту;

- уразливість країн, які все більше залежать від складних, взаємопов'язаних і мережевих інформаційних систем, з часом збільшується, тим самим надаючи супротивникам багате цільове середовище.

Для багатьох термін «кібервійна» створює образи смертоносних шкідливих програм, які викликають зависання комп'ютерів, вихід з ладу системи зброї завдяки технологічній майстерності для безкровного завоювання. Ця картина, в якій кібервійна ізольована від більш широкого конфлікту, діє в іншій сфері від традиційної війни. Поки такий сценарій не повністю виходить за межі можливостей, пропонує безкровну альтернативу небезпекам і витратам сучасної війни, і, отже, виглядає привабливим. Чиста кібервійна – це подія, що ведеться виключно у кіберпросторі.

Деякі дослідники вважають, що майбутні війни та сутички, які передують їм, передбачають поєднання звичайної чи кінетичної зброї з кіберзброєю, яка діятиме як руйнівник чи помножувач сили [38]. Можна виділити низку причин для цього. По-перше, багато критично важливих комп'ютерних систем захищені від відомих експлойтів та шкідливого програмного забезпечення, тому розробникам нової кіберзброї необхідно спочатку виявити нові вразливі місця. По-друге, наслідки кібератак важко передбачити – вони можуть бути менш потужними, ніж очікувалося, але також можуть мати більш масштабні наслідки, що випливають із взаємопов'язаності систем, що призведе до небажаної шкоди для зловмисників та їхніх союзників. І по-третє, немає жодної стратегічної причини, щоб агресор обмежувався лише одним класом зброї. Отже, кібервійна може мати реальні фізичні наслідки.

Як і інші елементи сучасної армії, кіберсили, швидше за все, будуть інтегровані в загальну стратегію бою як частина спільної кампанії. Кіберзброя

буде використовуватися окремо, у комбінації, а також одночасно змішуватися із звичайною кінетичною зброєю як помножувач сили [38]. Комп'ютерні технології, однак, відрізняються від інших військових засобів тим, що вони є невід'ємним компонентом усіх інших засобів у сучасних збройних силах. З цієї точки зору, це один критичний компонент, від якого залежать багато сучасних військових.

Країни по всьому світу розробляють і впроваджують кіберстратегії, розроблені для впливу на структуру командування та управління противника, матеріально-технічне забезпечення, транспортування, раннє попередження та інші важливі військові функції. Крім того, країни все більше усвідомлюють, що використання кіберстратегій може стати основним помножувачем і вирівнювачем сили. Менші країни, які ніколи не могли конкурувати в звичному військовому розумінні зі своїми більшими сусідами, можуть розвинути можливості, які дають їм стратегічну перевагу, якщо їх правильно використовувати. Вхідні витрати на ведення кібервійни досить скромні. Тому не дивно, що країни, які не так залежать від високих технологій у своїх військових структурах, вважають таку залежність потенційною «Ахіллесовою п'ятою» своїх ворогів.

Розвинені, постіндустріальні суспільства та економіки критично залежать від взаємопов'язаних комп'ютерних інформаційних та комунікаційних систем. Витонченість сама стала формою вразливості для використання ворогами. Порушення цивільної інфраструктури є привабливим варіантом для країн і недержавних суб'єктів, які хочуть брати участь в асиметричній війні та не мають можливості конкурувати на традиційному полі бою.

Але війна, зазвичай, визначається як застосування сили або насильства національною державою, щоб змусити іншу державу виконати її волю. Військовий конфлікт є способом досягнення національними державами своїх політичних цілей, коли інші засоби, такі як дипломатія, не працюють або менш доцільні, ніж насильство. Однак, застосування сили може бути менш очевидним у новому бойовому просторі, що складається з бітів і байтів, де

кордони між країнами розмиті, зброю набагато важче виявити, а солдатів можна легко замаскувати під цивільних. Важко уявити собі кібервійну, оскільки в історії бракує досвіду з кіберконфліктів. Немає минулого, з якого можна вчитися, а тим більше уявляти, як боротися з кіберконфліктом на національному рівні. Збільшення й ускладнення невизначеності щодо кібервійни — це проблеми, які випливають із природи кіберпростору, уразливостей, які постійно зростають, що уможливлюють кібератаки, а також основних проблем, невизначеностей та додаткових проблем кібервійни.

Висновки до другого розділу

З усього вище зазначеного стає зрозумілим, що інформаційна війна не менш складна, ніж традиційна. Вона включає багато різних засобів, технік, видів зброї та захисту. Аналіз інструментального набору ведення інформаційної війни може допомогти у розробці реальних планів щодо того, як боротися з загрозами, які перманентно виникають у політико-інформаційному полі. Окрім цього, важливо пам’ятати, що більшість інструментів, проаналізованих у даному дослідженні, дають змогу проводити у життя не тільки ефективну атакуючу стратегію, але й захисну.

Попри те, що інформаційна війна має відмінні ознаки та інструментарій від кінетичного аналогу, вона має спиратися на продуману стратегію як загальний план організаційних заходів. При цьому стратегія інформаційної війни має перманентно піддаватися моніторингу, оцінці та рафінуванню, адже її контексту властиві швидкі зміни та модернізація.

Одна з форм інформаційної війни – кібервійна – вирізняється динамічним розвитком та масштабуванням. Імовірно, найближчими роками вона стане домінуючою формою через низку причин економічного, географічного, політичного, технологічного порядку тощо. Загрози та уразливості національних систем безпеки перед кібератаками спричинюють необхідність більш глибоко вивчення проблеми. Для нас осягнення суті кібервійни набуває

логічності та комплексності в результаті розкриття каузальності між такими феноменами, як кіберпростір, кіберсила та кіберстратегія.

Список використаних джерел до другого розділу

1. Андрусова Т., Гомонова Ю. Информационное оружие и информационные войны. URL: file:///C:/Users/908/Downloads/informatsionnoe-oruzhie-i-informatsionnye-voyny.pdf.

2. Арзуманян Р. В. Кромка хаоса. Сложное мышление и сеть: парадигманелинейности и среда безопасности XXI века. Москва: «Регнум», 2012. 600с.

3. Архипова Є. О. Теоретична сутність та практика використанняасиметричної відповіді в умовах гібридної агресії. Інвестиції: практикатадосвід. 2016. № 24. С. 125-129.

4. Балабін В. В. Концептуальні засади захисту системи інформаційно-аналітичного забезпечення авдань інформаційної боротьби як складової воєнної безпеки / В.В. Балабін, І.В. Замаруєва , І.В. Пампуха // Вісник КНУ ім. Тараса Шевченка. Військовоспеціальні науки, №22, 2009. – С. 30-33.

5. Бебик В. М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблік рилейшнз: монографія. URL: https://studentbooks.com.ua/content/view/1028/42/

6. Бежевець А. М. Правовий статус роботів: проблемита перспектививизначення. Інформація і право. 2019. № 1. С. 61-67.

7. Білобородов О. О., Довгополий А. С. Технології інформаційно-психологічних війн та інформаційно-психологічна зброя. Озброєннятавійськова техніка. 2019. № 4.

8. Близнюк А.С. Пропаганда та контрпропаганда в умовахсучасноїгібридної війни. Наукові записки Інституту журналістики. 2015. Т. 60. С. 49-54.

9. Бурик З. Генеза понятійно-категоріального апарату стратегічного управління. URL: http://www.dridu.dp.ua/zbirnik/2014-01(11)/2.pdf.

10. Бутузов В. М., Тітуніна К. В. Сучасні загрози: комп'ютерний тероризм. Боротьба з організованою злочинністю і корупцією(теоріяіпрактика). 2007. Вип. 17. С. 316-324.

11. Висоцька О.Є. Пропагандистські технології як інструменти здійснення інформаційних війн в контексті комунікативної політикидержави. VМіжнародна наукова конференція Харківського національного університетуПовітряних Сил імені Івана Кожудуба «Сучасна війна: гуманітарнийаспект» : збірник матеріалів, 25-26 травня 2021 року. Харків: Факт, 2021. С. 56-62.

12. Геращенко О. С. Кібертероризм як фактор загрозинаціональнійбезпеці України: генеза поняття та шляхи протидії. Південноукраїнський правничий часопис. 2016. № 3-4. С. 39-42.

13. Гіда О. Ф. Соціальні мережі як засіб деструктивних впливів через інформаційний простір. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2013. № 3. С. 268-278.

14. Гриник Р. О., Пилипенко В. М. Кібертероризм як нова форма міжнародного тероризму. Актуальні задачі та досягнення у галузі кібербезпеки: матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листоп. 2016р. Кропивницький: КНТУ, 2016. С. 61-62.

15. Довгань Л. Є., Каракай Ю. В., Артеменко Л. П. Стратегічне управління. К., 2011. 440 с.

16. Запорожець О. Ю. Кризовий комунікативний менеджмент у сфері міжнародних відносин: монографія. К., 2006. 238 с.

17. Зозуля О. Інформаційна зброя як геополітичний чинник та інструмент силової політики. URL: http://academy.gov.ua/ej/ej18/PDF/12.pdf.

18. Зубарєва М. А. Прикладні антикризові PR-технології. Острог: Видавництво Національного університету «Острозька академія», 2014. 162 с.

19. Карлофф Б. Деловая стратегия: концепция, содержание, символы. М.: Экономика, 1991. 235 с.

20. Квинт В. К истокам теории стратегии. 200-летие издания теоретической работы генерала Жомини. Санкт-Петербург, ИПЦ СЗиу, 2017. 52 с.

21. Коробанов Ю. М., Коробанов А. Ю. Теорія і практика комунікацій: у 3 ч. Ч. 2. Комунікації в теорії прийняття рішень та в кризових ситуаціях. Миколаїв: НУК, 2010. 72 с.

22. Курбан О. В. Діагностика та моделювання PR-процесів: монографія. К.: Українська конференція журналістів, 2012. 160 с.

23. Левин А. Особенности и виды информационных войн. URL: file:///C:/Users/908/Downloads/osobennosti-i-vidy-informatsionnyh-voyn%20(1).pdf.

24. Мак-Квейл Д. Теорія масової комунікації [Пер. з англ. О. Возьна, Г. Сташків]. Львів: Літопис, 2010. 538 с.

25. Міждисциплінарний словник з менеджменту / Д. М. Черваньов, О. І. Жилінська, М. В. Петровський та ін.; за ред. Д. М. Черваньова, О. І. Жилінської. К.: Нічлава, 2011. 624 с.

26. Нежданов И. Технологии информационных войн в интернете. URL: http://bash.rosmu.ru/activity/attach/events/1283/01.pdf.

27. О'Коннор Дж., Мак-Дермот Я. Принципи НЛП. Библиотека Мета. URL: http://lib.meta.ua/book/11934/#

28. Пашенцев Е. Коммуникационный менеджмент и стратегическая коммуникация. М.: МЦСПИК, 2012. 396 с.

29. Расторгуев С. Формула информационной войны. URL: http://www.rc-analitik.ru/file/%7B76a67493-79d7-450b-be1d-87c430f27d0f%7D.

30. Расторгуев С.П. Философия информационной войны / С.П. Расторгуев. – М.: МПСИ, 2003 – 496 с.

31. Рось А. О. Концептуальні засади моделювання інформаційної боротьби / А.О. Рось, І.В. Замаруєва, В.Л. Петров // Наука і оборона, 2000, №2. – С. 47-53.

32. Рудаков А. Стратегия информационной войны. URL: http://elibrary.bsu.edu.az/files/books_aysel/N_317.pdf.

33. Стадник А. Інформаційна війна як комунікативна технологія впливу на масову свідомість та громадську думку. URL: file:///C:/Users/908/Downloads/340-Article%20Text-645-1-10-20161017.pdf.

34. Томпсон А. А., Стрикленд А. Дж. Стратегический менеджмент: искусство разработки и реализации стратеги: пер. с англ. М.: Банки и биржи, ЮНИТИ, 1998. 576 с.

35. Харченко І., Сапогов С., Шамраєва В., Новікова Л. Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу. URL: file:///C:/Users/908/Downloads/9974-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-19803-1-10-20171219.pdf.

36. Хорошко В.О. Особливості застосування сучасної інформаційної зброї / В.О. Хорошко, Т.І. Козел, О.О. Ярошенко // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. Вип 1(29), 2015. – С. 9-15.

37. Хорошко В.О. Концепція застосування інформаційних впливів та протидії інформаційній зброї / В.О. Хорошко, Ю.Є. Хохлачова, М.І. Прокофьєв // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – Вип. 1(31), 2016. – С. 9-24.

38. Чистоклетов Л. Г. Інформаційно-психологічні впливи як невід'ємна складова парадигми інформаційної безпеки / Л. Г. Чистоклетов, В. Й. Шишко // Науковий вісник Львівського державного університету внутрішніх справ. – 2012. – С. 183–192.

39. Шклярук М. Г. Стратегічні комунікації у системі державного управління: дис. ... кан. наук із держ. управління: 25.00.02 / Міжрегіональна академія управління персоналом. К., 2018. 226 с. URL: https://drive.google.com/file/d/1x-T18lR71vrdqXpyQtA2B0EwPRrLsW0J/view

40. Шуляк Н. Інформаційні війни в інтеграційних процесах / Назарій Шуляк // Міжнародні інтеграційні процеси: історичний досвід, сучасні виклики та перспективи . – С. 44–46.

41. Юськів Б. М. Опорний конспект лекцій з дисципліни “Інформаційні війни” / Б. М. Юськів. – Рівне: РІС КСУ, 2003. – 55 с.

42. Яворська Г.М. Гібридна війна як дискурсивний конструкт. Стратегічні пріоритети. Сер.: Політика. 2016. №4 (41). С. 41-48.

43. Alberts D. Defensive Information Warfare. URL: http://www.dodccrp.org/files/Alberts_Defensive.pdf.

44. Ansoff I. The State of Practice Planning Systems. Sloan Management Review, 1977. Winter, p. 1–24.

45. Arquilla J., Ronfeldt D. Cyberwar Is Coming! Comparative Strategy, Vol. 12, 1993, p.146.

46. Brenner S. Cyberthreats: The Emerging Fault Lines of the Nation State, New York, Oxford University Press, 2009.

47. Campen A. The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. Fairfax, VA, AFCEA International Press, 1992.

48. Clarke R., Knake R. Cyber War: The Next Threat to National Security and What to do About it, New York, Ecco, 2010.

49. Coleman K. The Cyber Arms Race Has Begun, CSO Online, 28 January 2008.

50. Coughlan S. Is there a common understanding of what constitutes cyber warfare? The University of Birmingham School of Politics and International Studies, 30 September 2003, p. 2.

51. Definitions for national strategy and strategy, respectively. Department of Defense, ashington, D.C., U.S. Government Printing Office, 1997.

52. Deptula D. Firing for effect: change in the nature of warfare. Firing for effect: change in the nature of warfare, 1995. 23 p.

53. Dolman E. Pure Strategy: Power and Principle in the Space and Information Age, London, Frank Cass, 2005.

54. Doyle P. Marketing Management and Strategy. Pearson Education Limited, 2006. 464 p.

55. Dunnigan J. The Next War Zone: Confronting the Global Threat of Cyberterrorism, New York, Citadel Press, 2002, p. 11.

56. Eriksson A. Viewpoint: Information Warfare: Hype or Reality? URL: https://www.nonproliferation.org/wp-content/uploads/npr/eriksss63.pdf.

57. Information warfare: planning the campaign. URL: https://irp.fas.org/threat/cyber/96-124.pdf.

58. Kopp C. The four strategies of information warfare and their applications. IO Journal, 2010. 1(4), p. 28 - 33.

59. Kuehl D. From Cyberspace to Cyberpower: Defining the Problem. Cyberpower and National Security, Washington D.C., National Defense University Press, Potomac Books, 2009.

60. Lewis J., Timlin K. Cybersecurity and Cyberwarfare 2011, Washington D.C., CSIS, UNIDIR Resources, 2011.

61. Libicki M. What is Information Warfare? Washington, National Defense University, 1995.

62. Libicki M. Conquest in Cyberspace: National Security and Information Warfare, New York, Cambridge University Press, 2007.

63. Lloyd M. The Art of Military Deception. London, Leo Cooper, 1997.

64. Lonsdale D. The Nature of War in the Information Age: Clausewitzian Future, London, Frank Cass, 2005.

65. Molander R., Riddile A., Wilson P. Strategic information warfare : a new face of war. URL: https://www.jstor.org/stable/10.7249/mr661osd.

66. NATO Allied Joint Publication (AJP) 3.10, Allied Joint Doctrine for Information Operations, 23 November 2009.

67. Nye J. Cyber Power, Cambridge, Harvard Kennedy School, Belfer Center for Science and International Affairs, May 2010, p. 3.

68. Rattray G. An Environmental Approach to Understanding Cyberpower. Cyberpower and National Security, Dullas, VA, Potomac Books, 2009.

69. Singh A. Information Warfare: Reshaping Traditional Perceptions. URL: http://www.idsa-india.org/an-mar-4.html.

70. Sommer P., Brown Ian. Reducing Systemic Cybersecurity Risks. OECD, OECD/IFP Project on Future Global Shocks, 14 January 2011, pp. 6-13.

71. Sulaiman R. Information Warfare. URL: https://www.giac.org/paper/gsec/1870/information-warfare/103284.

72. Sullivan G. War in the Information Age. URL: https://www.files.ethz.ch/isn/109690/War_Information_Age.pdf.

73. UN Security Council, Resolution 1113 (2011), 5 March 2011.

74. Williamson M., Knoz K. M. The Making of Strategy: Rulers, States and War, Cambridge, NY: Cambridge University Press, 1994.

75. Wingfield T. The Law of Information Conflict: National Security Law in Cyberspace, Aegis Research Corp., 2000.

РОЗДІЛ 3

ІНФОРМАЦІЙНІ ЗАСОБИ ПРОТИДІЇ ПОЛІТИЧНОМУ НАСИЛЛЮ В СУЧАСНИХ УМОВАХ

3.1 Міжнародний досвід боротьби з політичним насиллям засобами інформаційної війни

Російська інформаційна війна не є ізольованою загрозою лише для України, Європи чи США, це скоріше глобальна стратегія, яка впливає на кожен регіон світу різною мірою залежно від його розміру, маси та складності. Російський підхід до інформаційної війни є цілісним і включає як кібер-удари, так і інформаційні операції як об'єднані елементи, які працюють у тандемі для досягнення цілей російської зовнішньої політики [17]. Крім того, російський підхід має на меті підірвати не лише збройні сили супротивника, а й впливати на сприйняття цільового населення інформації на користь російських інтересів.

Хоча кібератаки стали можливими лише в 1990-х роках, інформаційні операції є набагато давнішою практикою, яку Кремль давно використовує для досягнення своїх цілей. Радянські лідери розуміли цінність інформації та те, як її можна використати для впливу на маси як вдома, так і за кордоном [28]. Згодом Російська Федерація почала використовувати Інтернет для підвищення ефективності інформаційної війни у недорогий спосіб.

Щоб зрозуміти продуктивність Росії в кіберпросторі, важливо усвідомити, що сприйняття загроз - як фізичних, так і ідеологічних - разом з історією Росії, сильно впливають на зовнішню політику Росії в кіберпросторі. Росія потерпає від ситуації, якої незнайомої багатьом іншим європейським країнам: відсутність природних географічних бар'єрів, які вона може використовувати для захисту. Це була постійна проблема, з якою стикався кожен лідер. Перший цар Іван IV реалізував ідею нападу як гарного захисту,

ідею, яка буде керувати майбутніми поколіннями російських і радянських лідерів у зовнішній політиці [38]. Те, чого Росії не вистачало в географічній обороні, вона створила, розширюючи в усіх напрямках, утворюючи буферну зону. Історія неодноразових вторгнень іноземних супротивників була використана для виправдання цієї агресивної наступальної стратегії.

Географічну проблему перетинає та посилює уявлення про те, що Росія замкнена у жорсткій конкуренції із Заходом, і що її дії мають оборонний характер. Ставлення та дії очолюваної США коаліції щодо Росії змусили російських стратегів вважати, що вони в облозі [14]. Ця облога проявляється як у фізичній, так і в ідеологічній формі. Перше можна побачити в таких подіях, як війна в Косово або вторгнення західних наднаціональних демократичних інституцій, таких як ЄС і особливо НАТО, у традиційну зону впливу Росії. Ідеологічно російські стратеги розглядають поширення ліберальних норм, що виходять із Заходу, як дедалі більш проблематичний виклик суверенітету Москви [9]. Політики вважають, що Захід використовує пропаганду для підриву внутрішньої безпеки Росії. Наприклад, вони вірять у причетність Заходу до кольорових революцій, протестів після переобрання Путіна у 2012 році та антирадянських настроїв у країнах Балтії.

На додаток до цих передбачуваних загроз, дії Росії можна частково пояснити іншим розумінням війни. У той час як американські військові мають концепцію «нульової фази», російські стратеги розглядають себе у межах постійного і затяжного конфлікту [14]. Це особливо стосується кіберпростору, де стратегія «політичної війни» радянських часів послужила основою для нинішньої російської стратегії інформаційної війни. Викладене прусським генералом Карлом фон Клаузевіцем розуміння «політичної війни», як уявлення про те, що країна повинна робити все, що в її силах, у мирний час для просування цілей своєї національної політики, знайшло відображення в міжнародній інформаційній практиці РФ [14]. У цьому контексті Російська Федерація працює над покращенням своїх можливостей, щоб домінувати в кіберпросторі за кордоном.

Не менш важлива довга історія Росії як глобальної наддержави. Після розпаду Радянського Союзу та подальшого ослаблення російського впливу на світовій арені Росія тепер бачить себе як відновлюючу силу і сподівається відновити світовий престиж, який колись був у Радянського Союзу. Росія сподівається досягти цього, співпрацюючи з іншими державами, щоб створити новий поліцентричний світ і утвердитися як могутній гравець із центральною роллю у глобальних конфліктах. Розширення глобальної продуктивності Росії також має сприяти збільшенню популярності Путіна. Нарешті, російські мотиви можна віднести до внутрішніх справ Росії та потреби відвернути увагу населення від цих нагальних проблем.

Хоча Росія знаходиться у стратегічно невигідному становищі по відношенню до США та їх союзників, вона використовує асиметричні інструменти у своєму арсеналі, щоб продовжити нарощувати свою вагу та знову стати глобальним гравцем. Одним із таких інструментів є інформаційна війна, яка є дешевим і ефективним способом досягнення російської зовнішньої політики за кордоном.

Російські кампанії інформаційної війни впливали на демократії, пропагували екстремізм і невдоволення, підтримували антидемократичних лідерів, намагаючись похитнути вплив Заходу. Російські стратегії збігаються в багатьох країнах і можуть служити різним цілям. Однак, є три чіткі загальні цілі:

- відновлення російського домінування в пострадянській/імперській сфері впливу;
- зменшення впливу західних демократичних цінностей, інститутів та систем з метою створення поліцентричної моделі світу;
- розширення політичної, економічної та військової гегемонії Росії в усьому світі, щоб зміцнити місце РФ як великої держави.

Для досягнення цих цілей Росія покладається на хакерів, свою все більш потужну розвідувальну спільноту, використання державних ЗМІ (наприклад, Russia Today або RT і Sputnik), ферми тролів і ботів [52].

Хоча Російська Федерація має все більш глобальні прагнення, інформаційна війна використовується, насамперед, для встановлення російського домінування в її колишній зоні впливу, яка включає колишні радянські та комуністичні республіки та території, які раніше входили до складу Російської імперії або перебували під її впливом.

До масштабного вторгнення в Україну, РФ брала участь у так званій «війні нового покоління», що використовує будь-які методи примусу, крім відкритої звичайної війни, включаючи інформаційну війну, політичний тиск та економічний тиск. Ця стратегія застосовувалася в надії, що Росія зможе змусити НАТО сповільнити або навіть змінити свій вплив і розширення в російському «ближньому зарубіжжі».

Держави та території, на які нападають, надзвичайно вразливі для російської інформаційної війни через свої історичні, політичні, економічні, культурні, етнічні та релігійні зв'язки з Росією, а також проблеми з корупцією та економічні труднощі.

Крім того, Росія використовує заморожені конфлікти в кількох країнах (Грузія, Азербайджан та Молдова) для владного впливу в цих регіонах [50]. Російські інформаційні кампанії спрямовані на загострення напруженості, сприяючи проросійським настроям у цих регіонах, використовуючи для цього молодий статус політичних систем і демократичних процесів багатьох цих країн. Росія сподівається на подальшу стагнацію розвитку в цих регіонах і гальмування їх руху до традиційно західних форм демократичного правління. Ці регіони також служили полігоном для випробувань тактики, яку згодом застосовувала Російська Федерація в інших країнах світу.

На тлі нових і триваючих глобальних проблем і конфліктів Росія хоче залишатися на передовій у створенні та реалізації можливих рішень. Кремль вважає, що США та їхні союзники постійно працюють над ізоляцією Росії та підривом російських інтересів. Політика Росії не лише повідомляє про відповідальність за захист своїх громадян і російської культури, а й бореться з однополярною системою, очолюваною США, і намагається переконати інших

робити те ж саме. На практиці Росія використовує цю стратегію для виправдання своїх операцій за кордоном. Як противник порядку, орієнтованого на США, Росія виявляє себе свого роду героєм для тих, хто розчарований однополярною системою, очолюваною США.

Аналіз відомих російських інформаційних операцій у західних демократіях висвітлює три ключові загальні цілі: дискредитувати довірені демократичні інституції; розколоти західну коаліцію та підірвати наднаціональні організації, які підтримують і пропагують ці демократичні цінності [47]. Після короткого періоду демократії в 1990-х, який збігся з національним збентеженням, високим рівнем бідності, широко розповсюдженою корупцією, війною та нестабільністю, В. Путін відновив країну без основ демократії. Сучасна Росія дає модель альтернативної форми правління, яка орієнтована на інформаційний суверенітет і пропагує традиціоналізм, націоналізм та авторитаризм. Західні ідеали та демократичні цінності, природно, суперечать власному більш автократичному баченню В. Путіна. Нинішній міжнародний порядок, який підтримується США та їх союзниками, критично ставиться до сучасної Росії та є єдиною перешкодою здатності Путіна реалізувати свій порядок денний вдома та за кордоном.

У більшості західних демократій расизм і страх щодо імміграції створюють сприятливий грунт для маніпуляцій. Зокрема на ці побоювання були спрямовані російські інформаційні кампанії, щоб вплинути на результати виборів [31]. Європейські демократії та США стикаються з усіма формами інформаційної війни, а вільні та чесні вибори є постійною мішенню. Росія сподівається радикалізувати населення в цих країнах, створивши не лише нестабільність і поляризацію, а й слабкі уряди. Великі наднаціональні блоки, такі як ЄС, можуть мати різкий вплив на економіку Росії, впроваджуючи санкції та формуючи колективний фронт проти потенційних військових дій. З цієї причини велика частина загальної міжнародної політики Росії зосереджена на порушенні єдності між західними демократіями.

Повернення глобального впливу та престижу, які колись мали Радянський Союз та Російська імперія, є ключовим пріоритетом для В. Путіна. Під його наглядом Росія намагалася довести західній коаліції, що вторгнення в історичну сферу впливу Росії не буде допускатися. Зовсім недавно В. Путін звернув свій погляд на регіони світу, де Росія була відсутня після розпаду Радянського Союзу. Росія розширила свої операції на Близькому Сході, в Латинській Америці, Азії та Африці. У порівнянні з операціями Росії в ближньому зарубіжжі, де її стратегічні та економічні інтереси є більш очевидними, ці далекі території можна не враховувати як неважливі для російського режиму [46]. Однак, для В. Путіна ця глобальна експансія служить трьом ключовим цілям. По-перше, він служить підриву ліберального порядку, очолюваного США/Заходом, і цінностей, які вони пропагує (економічна відкритість, демократична підзвітність, верховенство права тощо). Виходячи з першої, друга ціль має на меті залучити більше країн в орбіту Москви, створюючи поліцентричний світ, де Росія є глобальним посередником влади [46]. По-третє, це розширення служить для розгалуження та диверсифікації економічного охоплення Росії, щоб уникнути значної залежності від західних торгових партнерів. Анексія Криму в 2014 році продемонструвала, що санкції США/Заходу можуть мати значний вплив на російську економіку, однак, вони виявилися недостатніми, щоб зупинити країну-агресора від масштабного вторгнення в Україну.

ЗМІ, за якими стоїть російський уряд і які підтримуються російськими тролями та ботами, стали ключовим елементом російської кампанії інформаційної війни. Вони працюють над просуванням версії світових подій, яка відповідає цілям зовнішньої політики Росії, підриваючи як міжнародну систему після холодної війни, в якій домінував Захід, так і глобальні демократичні інститути. Вони допомогли посилити екстремізм по обидва боки політичного спектру і цілеспрямовано працювали, щоб допомогти в зовнішніх операціях Росії.

Ця медіа-машина має другу, більш зловісну мету. Вона прагне не тільки надати альтернативну розповідь з російською версією подій, але й викликати загальну плутанину та поставити під сумнів саме поняття істини [49]. Російський дискурс пропонує різні розповіді про події, які сприяють розбрату та плутанині.

Політичні актори з усього світу почали використовувати російський набір інструментів дезінформації для просування власних планів і наративів. Існує тенденція зростання недовіри до традиційних джерел ЗМІ, що призводить до розмивання фактів і появі вигадок [49]. Це у свою чергу, закладає платформу для кандидатів-популістів у багатьох країнах для націлювання на вільну пресу та підриває якісну журналістику.

RT і Sputnik знаходяться в авангарді російської міжнародної медіа-машини. Вони дотримуються програми Кремля, спрямованої на сіяння розбрату та сприяння настроям, які сприяють Росії або якимось чином підтримують цілі чи політичну позицію Кремля. RT надає послуги арабською, англійською, французькою та іспанською мовами. Вони також надають друковані новини арабською, англійською, французькою, німецькою, російською та іспанською мовами.

Глобальна доступність RT може ввести в оману, оскільки цього каналу щотижня набагато менше глядачів, ніж у CNN або BBC. Sputnik – це ще одна група, яка складає потужну російську міжнародну медіа-машину. Sputnik також подає друковану інформацію та доступний 32 мовами.

Незважаючи на обмежену кількість прихильників у традиційному розумінні, RT і Sputnik зуміли створити платформу для антиістеблішментських, популістських діячів. Вони також досягли певного успіху в новому кліматі соціальних мереж: статтями RT і Sputnik ділилися на таких платформах, як Twitter, Facebook та YouTube. Росія змогла створити високоефективну пропагандистську машину, а платформи соціальних медіа дозволили підтримуваним Росією ЗМІ поширюватися далі, швидше та для набагато ширшої аудиторії, ніж це було можливо раніше. Вони також активно

використовують невдачі та помилки США та ЄС, намагаючись відвернути увагу від власних дій.

Крім потужного міжнародного медіа-апарату, Росія також використовує «фабрики тролів» для поширення дезінформації через соціальні мережі. Найвідоміша з цих «фабрик тролів» розташована в Санкт-Петербурзі, на якій працюють сотні працівників [49]. «Фабрики тролів» примножують успіх російських дезінформаційних кампаній. Вони співпрацюють з російськими ЗМІ, щоб поширювати неправду та рекламувати будь-які матеріали, які підтримують інтереси Кремля.

Через глобальне охоплення як Інтернету, так і російських ЗМІ, є мало місць, де б не проводилася постійна російська інформаційна кампанія, яка поширює власний наратив про події у світі. У цьому підрозділі проведемо огляд деяких країн, які потерпають від цілеспрямованих російських дезінформаційних кампаній, а також детально розглянемо кілька випадків, щоб показати складність російської дезінформаційної війни.

Вірменія, колишня Радянська Соціалістична Республіка, мала тісні зв’язки як економічно, так і політично з Росією після розпаду Радянського Союзу. Громадська думка Вірменії залишається відповідною геополітичному порядку денному Кремля, і Вірменія вітає участь Росії у внутрішніх та регіональних питаннях. Незважаючи на вагомі докази того, що у Вірменії існує активна російська дезінформаційна кампанія, влада не визнала це як загрозу.

За кілька днів до парламентських виборів у квітні 2017 року відбувся значний сплеск активності тролів і ботів. Це включало розповсюдження фальсифікованого електронного листа USAID, який натякав, що США втручаються у вибори Вірменії. Документ оприлюднили в російськомовних акаунтах у Twitter. Хоча документ було розвінчано посольством США в Єревані, він був виправлений і знову опублікований у Twitter разом з оригінальним документом перед виборами 2017 року [39]. Це допомогло Кремлю досягти мети зобразити США як загрозу.

І Болгарія, і Молдова є двома сучасними державами, які залишаються тісно пов’язаними зі своїм радянським минулим. Російські дезінформаційні кампанії вплинули на обидві сторони політичного спектру в регіоні. У Болгарії ліва проросійська Болгарська соціалістична партія отримує підтримку через проросійські та антизахідні кампанії в соціальних мережах, здійснювані російськими та болгарськими джерелами. Так само, в Молдові проросійську Партію соціалістів підтримують російські соціальні мережі та медіа-кампанії. Болгарія є членом ЄС, але все ще стикається з високим рівнем корупції. Крім того, в уряді Болгарії багато людей, які пропагують проросійський порядок денний і використовують ідеалізовану пам’ять про своє комуністичне минуле.

Молдова має тісні зв'язки з Росією як в культурному, так і в економічному плані та має заморожений конфлікт у східній частині країни. Обидві країни все ще мають значну внутрішню підтримку російських ідеологій та політики, що можна пояснити спільною історією, культурою та релігією, а також ідеологічним успіхом гламуризованої радянської/комуністичної історії. Проте Росія все ще займається просуванням дезінформації через джерела ЗМІ цих країн. Ця техніка використовується для того, щоб відволікти увагу від внутрішніх проблем, звернувши на зовнішні, зберегти населення розділеним, а економіку — у стагнації.

Є вагомі докази того, що російська інформаційна операція була здійснена під час президентських виборів у Чехії на початку 2018 року. Після попереднього раунду голосування Росія розпочала кампанію дезінформації, зображаючи проєвропейського кандидата Й. Драгоша педофілом, який відкриватиме Чехію для небезпечної імміграції, ефективно використовуючи при цьому тактику розпалювання ксенофобських настроїв, щоб допомогти чинному кандидату М. Земану перемогти у другому турі голосування. Таким чином, проросійський, антиєвропейський та націоналістичний кандидат знову був обраний президентом.

Таке ефективне використання дезінформації можна знайти і в сусідніх країнах – Угорщині, Польщі та Словаччині [29]. Використовуючи побоювання

повної імміграції та упередження щодо тих, хто переважно прибуває з ісламських країн, Росія змогла розпалити страх і сприяти екстремізму в Центральній Європі, ефективно впливаючи на вибори по всій Європі.

Останніми роками шведська влада спостерігає зростання російських інформаційних операцій, спрямованих на поляризацію шведського суспільства, спроби підірвати стабільність та поширення неправдивих новин. Росія також користується побоюваннями багатьох європейських країн щодо імміграції. В. Путін використовує ці страхи і використовує Швецію як приклад нестабільної країни. Російські медіа-гіганти RT і Sputnik разом з російськими тролями ведуть такий діалог.

Росія сподівається використати Швецію як приклад, щоб посилити побоювання імміграції в інші європейські країни, щоб посилити антизахідну, націоналістичну та антиінтеграційну політику. Як і в інших випадках, Росія сподівається послабити демократичні інститути Швеції та підштовхнути до радикальної політики в країні.

Франція є одним із засновників Європейського економічного союзу (попередника ЄС) у 1957 році та НАТО в 1949 році. Нині Франція є однією з найпотужніших держав Європи у військовому та економічному плані, а її центральне положення як в ЄС, так і в НАТО робить її логічною метою для Росії. Як і в решті Європи, у Франції з 1980-х років відбулося зростання націоналістичної та антиєвропейської риторики. Цей політичний клімат є благодатним ґрунтом для російської інформаційної війни.

Вибори у Франції 2017 року, як і вибори 2016 року в США, були сповнені російського втручання. Е. Макрон, центристський кандидат у президенти, став мішенню хакерів, які використовували фішинг разом із фальшивими акаунтами у Facebook, щоб отримати інформацію про нього. Велика кількість цієї інформації була оприлюднена за півтора дня до виборів [15]. Крім того, московська консалтингова фірма зробила неправдиві твердження про опитування. Sputnik France та RT France, французькомовні версії медіа-платформ, контрольованих Кремлем, також були дуже активні в негативному

зображенні Е. Макрона. Російські хакери створили акаунти в Твіттері, націлені на цього кандидата, які проводили наклепницькі кампанії та поширювали фейкові новини, облікові записи, які також були націлені на інших лівих кандидатів. Націлюючись на центральний бастіон порядку після Другої світової війни, Росія сподівалася поставити там до влади кандидата, який виступає проти ЄС, з наміром дестабілізувати ЄС і НАТО.

Причини зростання російського впливу в Мексиці та інших регіонах Латинської Америки зосереджені на конфлікті Росії з США. У відповідь на уявне вторгнення США в російське «ближнє зарубіжжя» Росія прагне збільшити свою присутність у традиційній зоні впливу США. Росія прагне розширити свою економіку і створити проблеми для США, посилюючи антиамериканські дії, настрої та нестабільність у країні з тісними економіко-географічними зв'язками.

Росія використовує антиамериканські настрої через інформаційні операції в регіоні. Перед президентськими виборами в Мексиці 2018 року RT en Español (іспаномовна версія Russia Today) набирала обертів. RT en Español пропагував імідж США як загрозу мексиканському суверенітету та підтримував кандидата від демократів і соціалістів Андреса Мануела Лопеса Обрадора, який переміг би на президентських виборах. RT доступний по всій Латинській Америці, а в 2014 році Sputnik запустив іспанське радіо та веб-сервіс новин і розваг, також доступний по всій Латинській Америці.

Росія намагалася посилити свій вплив і у Південно-Східній Азії в політичному та економічному плані. У серпні 2018 року Асоціація держав Південно-Східної Азії майже підписала угоду з Росією щодо інтеграції кібербезпеки, і В. Путін здійснив свій перший візит до Сінгапуру в листопаді 2018 року на саміт організації. Зростаюча продуктивність Росії в інформаційному просторі різко зросла з 2017 року. Наприклад, того року Sputnik підписав меморандум про взаєморозуміння щодо обміну новинами з офіційним інформаційним агентством Малайзії Bernama [18].

На Філіппінах Росія уклала партнерство з поширення інформації разом із кількома іншими угодами. Це включало відправку співробітників державного філіппінського агентства новин до Росії для навчання щодо поширення інформації за допомогою Sputnik. Це посилене співробітництво, особливо щодо засобів масової інформації, може дозволити країнам використовувати російський інструментарій дезінформації, щоб приборкати опозицію та зашкодити демократичним процесам всередині країни.

Були повідомлення про активність тролів і ботів у Facebook на Філіппінах. У січні 2019 року Facebook закрив серію сторінок, пов’язаних з Агентством Інтернет-досліджень. Сторінки посилалися на так званих «експертів», щоб надати їхній фальсифікованій інформації легітимність і довіру. Дії Росії на Філіппінах демонструють бажання В. Путіна підтримувати сильних лідерів авторитарного типу, де б вони не були в світі. Це також демонструє надії Росії розширити зону впливу в нових для себе районах земної кулі.

Також у цьому підрозділі спробуємо описати російську кампанію інформаційної війни у кількох напрямках. Перший пов'язаний із набором даних загальнодоступної інформації про російські кібероперації по всьому світу. Другий - дослідження розширених постійних загроз і їх зв’язку з російськими спецслужбами та військовими.

Останніми роками кібер-дії Росії виявлені в 85 країнах, що охоплюють загалом 6 континентів і 16 регіонів світу: Центральна Америка, Центральна Азія, Східна Африка, Східна Азія, Східна Європа, Північна Америка, Північна Європа, Південна Америка, Південно-Східна Азія, Південна Африка, Південна Азія, Південна Європа, Західна Азія та Західна Європа. Незважаючи на те, що більшість атак зосереджені на Європі та США, ми також бачимо, що регіони, що оточують Росію, є сильною мішенню, включаючи Центральну Азію, Західну Азію, Південну Азію та Східну Азію.

Після розпаду Радянського Союзу розвідувальні обов'язки КДБ були поділені між новоствореними гілками розвідки. Сюди входять Федеральна

служба безпеки (ФСБ), Служба зовнішньої розвідки (СЗР), Федеральна служба охорони (ФСО) і Головне управління Генерального штабу Збройних Сил Російської Федерації (ГУ), більш відоме за назвою з радянських часів — Головне розвідувальне управління (ГРУ). Кожна з цих груп відіграє певну роль у російському кіберпросторі, але обов'язки та юрисдикція Федеральної служби охорони орієнтовані на внутрішнє середовище, і вважається, що вона не пов'язана з якимись російськими кібер-акторами.

ФСБ відповідає за контррозвідку, спостереження та нагляд у Російській Федерації, однак, останнім часом все активніше залучається до закордонних операцій. СЗР здійснює переважно розвідку, використовуючи людський ресурс, а її кібер-здатності не можна порівняти з ФСБ чи ГРУ. Однак, СЗР працює у координації з ФСБ і ГРУ щодо кібероперацій. ГРУ відрізняється від інших спецслужб тим, що це розвідувальна служба російських збройних сил. ГРУ, здається, є найактивнішою групою, яка має доступ до великої кількості ресурсів для підтримки своїх кібероперацій. Вважається, що ГРУ є головною організацією для APT28 і команди Sandworm. ФСБ була пов'язана з більшістю APT, включаючи Turla, APT29, Palmetto Fusion та Gamaredon Group. СЗР була пов'язаний лише з APT29.

Загалом функціонує біля десяти російських груп APT, які відрізняються за приналежністю та діяльністю в закордонних операціях. Щоб визначити, яка група APT відповідальна за конкретну атаку, фірми, що займаються кібербезпекою, використовують різні показники, включаючи поглиблений аналіз використовуваного шкідливого програмного забезпечення та минулих операцій, здійснених цим APT. Важливо зазначити, що значна частина атак не була чітко пов'язана з певною групою APT або відділенням спецслужб. Їхні цілі часто були перехресними, а часом певним чином відрізнялися.

APT28 або Fancy Bear є найвідомішою російською APT групою, і не дарма. У 2015 році APT28 успішно зламала мережі Пентагону, а в 2016 році — Національного комітету Демократичної партії. Організація діє принаймні з 2007 року і, як вважають, пов'язана з ГРУ. Завдяки вищим технологічним і

оперативним можливостям ГРУ спільні масштаби є глобальними. У них є великий набір шкідливих програм, які постійно розвивають і розширюють. Найчастіше організація використовує комбінацію фішингу та реєстрації підроблених доменів, щоб зламати ворожі системи [10].

Операції APT28 присутні майже в кожній частині земної кулі. Хоча вони, як правило, націлені на країни НАТО, за останні кілька років відбувся перехід до більш глобального погляду. Зокрема, зростає кількість кібероперацій, спрямованих на країни Близького Сходу та Східної Азії. Найпоширеніші цілі APT28 включають іноземні уряди та оборонну промисловість. Країни, які є найчастіше атакованими мішеняит – це США, Німеччина, Туреччина, Велика Британія, Катар, Польща, Швейцарія та Чорногорія. Регіони світу — Західна Азія, Західна Європа, Північна Америка, Північна Європа та Східна Європа.

Вважається, що APT28 пов’язаний з КіберБеркутом, який є проросійською групою, яка працює в Україні. Порядок денний КіберБеркуту більше зосереджений на Україні в порівнянні з більш глобальним масштабом його материнської групи APT28.

Вважається, що APT29 або Cosy Bear пов'язаний з СЗР і ФСБ і є однією з найскладніших і добре підтримуваних російських APT. Діяльність APT29 відстежується з 2008 року. У 2015 році організація успішно зламала несекретні мережі Білого дому, Державного департаменту та Об’єднаного комітету начальників штабів США. APT29, схоже, більш обережна у своїй діяльності, ніж інші APT, що ускладнює визначення їхніх кампаній. Крім того, вони мають великий набір шкідливих програм, який постійно розширюють. Вони, як правило, використовують спис-фішинг, щоб зламати цільові мережі [22].

Операції APT29 мають географічно великий обсяг, але найбільше вони представлені в Північній Америці, Північній Європі, Східній Європі, Західній Європі, а також у Східній та Західній Азії. Їхні операції були представлені загалом у 31 країні, найбільш поширеними цілями яких були США, Норвегія, Бельгія, Грузія, Німеччина, Угорщина, Нідерланди, Південна Корея, Іспанія та Україна.

На відміну від інших російських APT, APT29, схоже, збирає розвіддані для підтримки дипломатичних зусиль. APT29 активно націлювалася на Україну до кризи в 2014 році, але згодом там відбулося зниження активності, тому що Україна більше не була актуальною для APT29 у тому самому ключі.

Після здійснення атак на аналітичні центри та неурядові організації США та уряди Норвегії та Нідерландів у 2016 та 2017 роках відповідно, APT29 перебувала у бездіяльності приблизно рік. Однак, APT29 знову з'явилася наприкінці 2018 року з поновленими фішинговими кампаніями, націленими на кілька секторів.

Вважається, що Turla є надзвичайно досконалим учасником загроз і діє з 2004 року. Її активність пов'язується з ФСБ. Як і APT29, цей актор обережний і терплячий у своїх операціях. Деякі експерти кажуть, що програмний код, який використовується Turla, є більш просунутим, ніж той, який використовується в APT28 і APT29. Організація також може мати звязок з кампанією «Червоний жовтень», яка спрямована на дипломатів, військових чиновників і дослідників ядерної галузі.

Цілі Turla переважно пов'язані з урядом і обороною, а за останні шість років їхньою найпоширенішою метою була Німеччина. У 2017 році цей актор зміг проникнути до Департаменту 2 Міністерства закордонних справ Німеччини, який відповідає за зовнішню політику Німеччини як в ЄС, так і з іншими країнами Європи, Північної Америки, Центральної Азії та Росії [13]. Вони також відповідальні за численні кампанії в Швейцарії та Південній Кореї. Виявивлено інтерес до швейцарських оборонних технологій, націлений як на Федеральне міністерство оборони Швейцарії, так і на оборонного підрядника. Turla отримала доступ до 23 ГБ даних про технологію боєприпасів та аерокосмічні технології, включаючи дрони. Turla має цілі по всьому світу. Крім того, що вони присутні в Західній Європі та Східній Азії, вони також активно працюють у Західній Азії, Центральній Азії та Південній Азії.

Вважається, що команда Sandworm є частиною ГРУ, але на відміну від свого аналога APT28, цілі команди Sandworm часто пов'язані з енергетикою.

Команда Sandworm використовує шкідливе програмне забезпечення, відоме як BlackEnergy, яке вони продовжують оновлювати та використовувати для націлювання на інфраструктуру, пов’язану з енергетикою.

Найбільш активна команда Sandworm Team в Україні. Деякі з їхніх найбільш нищівних атак були у 2015 та 2016 роках, коли команда Sandworm відключила українську електромережу. У 2017 році команда Sandworm запустила одну з найбільш руйнівних атак, відомих на сьогоднішній день, під назвою NotPetya, яка була замаскована під програму-вимагач, яка фактично видаляла інформацію з відповідних систем. NotPetya мав на меті пошкодити українську фінансову систему на тлі конфлікту між Києвом та сепаратистами на Донбасі на сході України.

Команда Sandworm також працювала в інших частинах Східної Європи та Західної Азії. У 2015 році команда Sandworm використала зловмисне програмне забезпечення GreyEnergy, наступника набору інструментів BlackEnergy, для націлювання на польську енергетичну компанію [16]. Команда Sandworm відома тим, що обережно приховує та захищає свою довготривалу присутність за допомогою скомпрометованих систем. Це означає, що майбутні кампанії команди Sandworm можуть бути такими ж, якщо не більш руйнівними, ніж в Україні.

Palmetto Fusion є відносно новою командою APT, яка діє принаймні з 2015 року і, як вважають, пов’язана з ФСБ. Її цілі переважно пов’язані з енергією, хоча про Palmetto Fusion відомо небагато.Вони включають Ірландію, Велику Британію, Туреччину та США. У 2017 році організація націлювалася на атомні електростанції, інші енергетичні об’єкти та виробничі підприємства в США. Фірма з кібербезпеки Dragos з помірною впевненістю визначила, що Palmetto Fusion має готовий доступ для зриву електричних мереж і розуміє середовище, необхідне для розвитку руйнівних можливостей серед своїх заражених цілей [19].

Gamaredon Group є менш відомим глобальним загрозливим актором, який, як вважають, пов'язаний з ФСБ і націленим на державні установи в

Україні. У 2018 році Gamaredon Group розпочала скоординовані кібератаки на українські державні установи за кілька днів до захоплення Росією українських кораблів і моряків в Азовському морі.

3.2 Особливості захисту інформаційної сфери України в умовах інформаційної війни як засобу протидії політичному насиллю

У контексті гібридної війни особливої значущості набуває актуальне законодавство, що визначає правові засади функціонування інформаційного простору, захисту інформації, взаємодії інформаційних акторів тощо. У межах відкритого воєнного протистояння значення політико-правового регулювання інформаційної царини подвоюється, адже активність супротивника підвищується, і інформаційні засоби можуть використовуватися ворогом для координації кінетичних активностей. Саме тому, вважаємо доцільним проаналізувати особливості політико-правового захисту інформаційної сфери в Україні.

Отже, сьогодні в Україні інформаційна безпека вибудовується на низці законодавчих актів, нормативно-правових актів та нормативних актів щодо захисту інформації, зокрема, варто виділити наступні: Закон України «Про інформацію» від 02.10.1992 № 2657-XII; Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР; Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII; Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI; Постанову Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373; Постанову Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736 тощо.

Окрім вище зазначених Законів України та Постанов КМУ, створення і функціонування Комплексної системи захисту інформації (КСЗІ) регламентується нормативними документами в галузі технічного захисту інформації (НД ТЗІ) та державними стандартами України (ДСТУ). НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі, Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96, НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу, НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу – це далеко неповний перелік нормативної документації та стандартів, визначених державою задля технологічного забезпечення захисту інформації.

Аналіз відповідного комплексу законодавчих актів, нормативно-правових актів та нормативної документації дозволяє зробити висновок про те, що основними принципами інформаційної безпеки України є:

- верховенство права;
- пріоритет захисту прав і свобод людини, що стосуються інформації;
- своєчасний і адекватний захист життєво важливих національних інтересів від реальних і потенційних загроз інформаційній безпеці;
- захист інформаційного суверенітету України;
- свобода думки, свобода слова і вільне вираження думок і переконань;
- свобода збору, зберігання, використання та поширення інформації;
- захист від втручання в приватне та сімейне життя фізичної особи;
- доступ до інформації лише на підставі закону;
- узгодження особистих, громадських і національних інтересів, відповідальності всього українського народу для забезпечення інформаційної безпеки;

- розмежування повноважень, взаємодії та відповідальності державних та недержавних спеціалістів з інформаційної безпеки;

- пріоритет розвитку та розширення інформаційних технологій, продуктів і послуг, постійне вдосконалення каналів передачі інформації в кількісному та технічному аспектах;

- застосування міжнародних та колективних систем безпеки та механізмів забезпечення інформаційної безпеки України;

- гармонізація інформаційного законодавства з нормами міжнародного права та нормативними актами ЄС;

- захист інформаційного суверенітету, національного суверенітету, конституційного ладу та територіальної цілісності України;

- конструювання української ідентичності в інформаційному просторі, яка є невід'ємною частиною політико-соціального дискурсу;

- побудова подвійної системи суспільного обслуговування та комерційного мовлення;

- сприяння розвитку контенту в інформаційному просторі для захисту та охорони загальнолюдських цінностей, а також інтелектуального, духовного і культурного потенціалу українського народу тощо.

Основним напрямком державної політики з інформаційної безпеки є задоволення та захист життєво важливих інформаційних інтересів та потреб особи, громадянина, суспільства та держави, насамперед, в частині виробництва, споживання, поширення та розвитку національного стратегічного змісту та інформації в інтересах громадянина, суспільства і держави, а також - функціонування та безпеки кібернетичних, телекомунікаційних та інших автоматизованих комп'ютерних систем, що становлять інфраструктурну основу національного інформаційного простору.

Провідними фокусними точками державної політики з інформаційної безпеки України є:

- дотримання балансу між суворим виконанням конституційних прав і свобод особи щодо інформації, зокрема свободи слова, та реалізації державних

функцій щодо запобігання, своєчасного виявлення, усунення чи нейтралізації загроз інформаційній безпеці особи, громадянина, суспільства та держави;

- створення нормативної бази для організації розвитку інформаційного простору та його захисту від зовнішніх загроз та узгодження такої нормативної бази з нормами міжнародного права, вимогами міжнародного співробітництва та стандартами та правилами ЄС;

- розробка та реалізація ефективної національної інформаційної політики, спрямованої на розвиток національного інформаційного простору та гармонізацію системи контролю та координації серед практиків національної інформаційної політики та експертів з інформаційної безпеки;

- налагодження співпраці між державою, публічним сектором та приватним сектором, сприяння міжнародному співробітництву з метою реалізації національної інформаційної політики та забезпечення інформаційної безпеки, створення якісного національного інформаційного продукту;

- комплексна допомога, державна підтримка та пріоритетність розробки та розповсюдження національного інформаційного продукту, у тому числі за межами України;

- використання національного інформаційного продукту України для популяризації загальнолюдських цінностей у міжнародному інформаційному середовищі та інформаційного розвитку людства, зокрема обміну баченнями, підходами та механізмами із закордонними партнерами України щодо вирішення сучасних викликів, спричинених деструктивною політикою інших країн та спрямованих на підрив демократичних цінностей та свободи вираження поглядів в інформаційному просторі.

Державна політика України з інформаційної безпеки реалізується з метою запобігання втручанню внутрішніх та зовнішніх загроз інформаційній безпеці у виконання життєво важливих інформаційних інтересів та потреб людини, громадянина, суспільства та держави, що є наріжним каменем сталого розвитку національного інформаційного простору.

Загрозами інформаційній безпеці України є:

- комунікативні загрози щодо задоволення потреб людини, громадянина, суспільства та держави у сфері виробництва, споживання, поширення та розвитку національного стратегічного змісту та інформації;

- технологічні загрози щодо функціонування та безпеки кібернетичних, телекомунікаційних та інших автоматизованих комп'ютерних систем, що утворюють інфраструктурну (технічну, інструментальну) основу національного інформаційного простору.

До комунікативних загроз щодо задоволення потреб людини, громадянина, суспільства та держави щодо виробництва, споживання, поширення та розвитку національного стратегічного змісту та інформації можна віднести:

1) зовнішній негативний інформаційний вплив на людську та суспільну свідомість через засоби масової інформації та Інтернет, що здійснюється на шкоду державі з метою: змінити психічний чи емоційний стан особи, її психологічні та фізіологічні особливості; вплинути на свободу вибору шляхом культивування культури насильства та жорстокості, нахабства та зневаги до людської та національної гідності, розпалювання релігійної, расової чи етнічної ворожнечі та дискримінації за будь-якою ознакою, як-от етнічне походження, мова, релігія тощо; закликів до сепаратизму, повалення конституційного ладу або порушення територіальної цілісності країни;

2) інформаційний вплив на населення України, у тому числі військовослужбовців та мобілізаційного підкріплення, з метою погіршення обороноздатності та підриву іміджу служби в армії;

3) поширення корумпованої, недостовірної та упередженої інформації суб'єктами інформаційної діяльності з метою дискредитації органів державної влади та дестабілізації суспільно-політичної ситуації, що значно ускладнює прийняття політичних рішень, завдає шкоди національним інтересам чи створює негативний імідж України;

4) загрози свободі слова, зокрема втручання власників ЗМІ в редакційну політику; відсутність законодавчої бази для посилення ролі творчих колективів та редакційного персоналу у реалізації редакційної політики засобами масової інформації, як державними, так і приватними; монополії ЗМІ, що дозволяють цілеспрямовано впливати на споживачів інформації; адміністративні та нормативні передумови для обмеження свободи слова та маніпулювання громадською думкою як під зовнішнім впливом, так і з боку внутрішньополітичних організацій, бізнесу та окремих осіб;

5) створення, поширення, передача та зберігання інформації для підтримки або активізації злочинної чи терористичної діяльності.

До технологічних загроз щодо функціонування та безпеки кібернетичних, телекомунікаційних та інших автоматизованих комп'ютерних систем, що становлять інфраструктурну (технічну, інструментальну) основу національного інформаційного простору, можна віднести:

1) використання іноземними державами кіберсил, кіберпідрозділів, нових видів інформаційної зброї та кіберзброї на шкоду Україні;

2) акти кіберзлочинності, кібертероризму чи військової кіберагресії, що становлять загрозу стабільному функціонуванню національних інформаційно-телекомунікаційних систем, що здійснюється шляхом втручання, несанкціонованого доступу або порушення функціонування телекомунікаційних, кібернетичних та автоматизованих комп’ютерних систем, державних або приватних, з метою, зокрема здійснення диверсій або терористичних актів; підтримки або активізації кримінальної, екстремістської чи терористичної діяльності; здійснення деструктивного інформаційного впливу; перехоплення телекомунікацій; електронного заглушення або блокування інформаційних систем, засобів зв'язку та засобів управління з використанням програмного забезпечення та математичних засобів, які порушують функціонування інформаційної системи; додавання прихованих шкідливих функцій до програмних і апаратних засобів тощо;

3) нерозвиненість національної інформаційної інфраструктури, зокрема: залежність національної інформаційної інфраструктури від іноземних виробників високотехнологічної продукції; використання підробленого та несертифікованого програмного забезпечення та обладнання для обробки інформації; невідповідність норм відповідальності за скоєні правопорушення сучасним викликам та загрозам інформаційної безпеки; недостатній захист об’єктів критичної інформаційної інфраструктури України;

4) порушення порядку доступу, збору, обробки, зберігання, поширення чи передачі інформації, що охороняється державою (державна таємниця, конфіденційна інформація, персональні дані, авторські права та інтелектуальна власність) або операції з інформаційними ресурсами, що містять таку інформацію;

5) брак недержавного моніторингу діяльності практиків із інформаційної безпеки та безпеки національної інформаційної інфраструктури та інформаційного простору.

З моменту повномасштабного вторгнення військ РФ на територію України Верховна Рада України прийняла низку законів, які оптимізують захист інформації в умовах воєнного стану. У даному ключі принагідно згадати, зокрема Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції» від 03.03.2022 № 2110-IX (внесення змін до Кримінального кодексу України, Кримінального процесуального кодексу України), Закон України «Про внесення змін до деяких законодавчих актів України (щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора)» від 03.03.2022 № 2109-IX (внесення змін до статті 3 Закону України "Про друковані засоби масової інформації (пресу) в Україні"; статті 21 Закону України "Про політичні партії в Україні"; статті 2 Закону України "Про захист суспільної моралі"; статті 6 Закону України "Про телебачення і радіомовлення"; статті 4 Закону України "Про громадські

об’єднання"), Закон України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності досудового розслідування за "гарячими слідами" та протидії кібератакам» від 15.03.2022 № 2137-IX (внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації"), Закон України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану» від 24.03.2022 № 2160-IX, Постанова Верховної Ради України «Про Заяву Верховної Ради України про цінність свободи слова, гарантії діяльності журналістів і засобів масової інформації під час дії воєнного стану» від 14.04.2022 № 2190-IX тощо.

Окрім цього, 19 березня 2022 року В. Зеленським був підписаний Указ Президента України «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». Згідно цього документу було установлено, «що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об’єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації - цілодобовому інформаційному марафоні "Єдині новини #UAразом"» [7].

Відповідне рішення викликало невдоволення окремих експертів, зокрема М. Княжицького, які побачили у даному кроці обмеження прав телемовлення для великої кількості каналів, окрім "Інтера", Плюсів, "України" та ICTV, які роблять спільний марафон. Однак, насправді, всі телеканали мають можливість повністю або частково долучитися до єдиного

загальнонаціонального телемарафону, при цьому зберігається їх творча свобода. Попри наявність різних, часом суперечливих, точок зору щодо оцінки відповідного рішення, зауважимо, що під час воєнного стану наповнення телеефіру має відбуватися в контексті єдиної інформаційної політики, щодо дозволить транслювати населенню чітку позицію влади, надаватиме лише вивірену інформацію, підтримуватиме оптимістичні настрої та віру у перемогу тощо.

Варто пам’ятати, що діяльність ЗМІ в Україні не обмежується телемовленням, існує велика кількість друкованих та інтернет видань, які щоденно роблять свою роботу. Журналісти працюють в гарячих точках, ризикуючи власним життям з метою зібрати об’єктивну інформацію про найбільш актуальні події воєнного часу. На превеликий жаль, така робота пов’язана з високими ризиками. Відомо, що станом на 12 квітня загинуло 20 медійників, серед яких є і представники іноземних ЗМІ. Серед загиблих журналістів, фотографів, кореспондентів: П'єр Закжевський, Олександра Кувшинова, Олександр Литкін, Павло Лі, Сергій Пущенко, Євген Сакун, Брент Ентоні Рено, Оксана Бауліна, Дилербек Шакіров, Віктор Дідов, Віктор Дудар, Лілія Гумянова, Юрій Олійник, Олег Якунін, Максим Левін, Мантас Кведоравічюс, Сергій Заїковський, Денис Котенко, Євген Баль, Роман Нежиборець [6]. Життєвий шлях цих фахівців і смерть при виконанні роботи є свідченням їх відданості обраному покликанню, найвищим людським цінностям та героїчності.

У той же час, серед медійників є негідні особистості, що відверто висловлюють, пропагують та підтримують злочинні дії РФ на території України. Так, Національне агентство з питань запобігання корупції (НАЗК) та ГО Рух «ЧЕСТНО» внесли до Реєстру державних зрадників перші 100 осіб, серед яких 13 представників медіасфери. Ось імена цих людей: Кирило Вишинський, Ігор Гужва, Сніжана Єгорова, Андрій Єрмолаєв, Світлана Крюкова, Гліб Ляшенко, Оксана Марченко, Олеся Медведєва, Діана Панченко, Михайло Погребинський, Володимир Рогов, Олексій Романов, Олександр

Семченко. Окрім вище перелічених зрадників - один суддя, 73 політики та 13 правоохорнців [5].

На тимчасово окупованих територіях ворог встановлює власне теле- і радіомовлення з метою посилення дезінформації, загострення міжнаціональної ворожнечі, дискредитації української влади. Однак, його пропаганда сягає і підконтрольних Україні територій. Саме тому, уповноважені державні посадовці та політики розробляють своєрідні пам'ятки та комплекси рекомендацій щодо інформаційної гігієни серед населення. Так, Г. Маляр, заступник Міністра оборони України, ще в середині березня 2022 року звернулася до співвітчизників зі сторінки у Фейсбук, зазначивши, що перше правило інформаційної безпеки під час війни - не вірити джерелам інформації ворога. «Не шукайте в інформаційному полі ворога лояльних до України, таких що співчувають, розуміють та засуджують дії російської влади. Нинішні інструменти інформаційної війни дозволяють таких персонажів штучно створювати, або використовувати умовно щирих поза їх волею шляхом професійного впливу на них. Не вірте в акції протесту на центральному російському каналі, програмна сітка якого пишеться в Кремлі. Не вірте ніяким вибаченням, посипанням голови попелом, сльозам, згадуванням про історичне коріння, спільне минуле, місце народження в Україні тощо. Не вірте під час війни публічному засудженню Путіна його співгромадянами. Це може бути засідка. Не вірте під час війни опозиції ворожої країни. Це теж може бути засідка. І вони не повинні любити вашу країну більше за свою, навіть попри диктаторський режим на їх батьківщині. Уявіть, що інформаційне поле заміноване. І щоб у вашу свідомість не потрапила міна сповільненої дії, йдіть лише по дорозі офіційної інформації з українських джерел і не контактуйте з інформацією з території ворога. Ми ж з вами не тільки сильні, але й розумні!» [1].

Враховуючи те, що в сучасному цифровому світі джерелом інформації можуть бути не лише ЗМІ, а й звичайні люди через свої соцмережі та канали у месенджерах, варто пам'ятати та дотримуватися правил інформаційної

безпеки під час війни. Не постити: фото- та відеоматеріали з місцевості, де стався обстріл, або було влучання снаряду; відео з ракетами, які летять; точні координати бойових дій або адреси, де сталися вибухи; фото та відео з розпізнавальними знаками (таблички з назвами станцій метро, автобусними зупинками, вулиць, заводами та підприємствами тощо); українські ПВО за роботою; будь-які дані про ключові військові об'єкти чи інформацію про переміщення ЗСУ; неверифіковану інформацію про загиблих чи поранених; інформацію, непідтверджену офіційними джерелами, органами державної влади; організовувати стріми бомбардувань в прямому етері і т. д.

Натомість, кожен із нас може бути й корисним на інформаційному фронті. Зокрема, розвінчувати фейки, які розповсюджує ворог, нести правду у маси, повідомляти ЗСУ про місце дислокації ворожої техніки та сил ворога, через певний час після атаки оприлюднювати злочини окупантів, але крупним планом тощо.

Очевидно, що сьогодні політико-правовий захист інформації в Україні відбувається з урахуванням зовнішніх і внутрішніх загроз, вирізняється оперативністю та дієвістю, зваженістю та системністю. Державна політика з інформаційної безпеки має стратегічну спрямованість і деталізована продуманими тактичними рішеннями. Лише так можна утримати інформаційну стабільність в середині країни, посилити підтримку України акторами в міжнародному інформаційному полі та захиститися від інформаційних провокацій ворога.

Революція Гідності стала своєрідним тригером протистояння РФ та України у інформаційному просторі, злочинні активності країни-агресора в межах останнього почали активно нарощуватися, що змусило вітчизняні державні структури удосконалювати свій інформаційно-цифровий потенціал задля здійснення гідної відсічі ворожим зазіханням. Для нас в межах дослідження є важливим висвітлення, насамперед, двох ключових аспектів: змістового наповнення інформаційного дискурсу Росії та технологічного способу його донесення до аудиторії. Саме тому у даному підрозділі будуть

проаналізовані основні наративи, поширювані РФ у інформаційному просторі, та цифрові інструменти, зокрема за допомогою яких ці оповідки інкорпорувалися у публічний вимір.

Інформаційна війна Росії проти України провадилася и триває у трьох площинах: у межах власного інформаційного простору для закріплення у свідомості росіян хибних інформаційних патернів щодо українців, нашої держави, її офіційних представників, міжнародної діяльності тощо; у межах українського інформаційного поля з метою дезінформації, формування недовіри громадян до політичної влади, закладання підсвідомих страхів і т. д.; у світовому інформаційному просторі задля поширення неправдивих наративів щодо України. Усі ці активності інформаційного характеру мали політичну мету – шляхом дискредитації української держави та її населення виправдати зазіхання на суверенітет, територію та політичну владу в Україні.

Наративи, ініційовані РФ у всіх трьох вище згаданих вимірах мали однакову змістову наповнюваність, однак, - різні наслідки через відмінність ефективності своїх інформаційних каналів у цих трьох площинах. Найбільш сприйнятливим грунтом для поширення спотворених ідей щодо України виявився внутрішній інформаційний простір Росії. Важливим чинником дієвого проведення інформаційної кампанії проти України був тривалий контроль російського уряду над ЗМІ. Російський наратив був інструменталізований за допомогою одночасних повідомлень. Наприклад, основні російські телеканали активно залучалися до формування думок про ситуацію в Україні з самого початку кризи. Контроль здійснювався і здійснюється безпосередньо Адміністрацією президента, включаючи також контрольований урядом інтернет-тролінг. Цей контроль над ЗМІ ускладнив конкуренцію демократичним державам із вільними ЗМІ з сильними, синхронізованими повідомленнями російського уряду.

Російський антиукраїнський дискурс включає кілька домінуючих тем: позиціонування російської слов’янської православної цивілізації в опозиції до «декадентської» Європи; позиціонування України як невід'ємної частини

євразійства та створення Євразійського економічного союзу; пропагування Російського світу, який об'єднує східних слов'ян, передбачає, що росіяни та українці є однією нацією, і визнає природну зверхність Росії; зображення українців як псевдонації, яка не в змозі керувати власною країною та підтримувати свою державність; посилання на Велику Вітчизняну війну, таким чином виявляючи ненависть до нацизму та пов'язуючи це з протестувальниками Євромайдану, яких називають націоналістами, нацистами та фашистами, що становлять загрозу для етнічно російської частини населення України; розкол Заходу шляхом використання різних інтересів країн-членів ЄС і позиціонування США в опозиції до ЄС; використання правових та історичних обґрунтувань для легітимації дій Росії в Україні (включаючи Кримський референдум). Отже, деталізуємо ключові напрямки російського дискурсу з дискредитації України.

Аналізуючи наративи, поширювані російською пропагандою, важливо враховувати, що цей процес розпочався задовго до 2014 року. Теорія зіткнення цивілізацій, запропонована С. Гантінгтоном [8], стала дуже зручною для російської еліти як спосіб провести віртуальну лінію культурних відмінностей між Заходом і православною цивілізацією Сходу. Концепція зіткнення цивілізацій та діалогу між цивілізаціями часто з'являлася у виступах російської владної еліти та співпрацюючих з нею експертів у період 2004-2007 років. Кульмінацією цього дискурсу був виступ президента В. Путіна у 2007 році на Мюнхенській конференції з безпеки, де він критикував США за збереження однополярного світового порядку. Православна цивілізація виглядала б неповною без України. Політолог із Кремля В'ячеслав Ніконов просував концепцію України та Росії як центру спільної цивілізації, яка широко підтримується Російською Православною Церквою. Цей наратив доповнюється антиєвропейським наративом, який намагається або спотворити європейські цінності (наприклад, визначити толерантність до сексуальної різноманітності як ознаку декадансу), або загрожує потенційним економічним колапсом через тіснішу асоціацію з ЄС.

У контексті формування Євразійського економічного союзу концепція євразійства переживає відродження. Подібно до православної цивілізації та російського світу, Євразійський союз також хоче бачити Україну невід'ємною частиною. Найвидатнішим пропагандистом євразійства є О. Дугін, який адаптував класичні ідеї євразійства до сучасних реалій. Якщо євразійці 1920-х років вважали, що джерелом усього зла є «індивідуалістична і егоїстична Європа», то сьогодні О. Дугін відводить цю роль США і трансатлантистам [3]. На думку євразійців, Україна – це «поле битви титанів», де добро і зло борються за вплив. Ініціатива «Східне партнерство» розглядається як засіб для трансатлантів (НАТО, США, ЄС) викрасти Україну з Євразії.

Поряд з іншими російськими пропагандистами О. Дугін говорить про єдність східних слов'ян. Він називає українців – «малоросами», а росіян – «великоросами». Подібне покровительське, «батьківське» ставлення до України спостерігається у виступах російських політиків та політичних оглядачів. Російський світ, який у минулому був географічно об'єднаний, нині розділений кордонами різних країн. Народи, які живуть на території історичної російської землі, повинні відчувати свою приналежність до спільної цивілізації. Ця ідея була висловлена російським православним патріархом Кирилом на відкритті 3-ї Асамблеї російського світу в Москві в 2009 році. Він також запропонував використовувати термін «країни російського світу», маючи на увазі країни, які історично входили до складу Росії. Кирило уточнив, що ці країни об'єднує спільне використання російської мови, спільна культура та історична пам'ять. У цьому контексті Україна стає особливо актуальною для російського світу. Подібно до православної цивілізації, «рускій мір» також не можна вважати серйозним проєктом без включення України.

Хоча російські політики часто вживали термін «братні народи», у практиці російської зовнішньої політики це братство означає сувору ієрархію, де права українців на самовизначення ігноруються. У російських державних ЗМІ часто можна зустріти принизливі висловлювання щодо української

державності та її бажання інтегруватися із Заходом. Навіть розважальні програми показують українців як неповноцінну націю, яка розмовляє химерним російським діалектом. Аби ігнорувати українську мову як джерело сучасних слов'янських мов та українців як творців їхньої державності, російські ЗМІ навмисно ігнорують правду про давнє коріння слов'янської мови, збережену в сучасній українській мові, та історичні факти про походження стародавньої Руської держави з Києвом у центрі (Київська Русь). Таким чином, російська пропаганда продовжує культивувати серед українців комплекс меншовартості (уже сформований за радянської влади), коли українську таврували як сільську, селянську мову (нерозвинену), а російську асоціювали з мовою культури та інтелекту.

В останні роки святкування Дня Перемоги 9 травня зайняли центральну роль в ідеології російської держави. Провідні російські телеканали задіяні у створенні різноманітних програм і репортажів на цю тему, з якими вони виходять в ефір задовго до вшанування. Держава також надає фінансову підтримку для виробництва художніх фільмів про історичні події. Ці фільми підтримують старі міфи, що прославляють Росію, і допомагають створювати нові. У цьому контексті жителі Західної України зображуються як бандерівці, які, на жаль, не були знищені до останнього.

Росія застосувала лінійну стратегію у побудові свого наративу, починаючи з Петра Великого, з історичним акцентом на Великій Вітчизняній війні, щоб розпалити пафос, пов'язаний з нацистськими елементами. Застосування «ментальності війни» не випадкове, оскільки пов'язане з живою пам'яттю та справжніми проблемами Великої Вітчизняної війни. Звернення до прихильності російськомовного населення здійснювалося шляхом фабрикації інформації, історичного наративу, який підживлював певні культурні передумови, а потім спонукав до певних дій. Це полегшило завдання клеймити активістів Євромайдану нацистами, фашистами та антисемітами, а також створити побоювання у російськомовного населення України, що нова «фашистська» влада конфіскує майно, вдасться до насильства та заборонить

російську мову – все це емоційно пояснювали на телеекранах російських каналів «реальні люди».

Особливої уваги заслуговує спроба розділити Захід (включаючи НАТО та його партнерів) російським наративом. Спроба зосереджена на тому, щоб зробити Захід безсилим і не схильним до ризику, коли стикається з нечесною російською розповіддю. Наприклад, Кремль намагався розділити Німеччину та ЄС, погрожуючи завдати шкоди економіці першої, яка залежить від імпорту російського газу, нагадуючи німцям про недавню історію. У своєму публічному виступі після анексії Криму В. Путін сказав, що вірить у те, що європейці, в першу чергу, німці, його також зрозуміють. Він грав на відмінностях у поглядах між Новою (Східною) Європою та Старою Європою, продовжуючи нагадувати європейським лідерам про незручні історичні факти та апелюючи до дивної логіки, стверджуючи, що оскільки Росія повністю підтримує возз'єднання Східної та Західної Німеччини, Німеччина тепер має підтримати Росію у її возз'єднанні з Кримом.

В. Путін усвідомлював різні інтереси країн ЄС у співробітництві з Росією, зокрема економічні, а також труднощі європейських держав у пошуку твердої спільної позиції. Окрім різних національних інтересів, ЄС все ще стикається з деякими історичними примарами, зокрема відчуттям зради Східної Європи після Ялтинської конференції 1945 року. Усе це залишає багато наративних ліній для використання у спробі розколоти Захід. Російський наратив також намагається розірвати трансатлантичний зв'язок і поставити США в опозицію до Європи.

Російська стратегія передбачає інструменталізацію права як засобу легітимізації всіх своїх дій. Це також пов'язано з ідеєю російської цивілізації, з її власними правовими нормами та тлумаченням міжнародного права. Аспект легітимності дуже важливий для підтримки російського наративу. Це допомагає Росії звертатися до внутрішньої аудиторії, до співвітчизників за кордоном і навіть до міжнародної спільноти, демонструючи, що Росія є законослухняною і «чинить правильно». Для Росії було важливо заохочувати

«легальне» самовизначення в Криму, а також заохочувати подібні референдуми про самовизначення на Сході України, накриваючи таким чином завісу «легітимності» на анексію Криму. Дуже важливо було також те, що самопроголошене керівництво Криму (а згодом і Східної України) офіційно звернулося з проханням про допомогу, інтервенцію чи навіть анексію Росії.

Підтримка російської інформаційної кампанії була зосереджена на спробах провести паралелі зі справою Косова та апелювала до історичної несправедливості, скоєної в 1954 році, коли Крим було віддано Україні керівництвом СРСР. У своєму зверненні 18 березня 2014 року після референдуму в Криму В. Путін перерахував цілий спектр «законних» причин того, що сталося: Статут ООН, який говорить про право націй на самовизначення, відомий косовський прецедент, обурливі історичні несправедливості, вчинені проти Росії (включно з розпадом СРСР і Заходом, які спровокували кольорові революції), і необхідність захистити співвітчизників за кордоном від спроб української влади «позбавити росіян їхньої історичної пам'яті». Політика щодо захисту співвітчизників також могла дати достатньо законні підстави для входження Росії на українську територію у разі виявлення будь-яких доказів гуманітарної кризи. Існувала безперервна наративна лінія, яка культивувала історії про порушення прав людини, військові злочини та погіршення гуманітарної ситуації. Наратив проти кольорових революцій також звертався до інших авторитарних урядів, які готові підтримати лінію Росії в цьому відношенні.

Частина наративу включає постійні спроби звинуватити НАТО і Захід у порушенні всіляких законів і перерахувати втручання в Югославію, Ірак, Афганістан та Лівію як очевидні приклади. Росія також звинувачує НАТО в порушенні обіцянки, нібито даної Росії в 1990 році, про те, що Альянс не буде розширюватися на Східну та Центральну Європу, не створюватиме військову інфраструктуру поблизу кордонів Росії та не розгортатиме там війська. У інформаційній кампанії Росія подається як щира і справедлива, а Захід зображується як такий, що дотримується подвійних стандартів, цинічно

ставиться до зловживання правами людини та віддає перевагу «правилу зброї» перед міжнародним правом.

Український уряд також звинувачується у порушенні угоди від 21 лютого між колишнім президентом В. Януковичем та деякими представниками опозиції за посередництва міністрів закордонних справ ЄС. Росія вважала це достатньою підставою для того, щоб визнати українську владу нелегітимною, а парламентське голосування за відсторонення В. Януковича від влади як спробу державного перевороту. Є також схожість з російсько-грузинським військовим конфліктом (2008), що можна спостерігати в Україні: спроби дискредитувати та криміналізувати грузинський уряд, клеймити грузинські військові операції як геноцид та штучно створити діаспору російських громадян на спірних територіях шляхом заохочення, а в деяких випадках примушуючи громадян цільової країни відмовитися від національного громадянства на користь російського (т. зв. «паспортизація»).

Своєю інформаційною кампанією Росія намагалася довести, що мала на меті підтримати волю місцевого населення, груп самооборони в Україні. Одним із важливих аспектів російського наративу є поняття «історичної російської присутності», яке використовується у спробі легітимізувати російські інтереси та діяльність на територіях, де росіяни були (або досі) історично присутні з будь-яких геополітичних причин. Крим називають історично російською землею, а Севастополь — російським містом. В. Путін стверджував, що у серцях і умах [російських] людей Крим завжди був невід'ємною частиною Росії.

Усі ці розповіді підтримуються за допомогою так званих тематичних комунікаційних рамок, які є способом асоціювати певне враження чи думку з об'єктом чи предметом. Характеристиками тематичних рамок є їхні тісні взаємозв'язки в певному контексті та інтерпретації. Тематичне обрамлення може бути застосовано до окремої особи (наприклад, назвати президента України П. Порошенка «Королем шоколаду»), до групи людей (жителі Західної України є послідовниками Бандери та неонацистів), або до процесу,

подія або конкретне місце в часі та просторі (Євромайдан дорівнює хаосу). Створення тематичних рамок пов’язане з бажанням людини спростити зовнішній світ і легко відрізнити друзів від ворогів. На жаль, тематичне обрамлення також можна використовувати для маніпулювання аудиторією. Основними тематичними рамками, використаними під час російської інформаційної кампанії, були:

- соціально-економічні проблеми, залежність від Росії та неспроможність української держави забезпечити своїх громадян/жителів;

- радикалізація опозиції шляхом позиціонування її або як творця думок, які можуть викликати страх і паніку в громаді, або як насмішку;

- відсутність соціального порядку та безпеки, які використовуються як привід для виправдання дій «Беркуту» або створення проросійських груп самооборони на Сході України;

- Євромайдан – це сателіт США/ЄС, а його прихильники – зрадники;

- Захід «злий», оскільки не хоче/не може врятувати Україну від економічних проблем, впливає на українську владу, щоб здійснити якусь змову, інспірує насильство (як і в інших країнах світу), готується екстремістів у спричиненні громадських заворушень в Україні, сприяє моральному занепаду;

- Росія близька Україні, а західні демократії – чужі;

- спільна історія Росії та України та православна релігія як об'єднуючий елемент тощо.

Дезінформаційна та кібернетична діяльність Росії мали суттєвий вплив на різні галузі вітчизняної життєдіяльності (соціально-політичну, економічну, технологічну тощо), а також вагомий міжнародний ефект. У силу значущості цих впливів вважаємо доцільним розглянути їх більш предметно.

На соціальному рівні люди зі Східної України та Криму, які є переважно російськомовними регіонами, стали повністю ізольованими від будь-якої сторонньої інформації. Вони могли слухати лише російське радіо або дивитися російське телебачення, і тому мали дуже обмежений доступ до інших форм

ЗМІ, фактично це не давало їм можливості сформувати інші думки, ніж ті, які пропагувалися російськими ЗМІ. Збереження цієї ізоляції є важливою частиною російської інформаційної війни, метою якої є контроль громадської думки та опосередковане формування рішень на користь Росії [36].

Російська пропаганда вважається доволі високоефективною. Вона транслюється через велику кількість різноманітних каналів: від традиційного телебачення до соціальних мереж і чатів. Це дозволяє пропаганді охопити більшу кількість людей і публікувати новини швидше, ніж традиційні медіа-канали, обмежені необхідністю перевірки фактів перед публікацією [45]. Російські пропагандисти також намагалися підвищити довіру та помітність своїх новинних платформ, запрошуючи експертів або знаменитостей, таких як Джуліан Ассанж і Ларрі Кінг [12].

Значний обсяг кібератак на українські державні інституції певною мірою підірвав віру і довіру людей цих регіонів у спроможність української влади в захистити їх. Це також сприяло створенню різноманітних хакерських груп в Україні, включно з Українськими кібервійськами/армією Докукіна. На початку конфлікту українській владі не вистачало можливостей для боротьби з різними кібератаками. Як наслідок, такі приватні ініціативи, як приклад Докукіна, підтримали владу та український народ проти тролів та інших російських кіберактивностей [34].

Ще одним прикладом зниження довіри людей до своєї влади стала поширена атака «Відмова в телефонних послугах», запущена на кол-центр українського постачальника електроенергії під час відключення електроенергії в грудні 2015 року. Кол-центр був переповнений фальшивими телефонними дзвінками, через що він не міг відповісти на дзвінки від реальних клієнтів, які зазнали відключення електроенергії.

Економічні наслідки кібератак в контексті російсько-українського конфлікту здебільшого стосувалися наслідків DDoS-атак та атак зі знешкодженням. DDoS-атаки, зазвичай, призводять до прямих витрат для бізнесу у вигляді втрати доходів і втрати продуктивності. Середня економічна

шкода оцінюється в 22 000 доларів США за хвилину недоступності веб-сайту, а середня очікувана тривалість цих атак становила 54 хвилини [33]. Таким чином, такі атаки можуть коштувати значних грошей для бізнесу, на який вони спрямовані. Однак, на кожну компанію впливають DDoS-атаки по-різному, а інші витрати, такі як розслідування, технічна реакція, підтримка клієнтів і витрати на зв'язки з громадськістю, додають до рахунку.

Непрямі витрати, включаючи шкоду репутації, крадіжку важливих даних та альтернативні витрати, також необхідно враховувати, і вони також можуть мати серйозні наслідки [41]. В умовах російсько-українського конфлікту жертвами таких атак ставали переважно ЗМІ, банки та урядові сайти. Для перших двох типів жертв втрата доходу може бути найважливішою проблемою, тоді як для державних установ, чиї веб-сайти були поцілені, репутаційна шкода та непрямі витрати, понесені від таких атак, є найбільш гострими проблемами. У випадку останніх люди можуть почати сумніватися в здатності державних установ виконувати свої завдання або захищати громадськість (особливо якщо установи не змогли захистити власні веб-сайти від кібератаки).

Зараження зловмисним програмним забезпеченням може бути таким же економічно небезпечним, як і DDoS-атаки для жертв. Проте, схоже, що в російсько-українському конфлікті шкідливе програмне забезпечення використовувалося для збору інформації в розвідувальних цілях, а не для збагачення чи кіберзлочинної діяльності. Ці вторгнення спричиняють подібні витрати, як і DDoS-атаки, оскільки жертвам потрібно залучити бригади екстреної допомоги, щоб зупинити втручання та розслідувати атаку. Вони також впливають на репутацію установ з тих самих причин, що й DDoS-атаки [11].

У межах російсько-українського протиборства мали місце фізичні атаки на телекомунікаційні інфраструктури, а також кібератаки на критичні інфраструктури. Зокрема, під час вторгнення в Україну в березні 2014 року так звані «зелені чоловічки» здійснили рейд на кримську інфраструктуру

українського телекомунікаційного провайдера «Укртелекому». Вони втрутилися в кримський пункт обміну Інтернетом, щоб ізолювати півострів від решти світу та не дати йому повідомити про події. У даному випадку завдана фізична шкода була не результатом кібератаки, а скоріше матеріального втручання в роботу Інтернету в Криму. Росія, яка визнала, що «зелені чоловічки» насправді були російськими військами у квітні 2014 року, не намагалася повністю відключити Інтернет в Україні з кількох причин [32]. По-перше, це було б занадто складно, оскільки в Україні є шість точок доступу до Інтернету, всі вони проходять через Київ. Крім того, багато українців використовують російські соціальні мережі, такі як vKontakte, та російські інтернет-ресурси, такі як електронні адреси, що дозволяє російській владі перехоплювати та читати або прослуховувати всі розмови, що ведуться через ці платформи. Навіть деякі українські чиновники використовували облікові записи електронної пошти, надані російськими компаніями, що дозволяло російському уряду легко отримувати необхідну інформацію навіть без кібератак [44]. Це частково пояснює, чому було так мало атак на комунікаційні інфраструктури у фізичній та кіберсфері та показує, що технологічна залежність від іншої держави може мати значні наслідки.

Перші кібератаки на критичні інфраструктури відбулися в грудні 2015 року, коли кілька українських електростанцій були зупинені на кілька годин. Атаки стосувалися шкідливого програмного забезпечення BlackEnergy3. Слідчі повідомляли, що ці електростанції не повернулися до повного рівня навіть через два місяці після атак. Зловмисники перезаписали код мікропрограми для 16 підстанцій, в результаті чого оператори не змогли дистанційно увійти в систему підстанцій і їм довелося керувати ними вручну. Крім того, зловмисне програмне забезпечення містило корисне навантаження на ім’я KillDisk, яке стирало та збивало заражені комп’ютери. Не вдалося перезапустити заражені машини. Усі збережені дані та інформація були втрачені та потребували заміни.

Ця конкретна атака на електростанції могла бути відповіддю на фізичну атаку проукраїнської групи на електростанції в Криму. Проте судово-медичне розслідування показало, що зараження почалося вже навесні 2015 року. Слідчі стверджували, що зловмисники могли завдати значно більшої шкоди, ніж просто відключення електроенергії на кілька годин. Вони припускають, що атака була лише повідомленням, щоб продемонструвати свої можливості [55].

Друга кібератака на критичні інфраструктури сталася в грудні 2016 року і була дуже схожа на попередню. Вона націлювалася на електростанцію під Києвом і спричинила відключення електроенергії приблизно на годину. Атака використовувала як те саме шкідливе програмне забезпечення BlackEnergy, так і корисне навантаження KillDisk. Шкідливе програмне забезпечення було впроваджено в систему за допомогою фішингової кампанії. Однак, інцидент завдав меншої матеріальної шкоди, ніж у 2015 році [25].

Техніки, використані в кіберпросторі в українському конфлікті, не є новими і не досягли такої інтенсивності, як, приміром, під час конфлікту між Грузією та Росією у 2008 році [53]. Новим елементом у цьому конфлікті була поява нових шкідливих програм, включаючи Snake, Operation Armageddon і X-Agent, які також виявили розвиток злочинного шкідливого програмного забезпечення, такого як BlackEnergy, для розвідувальних і наступальних операцій. Виявлення шкідливого програмного забезпечення, націленого на смартфони, тобто X-Agent, було ще одним важливим технологічним розвитком під час конфлікту. Це являє собою абсолютно новий елемент у вимірі збору розвідувальних даних і комунікації на полі бою. Ці нові типи шкідливих програм можуть спровокувати гонку кібер-озброєнь серед держав, які побоюються кібератак з боку Росії. Ці держави можуть створювати нові засоби кіберзахисту або наступальні можливості, щоб захистити себе. Також існує ризик того, що зловмисне програмне забезпечення, використане під час конфлікту, може бути використане у злочинних цілях.

Після Євромайдану та подальшої анексії Криму в березні 2014 року кількість кібератак на Україну з боку Росії зросла. Насправді, конфлікт

відбувався одночасно в кіберпросторі та фізичному світі: кіберзасоби використовувалися в поєднанні з кінетичними операціями та для їх підтримки. У цьому випадку можлива модель ескалації діяльності в кіберпросторі та перекидання у фізичну сферу не відбулася, оскільки конфлікт загострювався паралельно в обох сферах. Кібероперації були використані заздалегідь для підтримки кінетичних операцій шляхом збору розвідданих і дезінформації. Більше того, кіберпросторовий аспект конфлікту був значущим на початку війни, потім заспокоївся і відтоді залишився на більш-менш постійному рівні інтенсивності. Кібератаки в основному обмежувалися кібер-зривними атаками, такими як DDoS, пошкодження веб-сайтів і зловмисне програмне забезпечення для збору розвідувальних даних [48, с. 121]. Здається, інтенсивність знову зросла з грудня 2015 року, але навіть у цих випадках пошкодження було навмисно обмеженим. Кібератаки на українську електромережу в грудні 2015 та 2016 років могли спричинити загострення конфлікту, однак, зловмисники обмежили заподіяну шкоду. Експерт ВПС США, який допомагав українській владі в їх розслідуваннях, заявив, що нападники могли завдати набагато більшої шкоди, але через кілька годин припинили атаку [55]. Експерт припустив, що обидва напади були спрямовані лише на те, щоб показати, на що були здатні зловмисники. Таке самообмеження можна також розуміти як спосіб уникнути подальшої ескалації конфлікту, що загрожує значною відповіддю з боку України чи її союзників. Критичні інфраструктури та людські життя вважаються «червоними лініями», які не можна перетинати, якщо учасники хочуть стримати конфлікт [37].

Конфлікт в Україні показав, що Росія готова використовувати військову силу як інструмент зовнішньої політики, як це було 2008 року під час конфлікту між Грузією та Росією. У той же час, використання кіберзасобів Росією значно розвинулося після конфлікту 2008 року на Кавказі. Відтоді Росія створила «інформаційний взвод», який пізніше був перетворений на ферми тролів [23, с. 29–30]. Однак, конфлікт у Грузії відрізнявся тим, що Росія

в 2008 році мала більше проблем з контролем «інформаційного простору» і сприймалася як країна, що програла інформаційну війну [40, с. 26]. З іншого боку, у 2014 році Україна опинилася повністю ізольованою від сторонньої інформації, і іноземним ЗМІ було важко отримати точну інформацію про те, що відбувається в країні.

Той факт, що західні ЗМІ не змогли підтвердити присутність російських військових в Україні по суті протягом 2014 року, свідчив про те, що російська тактика ізоляції українського «інформаційного простору» стала ефективнішою в порівнянні з 2008 роком. Тоді як західні країни вважали російську пропаганду та дезінформацію занадто очевидними та легко ідентифікованими, росіяни могли забруднити інформаційні канали, викликаючи плутанину щодо достовірності інформації, що надходила з регіону [24, с. 25–27]. Росія також скористалася своїми проксі-силами у фізичній частині конфлікту в Україні, щоб ускладнити ситуацію. Це дало Росії можливість заперечувати будь-яку фізичну причетність до конфлікту. Цей метод також був успішно розгорнутий у кіберпросторі, про що свідчить наявність КіберБеркута, який одні джерела називали проросійською хакерською групою з України, а інші - стверджували, що, насправді, це російська хакерська група APT28 [35, с. 57].

На міжнародному рівні після анексії Криму Україна опинилася ізольованою від будь-якої допомоги та відданою на милість ефективної російської інформаційної війни. У грудні 1994 року США, Великобританія, Франція та Китай пообіцяли Україні в Меморандумі про гарантії безпеки, що вони звернуться за допомогою до Ради Безпеки ООН у разі будь-якої агресії з боку Росії [51]. Насправді, колишня Радянська Республіка географічно знаходиться надто близько до Росії і занадто далеко від Західної Європи, щоб отримати будь-яку значну військову підтримку з боку західних держав. Крім певної матеріальної та освітньої допомоги, армії західних країн не зробили багато, щоб запобігти анексії Криму Росією чи зупинити конфлікт на сході України [12]. Допомога з боку НАТО надходила у вигляді фінансування та

досвіду для захисту кіберпростору України, але війська НАТО не були розгорнуті. У вересні 2014 року на саміті НАТО було прийнято рішення про створення п’яти фондів для допомоги Україні, одним з яких є Трастовий фонд кіберзахисту, спрямований на навчання персоналу та консультування українських органів влади щодо кіберполітики [20]. НАТО також проводив регулярні міжнародні військові навчання в українському регіоні, щоб продемонструвати, що про регіон не забули. США також допомагали українським силам, тренуючи війська та даруючи обладнання, таке як радари, медичні товари тощо [26].

Після анексії Криму західні держави ввели економічні санкції проти Росії. Ці санкції не були накладені на Росію спеціально через кібератаки в Україні. Тим не менш, заборони та ембарго мали певний вплив на російську економіку. Ціль цих санкцій полягала в тому, щоб західні держави чинили тиск на російські ринки в довгостроковій перспективі, щоб показати своє засудження війни в Україні та анексії Криму. Санкції обмежили доступ до європейських та американських ринків капіталу для російських фінансових, енергетичних та оборонних компаній, заборону на імпорт і експорт зброї, заборону на експорт товарів подвійного призначення, обмеження доступу до чутливих технологій та обмеження на послуги, пов’язані з видобуток нафти [27]. Ці санкції вплинули на російську економіку, спричинивши її скорочення на 1,5% у 2015 році, але їхня дія фактично була обмеженою. Насправді, падіння цін на нафту в 2015 році мало сильніший вплив на російську економіку, ніж санкції (Emmott, 2016). Проте, санкції чинили тиск на російську економіку, хоча й не вплинули на російську політику щодо України.

З моменту вторгнення армії РФ на територію України у лютому 2022 року боротьба на інформаційному «фронті» суттєво масштабувалася. Зросла частота кібернетичних атак та інформаційних провокацій з боку супротивника. Українській стороні довелося активно захищатися та контратакувати силами СБУ, Міністерства цифрової трансформації, кіберполіції, РНБО, ЗСУ тощо. Лави кібервійська стрімко поповнюються

небайдужими спеціалістами з ІТ царини приватного сектору, які хочуть використати свої знання та вміння у боротьбі з агресором в інформаційно-цифровому просторі. І якщо у січні 2022 року біля 70 українських веб-сайтів зазнали атак з боку Росії (включаючи Міністерство освіти і науки України, Міністерство закордонних справ тощо), то за перший місяць військової агресії РФ у 2022 році було здійснено понад 3000 кібернетичних атак. Рекордною була кількість 275 - на день.

Загалом боротьба у інформаційно-кібернетичному просторі, методики, інструменти, теоретичні засади і багато інших наукових аспектів цієї проблематики вивчаються широким колом як вітчизняних, так і зарубіжних пошуковців. У цьому контексті принагідно згадати таких експертів, як Б. Брейк, О. Буров, І. Валюшко, Л. Веселова, Дж. Гулд, С. Колінз, М. Лібіцкі, П. Паганіні, Р. Стендіш, О. Трофіменко, Г. Форос тощо.

Однак, аналітик, присвячених деталізації кібернетичних інструментів, якими оперує РФ від моменту вторгнення на українські землі в лютому 2022 року, поки що бракує.

Саме тому одне із завдань даного підрозділу полягає у дослідженні основних видів кібернетичних атак, до яких активно вдається Росія з моменту широкомасштабного нападу. Це дозволить вивчити кібернетичну поведінку супротивника, його провідні інструменти та проаналізувати можливі соціально-політичні наслідки їх застосування для України.

«Хакери насамперед атакують фінансову, державну та телекомунікаційну інфраструктуру. Попри це, всі сервіси працюють і доступні для користувачів. Провайдери і оператори справляються з кібератаками на свої мережі. Більшість проблем у роботі мереж пов'язана з фізичними пошкодженнями, які також вдається швидко усувати» [2], – зазначив Віктор Жора, заступник Голови Держспецзв'язку з питань цифрового розвитку, цифрових трансформацій та цифровізації.

Загалом кібератаки, які використовує Росія проти України, можна класифікувати за трьома типами: DDoS-атаки, пошкодження веб-сайтів та

зараження зловмисним програмним забезпеченням шляхом фішингу. Перші два інструменти точніше описуються як кібер-зриви, тоді як останній більш спрямований на кібершпигунство для збору розвідданих і підготовки поля бою до подальших кінетичних наступів або кібератак [48, с. 121].

Під час DDoS-атаки зловмисники перевантажують цільові веб-сайти запитами, що спричиняє збій у роботі служб веб-сайту та заважає легальним користувачам отримати доступ до цих сторінок. Цей метод вимагає використання кількох комп'ютерів, заражених бот-мережами, або координації роботи великої кількості користувачів. Зловмисники контролюють такі комп'ютери, скомпрометовані ботнетами, щоб надсилати запити до цільової мережі, про що користувачі заражених комп'ютерів навіть не здогадуються. DDoS-атаки також можуть відволікати увагу, щоб монополізувати увагу екстреної служби цільової установи. Поки вона зайнята боротьбою з DDoS-атакою, зловмисники можуть здійснювати інші шкідливі дії у відповідній мережі, наприклад, встановити бекдор або шкідливе програмне забезпечення з метою крадіжки даних [41, с. 4].

Пошкодження веб-сайту також спостерігається як інструмент кібернетичних активностей, задіяних проти українських цифрових ресурсів. Ця техніка передбачає, що хакер зламує веб-сервер за допомогою ін'єкції SQL, щоб отримати адміністративний доступ. Такий вид кібератаки вважається кібер-версією вандалізму. Після проникнення в систему зловмисник змінює зовнішній вигляд веб-сайту або замінює сторінки своїми матеріалами. Зазвичай, цю техніку використовують для поширення політичних меседжів.

Різні шкідливі програми також активно використовуються у інформаційному протистоянні. Серед останніх превалює використання трьох груп шкідливих програм, зокрема BlackEnergy, Snake та Operation Armageddon.

BlackEnergy - це сімейство шкідливих програм, які часто використовуються кіберзлочинцями. Перша версія BlackEnergy використовувалася для отримання доступу до мереж з метою запуску DDoS-

атак. Друга версія, BlackEnergy2, була оновлена функціями, які дозволяють красти дані. Остання версія, BlackEnergy3, була оновлена для націлювання на системи контролю та збору даних (SCADA) і додала нову функцію KillDisk, яка зробила заражені комп'ютери непридатними для використання. Ця версія була використана для атаки на українську енергосистему ще в грудні 2015 року [21].

Зловмисники використовують фішингові електронні листи зі зламаним вкладенням, щоб заразити комп'ютери. Потім зловмисне програмне забезпечення встановлює бекдор, щоб надати хакерам доступ до мережі. Останні дві версії зловмисного програмного забезпечення були розгорнуті для збору інформації та імплантовані в конкретні цілі, такі як український уряд та українська енергосистема.

Шкідливе програмне забезпечення Snake було виявлено у 2014 році, але було активним принаймні з 2010 або 2011 року. Воно схоже на більш стару зловмисну програму Agent.btz. Жертви заражалися або відкриваючи фішингові електронні листи, або шляхом відвідування веб-сайтів водопою, тобто веб-сторінок, заражених шкідливим програмним забезпеченням. Після того, як зловмисне програмне забезпечення заражає комп'ютер, воно чекає, поки користувач відкриє веб-браузер, а потім одночасно відкриває бекдор для спілкування зі зловмисниками без відома користувача [42]. Цей засіб призначений для копіювання та видалення файлів, підключення до заражених серверів, а також для завантаження та виконання інших шкідливих програм. Зловмисне програмне забезпечення Snake складається з двох елементів: руткіта і драйвера. Перший бере контроль над комп'ютером і приховує його діяльність від користувача, щоб вкрасти дані та захопити мережевий трафік. Драйвер вводить код у веб-браузер, щоб приховати обмін інформацією з серверами зловмисників, і створює прихований файл для зберігання конфігурації та вкрадених даних [43]. З початку Євромайдану в Україні зросла кількість комп'ютерів, заражених саме Snake.

Operation Armageddon – це інструмент віддаленого адміністрування або доступу, був спрямований на український уряд, правоохоронні органи та військові мережі. Його виявила у вересні 2014 року американська охоронна фірма LookingGlass. Експерти з безпеки та українські чиновники підозрюють Росію у створенні та використанні цього шкідливого програмного забезпечення [54]. Його метою є збір інформації про своїх противників, можливо, щоб отримати перевагу на полі бою. Ця практика демонструє, що кібершпигунство можна використовувати як інструмент для підтримки фізичної війни. Вважається, що ця шкідлива програма була активна щонайменше з 2013 року, коли Україна почала обговорювати Угоду про асоціацію з ЄС. Вона заражала машини через фішингові електронні листи зі скомпрометованим вкладенням Microsoft Word. Було відзначено, що деякі вкрадені документи були введені зловмисним програмним забезпеченням і надіслані новим цілям фішингових листів [30].

15 березня 2022 року в Україні фахівцями компанії ESET було виявлене нове зловмисне програмне забезпечення – вірус-вейпер CaddyWiper. За свідченням експертів, CaddyWiper знищує дані юзера та інформацію про розділи з будь-яких накопичувачів, які підключені до ураженої системи. Спеціалісти зазначають, що програма-шкідник деформує файли на накопичувачі у спосіб перезапису символами нульового байта, в результаті чого їх неможливо відновити.

«Раніше дослідники виявили два інших штами шкідливого програмного забезпечення Wiper, націленого на комп’ютери в Україні. Перший штам під назвою HermeticWiper був виявлений 23 лютого, за день до того, як Росія розпочала військове вторгнення в Україну. Версія IsaacWiper була розгорнута в Україні 24 лютого. При цьому в ESET припускають, що IsaacWiper і HermeticWiper перебували в розробці за кілька місяців до їх появи. Їхні перші зразки були виявлені у жовтні та грудні 2021 року, відповідно» [4].

Росія також інвестує багато ресурсів у скоординовані кампанії з дезінформації, а не лише у відкриті хакерські операції. Росія просуває

неправдиві наративи про вторгнення в Україну як на власній території, так і в українському та світовому інформаційному полях, включаючи підроблені відео (зустріч В. Путіна зі співробітницями авіаційної галузі, коли його рука магічним чином проходить крізь мікрофон), фото (Р. Кадиров у молитві на колінах в Україні, але на російській заправці) та новини (катування російських полонених, обстріли українськими військами своїх же населених пунктів, вербування українськими посольствами по всьому світу іноземних найманців та терористів, пропагування ненависті до мешканців Донбасу в українських підручниках). Російські чиновники заблокували доступ до соціальних мереж у країні, щоб запобігти поширенню інформації, яка не відповідає внутрішнім наративам.

Цілком зрозуміло, що вище описані злочинні активності хакерів від РФ у короткостроковій перспективі є деструктивними для державної та інформаційної інфраструктури України. Зокрема, такі дії можуть чинити тимчасовий збій у роботі банківської та фінансової систем, енергетичної галузі, системах мобільного та стаціонарного зв'язку тощо, що у свою чергу, може негативно відбиватися на життєзабезпеченні населення, координованості дій різних гілок влади, комунікації між громадянами та з громадянами і т. д.

Значний обсяг кібератак на українські державні інституції може підірвати віру людей в ці інституції та посилити загальне відчуття незахищеності. DDoS-атаки та пошкодження підривають довіру людей до їхніх інституцій та їхню здатність захищати власне населення. Пошкодження недержавних веб-сайтів передбачає переспрямування відвідувачів на інший веб-сайт, цільові веб-сторінки можуть втратити клієнтів, поки пошкодження зберігається. Такі пошкодження додатково спричиняють втрату довіри у власників зіпсованих веб-сайтів. Ці атаки виявляють слабкі місця в безпеці веб-сторінки, що може вказувати на подальшу вразливість і, таким чином, зробити сайти та власників сайтів ненадійними. Але в умовах воєнного стану такі нетривалі перепони (адже як доводить практика державний та приватний сектори оперативно

вирішують створені ворогом цифрові проблеми), не є першорядними і не завдають непоправної шкоди цифровій критичній інфраструктурі України.

Якщо ж оцінювати кібернетичні атаки агресора більш далекоглядно, стає зрозумілим, що вони сприяють удосконаленню вітчизняної системи цифрової та інформаційної безпеки, проактивній позиції держави, міжнародній співпраці у протистоянні агресору, обізнаності населення у технологіях цифрової та інформаційної боротьби, гігієні українських соціальних мереж, відповідальній поведінці користувачів комп'ютерами, телефонами та планшетами тощо.

Виходячи з сьогоднішнього досвіду України, можна стверджувати, що основна небезпека у інформаційно-цифровому протистоянні - це зосередженість Росії на інформаційній війні з використанням пропаганди, систематичного інтернет-тролінгу та дезінформації. Важливо, щоб демократичні держави визнали, що така кібер-діяльність може бути менш складною технічно, ніж прямі кібератаки на критичні інфраструктури, але також може завдати значної шкоди суспільству. Це питання потребує відкритого обговорення у вищих політичних колах, щоб підвищити рівень обізнаності серед політичних лідерів та суспільства, оскільки демократіям важко протистояти пропаганді. Свобода преси та свобода слова є основними демократичними принципами, але вони також забезпечують простір, у якому можуть легко поширюватися пропаганда та дезінформація. Російські ЗМІ розуміють цю вразливість і охоче її використовують.

Окрім відкритих дебатів щодо дезінформації та пропаганди, демократичні держави можуть вживати інших заходів для пом'якшення наслідків цієї тактики. Проте важливо, щоб демократії по-справжньому розуміли наслідки пропаганди та дезінформації, якщо вони хочуть ефективно протистояти цій тактиці та мати можливість розробити ефективні програми інформування. Такі програми мають пояснити населенню труднощі, пов'язані з інформаційною війною. Хоча державні установи можуть побажати попередити національну аудиторію про кампанії дезінформації та надати

поради щодо їх виявлення та засудження, вони також повинні інтегрувати інших учасників, включаючи ЗМІ. Вони також повинні прояснити, що таке тролі та яку роль вони відіграють у пропагандистських операціях. Просвітницькі та інформаційні кампанії можуть бути розроблені, щоб допомогти населенню легше розрізняти пропагандистські матеріали та зайняти більш критичну позицію до того, що вони читають або дивляться. Для демократій також було б важливо виявляти та виправляти дезінформацію та невідповідності в новинах, щоб обмежити вплив пропаганди [45].

Український кейс доводить, що використання іноземних технологій у роботі критичних інфраструктур може бути критичним у разі конфліктів. Тому важливо, наскільки це можливо, обмежити залежність від іноземних компаній щодо апаратного чи програмного забезпечення. Покладатися на іноземні технології проблематично як з міркувань безпеки, так і з логістичних міркувань. Наприклад, іноземному постачальнику може знадобитися поїхати в країну для технічного обслуговування або оновлення продукту. Це може відкрити можливість збирати інформацію про те, як продукт використовується та які його цілі. Відтак, може виникнути спокуса продати зібрану інформацію іншим державам. З точки зору державної безпеки, краще виробляти апаратне та програмне забезпечення всередині країни, якщо держава має відповідні можливості та потенціал. Там, де це неможливо, держави повинні віддавати перевагу аспектам безпеки таких дій. Незалежні перевірки апаратного та програмного забезпечення повинні виконуватися регулярно або застосовуватися до іноземних активів, щоб виявити будь-які реальні та передбачувані вразливості, залишені (навмисно чи випадково) постачальником.

Західні держави не є прямими жертвами кібератак в межах російсько-українського протистояння, але приватні компанії та окремі особи можуть постраждати опосередковано. Держави, які діють на посередницькій арені в Україні через ОБСЄ, можуть бути конкретною мішенню. Їхня участь підвищує ризик стати жертвою майбутніх кібератак. Насправді, ОБСЄ була мішенню

кібератаки, нібито скоєної Fancy Bear у грудні 2016 року. Держави повинні уважно стежити за кіберактивністю в українському регіоні, щоб оцінити, чи збільшується ризик прямих і непрямих кібератак на їх інфраструктуру, окремих осіб або бізнес.

Розробка оновлених правил безпеки у інформаційно-цифровому вимірі під час миру та війни могла б допомогти зменшити невизначеність та помилкове сприйняття. Демократичні держави погоджуються, що міжнародне право може застосовуватися до діяльності держав у кіберпросторі, і нові регулятиви можуть допомогти підвищити довіру та прозорість між державами у кіберпросторі. Труднощі приписувати дії акторам у кіберпросторі можуть викликати неясності, які можуть призвести до подальшої міжнародної напруженості. Більш чіткі міжнародні протоколи, угоди чи керівні принципи, узгоджені в рамках двосторонніх процесів або на регіональних/міжнародних форумах, можуть допомогти пом’якшити відповідні проблеми.

Можна запропонувати серію регулятивних заходів в контексті кібербезпеки, до якої відносяться:

- заходи прозорості (діалог щодо кіберполітики/стратегії/доктрини, обмін військовим персоналом, спільні симуляційні навчання тощо); показники відповідності та моніторинг заходів прозорості (наприклад, домовленість щодо заборонених цілей, таких як лікарні, спільні механізми в кризовому управлінні, такі як гарячі лінії);
- спільні заходи (наприклад, розробка загальної термінології, розробка спільних рекомендацій на випадок інцидентів, спільна оцінка загроз тощо);
- механізми комунікації та співпраці (наприклад, канали зв’язку в разі ескалації);
- заходи стримування (наприклад, зобов’язання скасувати стимули для наступальних дій першого удару або дій у відповідь, виключення кібернаступальних операцій проти третіх сторін тощо).

Такі заходи також розширять співпрацю між державами та призведуть до розширення діалогу, який також міг би перерости в міжнародні норми чи

договори. Це, у свою чергу, може покращити безпеку як у кібернетичній, так і у фізичній сферах.

Як ми бачимо, низка соціально-політичних наслідків може бути вичленована з кіберактивності, яка має місце в російській кампанії інформаційної війни проти України. Досвід нашої держави може стати у нагоді для багатьох інших країн, які бажаючи лишатися відкритими та демократичними, мають дбати про безпеку власного інформаційного поля. Зокрема, вони повинні активно намагатися зміцнити свою позицію, щоб їхня держава не стала жертвою пропагандистських кампаній. Крім того, вони повинні підвищити кібербезпеку державних онлайн-інфраструктур від атак розподіленої відмови в обслуговуванні та пошкодження веб-сайтів. Також покращення кібербезпеки може бути пов’язане з обмеженням залежності від іноземних технологій та наданням рекомендацій приватному сектору щодо того, як реагувати на кібератаки. Демократичні держави повинні уважно стежити за тим, як розвивається україно-російське протистояння у інформаційному просторі, і сприяти заходам зміцнення довіри на міжнародному рівні. Майбутні наукові розвідки в контексті даної проблематики можуть бути спрямовані на аналіз нових видів атак, які можуть з’явитися з часом у кібернетичному протистоянні проти РФ, компаративних студій різних видів кібератак, а також дослідження дієвих засобів протидії та контрнаступу у інформаційно-цифровому просторі.

Висновки до третього розділу

Дослідження практичного виміру політичного насилля, яке здійснюється засобами інформаційної війни, базувалося на аналізі досвіду інформаційних протистоянь України з РФ з урахуванням законодавчо-нормативної бази, що визначає правове поле для інформаційної безпеки та набуває ще більшої значущості в умовах повномасштабного вторгнення військ РФ на територію України та запровадження нашою державою воєнного стану. Окрім цього,

було вивчено інформаційно-воєнну практику РФ по відношенню до інших держав світу, насамперед, демократичних, з урахуванням як інструментарію, так і конкретних кейсів.

Проведена наукова робота свідчить про перманентне оновлення законодавства України з метою посилення інформаційної безпеки (з 24 лютого 2022 року Верховною Радою України прийнято Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції», Закон України «Про внесення змін до деяких законодавчих актів України (щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора), Закон України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності досудового розслідування за "гарячими слідами" та протидії кібератакам», Закон України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану» тощо.

Загалом аналіз законодавчих та нормативно-правових документів дозволив вичленувати основні принципи державної політики щодо інформаційної безпеки (верховенство права; пріоритет захисту прав і свобод людини, що стосуються інформації; своєчасний і адекватний захист життєво важливих національних інтересів від реальних і потенційних загроз інформаційній безпеці; захист інформаційного суверенітету України; свобода думки, свобода слова і вільне вираження думок і переконань; свобода збору, зберігання, використання та поширення інформації тощо), її ключові напрямки (створення нормативної бази для організації розвитку інформаційного простору та його захисту від зовнішніх загроз та узгодження

такої нормативної бази з нормами міжнародного права, вимогами міжнародного співробітництва та стандартами та правилами ЄС; розробка та реалізація ефективної національної інформаційної політики, спрямованої на розвиток національного інформаційного простору та гармонізацію системи контролю та координації серед практиків національної інформаційної політики та експертів з інформаційної безпеки) та загрози (комунікативні та технологічні).

Виявлено провідні наративи РФ з дискредитації та дестабілізації України: позиціонування російської слов'янської православної цивілізації в опозиції до «декадентської» Європи; позиціонування України як невід'ємної частини євразійства та створення Євразійського економічного союзу; пропагування Російського світу, який об'єднує східних слов'ян, передбачає, що росіяни та українці є однією нацією, і визнає природну зверхність Росії; зображення українців як псевдонації, яка не в змозі керувати власною країною та підтримувати свою державність і т. д. Виділено три групи кібернетичних атак РФ проти України (DDoS-атаки, пошкодження веб-сайтів та зараження зловмисним програмним забезпеченням шляхом фішингу), які використовуються ворогом найчастіше.

Російський підхід до інформаційної війни – це глобальна стратегія, яка включає як кібер-удари, так і інформаційні операції проти більшості демократичних акторів світу. Її цілі: відновлення російського домінування в пострадянській/імперській сфері впливу; зменшення впливу західних демократичних цінностей, інститутів та систем з метою створення поліцентричної моделі світу; розширення політичної, економічної та військової гегемонії Росії в усьому світі, щоб зміцнити місце РФ як великої держави.

Список використаних джерел до третього розділу

1. Андреєва О.М. Національна безпека України в контексті національної ідентичності і взаємовідносин з Росією [Текст] / О.М. Андреєва. – Київ: Парламентське видавництво, 2009. – 360 с.

2. Бухтатий О., Радченко О., Головченко Г. Україна медійна: на порозі інформаційної революції. URL: http://archive.nsju.org/uploaded/Ukraine_Mediyna.pdf

3. Вєдєнєєв Д.В. Гострі когті орла. Сили спеціальних операцій США: історія та сучасність [Текст]: монографія / Д.В. Вєдєнєєв, Г.С. Биструхін, А.І.Семука. – Київ: К.І.С., 2010. – 400 с.

4. Ганна Маляр: Перше правило інформаційної безпеки під час війни - не вір джерелам інформації ворога. URL: https://www.kmu.gov.ua/news/ganna-malyar-pershe-pravilo-informacijnoyi-bezpeki-pid-chas-vijni-ne-vir-dzherelam-informaciyi-voroga.

5. Гарькавий Є. М. Кризові комунікації як напрям реалізації стратегічних комунікацій у силах оборони України. Політичне життя: наук. журнал. 2019. № 3. С. 64-70.

6. Гарькавий Є. М. Механізми формулювання стратегічних наративів у системі реалізації стратегічних комунікацій сил оборони України. Держава і право: зб. наук. праць. Серія: «Політичні науки» / Ін-т держави і права ім. В. М. Корецького НАН України. К.: Юридична думка, 2019. Вип. 84. С. 100-111.

7. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення [Текст] / Ю.О. Горбань // Вісник НАДУ. – 2015, №1. – С. 136-141

8. Горбулін В. П. Забезпечення оборони та безпеки України: актуальні проблеми і шляхи їх вирішення. Вісн. НАН України. URL: http://www.nas.gov.ua/UA/Messages/Pages/View.aspx?MessageID=5517

9. Даниленко С. І. Інформаційне суспільство в контексті цивілізаційного вибору України. Проблеми міжнародних відносин. URL: http://nbuv.gov.ua/UJRN/Pmv_2013_7_6

10. Даниленко С. І. Регулювання й саморегулювання інтернету в світі: стійкі тенденції утвердження громадянського права на комунікацію. Актуальні проблеми міжнародних відносин. URL: http://nbuv.gov.ua/UJRN/apmv_2011_103%281%29__8

11. Держспецзв'язку: Від 15 лютого Україна зазнала понад 3000 DDoS-атак. URL: https://www.kmu.gov.ua/news/derzhspeczvyazku-vid-15-lyutogo-ukrayina-zaznala-ponad-3-000-ddos-atak.

12. Дубов Д. В. Політико-комунікативна безпека України у євроінтеграційному контексті: дис. ... канд. політ. наук: 21.01.01 / Національний ін-т проблем міжнародної безпеки Ради національної безпеки та оборони України. К., 2007. 218 с.

13. Дугин А. Евразийский реванш России. М.: Алгоритм, 2014. 256 с.

14. ESET виявила в Україні новий вірус-вайпер CaddyWiper, який знищує дані на накопичувачах. URL : https://itc.ua/ua/novini/eset-viyavila-v-ukrayini-novij-zlovred-caddywiper-yakij-znishhuye-dani-na-nakopichuvachah/.

15. Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандиської війни [Текст] / В.В. Зеленін. – Вінниця: Віндрук, 2014. – 384 с.

16. Зінченко М.О., Плугова О.Б, Драглюк О.В. Інформаційна війна, засоби реалізації та протидії. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ : НУОУ, 2017. С. 38–40.

17. Золотухін Д. Протидія інформаційній агресії Росії на рівні законодавчих актів: Резолюція Європарламенту. URL: http://bit.ly/2mVqxzW

18. Как работает фабрика «кремлевских тролей?» [Електронний ресурс] / Gordon.com [сайт]. – Режим доступу: http://gordonua.com/news/worldnews/Kakrabotaet-fabrika-kremlevskih-trolley-71305.html

19. Капштик О. В. Державні механізми стратегічних комунікацій у секторі безпеки і оборони України: дис. ... кан. наук із держ. управління:

25.00.05 / Хмельницький університет управління та права. Хмельницький, 2019. 197 с.

20. Карлова В. В. Вплив засобів масової інформації на формування української національної свідомості. URL: http://academy.gov.ua/ej/ej6/txts/07kvvunc.htm

21. Кемаль А. Кибер война. Как Россия манипулирует миром [Текст] /А.Кемаль. - Москва: Алгоритм, 2015. – 208 с.

22. Козлітін В.Д. Основні напрями світових глобалізаційних процесів кінця XX – початку XXI ст., дискусії між глобалістами та антиглобалістами про їх наслідки /В.Д.Козлітін // Збірник наукових праць. Серія «Історія та географія». – 2004. – Вип.17. – С. 26–30.

23. Коровин В. Третья мировая сетевая война [Текст] / В.Коровин. – Санкт-Петербург: Питер. 2014. – 352 с.

24. Литвиненко О. Система захисту інформаційного простору від спеціальних інформаційних операцій [Електронний ресурс] / О. Литвиненко // Національний інститут стратегічних досліджень [сайт]. – Режим доступу: http://www.niss.gov.ua/book/Litv/010_1.htm#a1.

25. Малик Я. Інформаційна війна і Україна. Науковий вісник. 2015. Вип. 15. URL : http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/ fail/Malyk.pdf.

26. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій. URL: http://euinfocenter.rada.gov.ua/uploads/documents/29377.pdf

27. Нацрада внесла до реєстру 13 «медійників-зрадників». URL: https://www.slovoidilo.ua/2022/04/12/novyna/suspilstvo/naczrada-vnesla-reyestru-13-medijnykiv-zradnykiv.

28. Ожеван М. А. Глобальна війна стратегічних наративів: виклики та ризики для України. Стратегічні пріоритети. URL: http://nbuv.gov.ua/UJRN/sppol_2016_4_6

29. Під час війни в Україні загинуло 20 журналістів: опубліковано їхні імена. URL: https://www.slovoidilo.ua/2022/04/12/novyna/suspilstvo/vijny-ukrayini-zahynulo-20-zhurnalistiv-opublikovano-yixni-imena.

30. План дій щодо впровадження оборонної реформи в 2016 – 2020 роках (дорожня карта оборонної реформи), затверджений Міністром оборони України від 15.08.16. URL: https://www.mil.gov.ua/content/tenders/Plan_2208.pdf

31. Російське іномовлення як інструмент маніпулювання громадською думкою у трансатлантичному просторі. НІСД. URL: http://www.niss.gov.ua/articles/1834/

32. Світова гібридна війна: український фронт / за ред. В. П. Горбуліна. URL: http://www.niss.gov.ua/articles/2431/

33. Семен Н.Ф. Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.Ру» та «Российский диалог») : ареф. дис. к. н. соц. комун; спеціальність 27.00.01. Дніпро : Дніпровський національний університет імені Олеся Гончара, 2018. 23 с.

34. Суспільні настрої на Донбасі-2020 – регіональне опитування. Фонд Демократичні ініціативи імені Ілька Кучеріва. URL: https://dif.org.ua/article/suspilni-nastroi-na-donbasi-2020-regionalne-opituvannya

35. Тихомирова Є. Б. Стратегічні комунікації ЄС: інституціональний вимір. Політичні проблеми міжнар. систем та глобальн. розвитку. 2016. № 4. С. 103-112.

36. У Гельсінкі офіційно відкрили Європейський центр протидії гібридним загрозам. URL: http://bit.ly/2mYstsk

37. Указ Президента України «Про рішення Ради національної безпеки оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». URL: https://zakon.rada.gov.ua/laws/show/152/2022#Text.

38. Фролова О.М. Нормативно-правові аспекти протидії інформаційним впливам РФ. Матеріали Міжнародної науково-практичної

конференції «Деокупація і реінтеграція інформаційного простору Криму: міжнародно-правові та медіа комунікативні інструменти». Київ : Інституту міжнародних відносин. 2019. С. 69–74.

39. Хантингтон С. Столкновение цивилизаций? Полис. 1994. № 1. С.33–48.

40. Черненко Т. В. Сучасний вимір публічної дипломатії в системі стратегічних комунікацій. Стратегічні пріоритети. URL: http://nbuv.gov.ua/UJRN/sppol_2016_4_10

41. Ajir M., Vailliant B. Russian Information Warfare: Implications for Deterrence Theory. Strategic Studies Quarterly 12. 2018. № 3. P. 70-89.

42. Alperovitch D. Bears in the Midst: Intrusion into the Democratic National Committee. URL: https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

43. BanffCyber Technologies. Business Implications of Web Defacement. URL: https://www.banffcyber.com/businessimplications-of-web-defacement.

44. Besemeres J. Russian disinformation and Western misconceptions. URL: http://insidestory.org.au/russiandisinformation-and-western-misconceptions.

45. Baumgartner M., Beuth P., Diehl J., Esch C., Gebauer M., von Hammerstein K., Wiedmann-Schmidt W. Cyber-Espionage Hits Berlin: The Breach from the East. Spiegel Online. URL: https://www.spiegel.de/international/germany/cyber-espionage-likely-from-russia-targets-german-government-a-1196520.html.

46. Blank S. Cyber War and Information War à La Russe – Understanding Cyber Conflict: 14 Analogies. Carnegie Endowment for International Peace. URL: https://carnegieendowment.org/2017/10/16/cyber-war-and-information-war-la-russe-pub-73399.

47. Brattberg E., Maurer T. Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks. Carnegie Endowment for International Peace. URL: https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyberattacks-pub-76435.

48. Cherepanov A. GreyEnergy: A Successor to BlackEnergy. White paper. URL: https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf.

49. Connell M., Vogler S. Russia's Approach to Cyber Warfare. CNA analysis and Solutions. URL: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

50. Connelly A., Cibralic B. Russia's Disinformation Game in Southeast Asia. URL: https://www.lowyinstitute.org/the-interpreter/russias-disinformation-game-southeast-asia.

51. Dragos. Allanite.URL: https://dragos.com/resource/allanite/.

52. Fiscutean A. Cyber war in Ukraine: How NATO is helping the country defend itself against digital threats. URL: http://www.zdnet.com/article/ukrainescyber-warfare-how-nato-helps-the-countrydefend-itself-against-digital-threats/.

53. FireEye Inc. FireEye Industry Intelligence Report cyber attacks on the Ukrainian grid: what you should know. FireEye Inc. Milpitas. CA. 2016.

54. F-Secure Labs Threat Intelligence. The Dukes: 7 years of Russian cyberespionage. URL: https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf.

55. Giles K. Russia's "new" tools for confronting the West: continuity and innovation in Moscow's exercise of power. Chatham House, London. 2016.

56. Giles K. Russia and Its Neighbours: Old Attitudes, New Capabilities. Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers. 2015.Tallinn. P. 19–28.

57. Goodin D. Hackers trigger yet another power outage in Ukraine. URL: http://arstechnica.com/security/2017/01/thenew-normal-yet-another-hacker-causedpower-outage-hits-ukraine/.

58. Gould J. Electronic Warfare: What US Army Can Learn From Ukraine. DefenseNews. URL: http://www.defensenews.com/story/defense/ policy-budget/warfare/2015/08/02/us-armyukraine-russia-electronic-warfare/30913397/.

59. Gros D., Mustilli F. The Effects of Sanctions and Counter-Sanctions on EU-Russian Trade Flows. URL https://www.ceps.eu/publications/effectssanctions-and-counter-sanctions-eu-russiantrade-flows.

60. Gurganus J., Rumer E. Russia's Global Ambitions in Perspective. URL: https://carnegieendowment.org/2019/02/20/russia-s-global-ambitions-in-perspective-pub-78067.

61. Győri L., Syrovátka J. Russian Propaganda in the Czech Republic, Slovakia and Hungary. Security and Human Rights Monitor. URL: https://www.shrmonitor.org/russian-propaganda-in-the-czech-republic-slovakia-and-hungary/.

62. Hackett R. Russian cyberwar advances military interests in Ukraine, report says. URL : http://fortune.com/2015/04/29/russiancyberwar-ukraine/.

63. Ioffe J. The History of Russian Involvement in America's Race Wars. The Atlantic. URL: https://www.theatlantic.com/international/archive/2017/10/russia-facebook-race/542796/.

64. Karmanau Y., Isachenkov V. Vladimir Putin admits for first time Russian troops took over Crimea, refuses to rule out intervention in Donetsk. URL: http://news.nationalpost.com/news/world/vladimir-putin-admits-for-first-time-russiantroops-took-over-crimea-refuses-to-rule-outintervention-in-donetsk.

65. Kenig R. How Much Can a DDoS Attack Cost Your Business? URL: https://blog.radware.com/security/2013/05/how-much-can-a-ddos-attack-cost-yourbusiness/.

66. Kerkkänen T., Kuronen A. Russia's Cyberwar in Ukraine is Relentless – This Hacktivist Strikes Back. URL: http://yle.fi/uutiset/osasto/news/russias_cyberwar_in_ukraine_is_relentless__this_hacktivist_strikes_back/8918200.

67. Koval N. Revolution Hacking. Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers. Tallinn. 2015. P. 55–58.

68. Lewis J. Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine. Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers. Tallinn. 2015. P. 39–47.

69. Lin H. Escalation Dynamics and Conflict Termination in Cyberspace. Strateg. Stud. 2012. Q. 6. P. 46–70.

70. Marshall T. Russia and the Curse of Geography. https://www.theatlantic.com/international/archive/2015/10/russia-geography-ukraine-syria/413248/.

71. Nimmo B. Fakes, Bots, and Blockings in Armenia. Medium. URL: https://medium.com/dfrlab/fakes-bots-and-blockings-in-armenia-44a4c87ebc46.

72. Nocetti J. Guerre de l'information : le web russe dans le conflit en Ukraine. Focus Strat. 2015. № 62. P. 1–47.

73. NSFocus Inc. Distributed Denial-of-Service (DDoS) Attacks: An Economic Perspective (Whitepaper). NSFocus Inc. Santa Clara. CA. 2016.

74. Paganini P. BAE Systems Applied Intelligence has disclosed a Russian cyber espionage campaign codenamed as SNAKE that targeted Governments and Military Network. URL : http://securityaffairs.co/wordpress/22875/intelligence/snake-cyber espionagecampaign.html.

75. Paganini P. Crimea – The Russian Cyber Strategy to Hit Ukraine. URL : http://resources.infosecinstitute.com/crimearussian-cyber-strategy-hit-ukraine/.

76. Pakharenko G. Cyber Operations at Maidan: A First-Hand Account. Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers. Tallinn. 2015. P. 59–66.

77. Paul C., Matthews M. The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It (No. PE-198-OSD), Perspectives. RAND Corporation, Santa Monica, CA. 2016.

78. Rumer E., Weiss A. Vladimir Putin's Russia Goes Global. Carnegie Endowment for International Peace. URL:

https://carnegieendowment.org/2017/08/04/vladimir-putin-s-russia-goes-global-pub-72736.

79. Sokolsky, R., Stronski P. The Return of Global Russia: An Analytical Framework. Carnegie Endowment for International Peace. URL: https://carnegieendowment.org/2017/12/14/return-of-global-russia-analytical-framework-pub-75003.

80. Torruella R.A., Determining Hostile Intent in Cyberspace. Jt. Force. 2014.Q. 75. P. 114–121.

81. Troianovski A., Warrick J. How a powerful Russian propaganda machine chips away at Western notions of truth. Washington Post. URL: https://www.washingtonpost.com/graphics/2018/world/national-security/russian-propaganda-skripal-salisbury/.

82. Ulrich K. Russian Interests and Strategy – Preventing Escalation in the Baltics: A NATO Playbook. Carnegie Endowment for International Peace. URL: https://carnegieendowment.org/2018/03/28/russian-interests-and-strategy-pub-75880.

83. United Nations. Memorandum on Security Assurances in Connection with Ukraine's Accession to the Treaty on the NonProliferation of Nuclear Weapons. 1994.

84. Watts C. Russia's Active Measures Architecture: Task and Purpose. Alliance For Securing Democracy. URL: https://securingdemocracy.gmfus.org/russias-active-measures-architecture-task-and-purpose/.

85. Weedon J. Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine. Cyber War in Perspective: Russian Aggression against Ukraine. Kenneth Geers. 2015.Tallinn. P. 67–77.

86. Witty R. LookingGlass Cyber Threat Intelligence Group Links Russia to Cyber Espionage Campaign Targeting Ukrainian Government and Military Officials. URL : https://www.lookingglasscyber.com/pressrelease/lookingglass-

cyber-threat-intelligencegroup-links-russia-to-cyber-espionagecampaign-targeting-ukrainian-governmentand-military-officials/.

87. Zetter K. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. URL: https://www.wired.com/2016/03/insidecunning-unprecedented-hack-ukraines-powergrid/.

ВИСНОВКИ

У дисертації здійснено системне дослідження інформаційної війни як засобу політичного насилля на теоретичному, змістовому та практичному рівнях, проаналізовано її понятійно-категоріальний каркас, інструментальне забезпечення й реалізацію у прикладному вимірі. Комплексний аналіз даної проблематики уможливив осягнення предмету і як поняття, і як явища, що особливо актуально у сучасному цифровому світі. Отримані у процесі дослідження результати дають можливість сформулювати наступні висновки:

1. Основою рефлексії теоретичних засад політичного насилля постає комплекс наукових робіт вітчизняних та зарубіжних дослідників (Г. Арендт, Ж. Бодріяр, О. Бойченко, П. Бурьє, М. Вебер, Н. Волковський, Т. Гоббс, А. Грамші, О. Дубас, Г. Жекало, А. Кампен, М. Кіца, А. Кугай, М. Лойд, Н. Луман, Н. Макіавеллі, К. Маркс, Д. Міллер, Г. Почепцов, М. Примуш, А. Сірик, К. Старостенко В. Ткач, Е. Тофлер, І. Федірко, М. Фуко тощо), у результаті опрацювання яких формується авторська інтерпретація генези та змісту політичного насилля.

Політичний інтерес, спричинений соціально-політичними потребами, оформлюється у конкретну політичну мету, є мотивацією до політичної дії, вирізняється мультисуб'єктністю (переважно групи інтересів) і в разі труднощів в процесі реалізації (протистояння різних політичних інтересів) може призвести до політичного конфлікту. Останній, у свою чергу, має два основні способи реалізації: мирний та агресивний. Мирний спосіб розгортання передбачає толерантне поводження суб'єктів по відношенню один до одного, ведення перемовин і пошук компромісного варіанту розв'язання конфлікту. Агресивний спосіб означає жорстку позицію кожного із суб'єктів протиборства, відмову від конструктивного діалогу, боротьбу за кінцеву мету будь-якою ціною. Власне, в межах останнього способу найчастіше і знаходить простір застосування політичне насилля. Його можна визначити як фізичний та/або психологічний тиск одного політичного актора (акторів) на іншого

(інших) з метою реалізації власної політичної волі у вигляді досягнення конкретної політичної цілі, що може мати як ідеалістичний, так і матеріалістичний характер.

Політичне насилля поряд з іншими різновидами (економічне, соціальне, фінансове тощо) може відбуватися в інформаційній площині і бути одним із виявів інформаційного насильства. Не все насильство в інформаційному полі можна вважати політичним. До останнього можна віднести лише заходи, коли політичні цілі досягаються інформаційним інструментарієм. Окрім інформаційної війни до його арсеналу можуть бути зараховані: інформаційна атака, інформаційна операція, інформаційна експансія.

2. Розвиток інформаційно-комунікаційних технологій суттєво вплинув на посилення інформаційної складової військових активностей, створивши новий вид війни – інформаційної, яка з 1990-тих років стала чи не одним із найбільш уживаних засобів політичної боротьби. Враховуючи той факт, що політика – це сфера управління усіма суспільними процесами, а держава є єдиним джерелом легітимного насилля, явище інформаційної війни важко помислити за межами політичного. Будь-яка війна, у тому числі інформаційна, переважно носить політичний характер, адже має за мету або ж завоювання, утримання, зміцнення політичної влади, або ж нав’язування політичної волі суб’єктами об’єктам публічного управління.

Інформація завжди була дієвим елементом політичної боротьби (агітація, пропаганда, дезінформація тощо). Але сьогодні інформаційні операції вийшли на новий рівень і можуть нести системну загрозу, приміром, електронним системам державної інфраструктури, збройних сил, енергетичної царини, національній безпеці загалом і т. д. Інформаційна війна - це сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій, або служб інформаційної інфраструктури загалом, або окремих її елементів. При дослідженні інформаційної війни стрижневим є поняття інформації. Адже інформаційна природа такого роду протистояння проявляється у тому, що

інформація є або ціллю, або джерелом або середовищем для досягнення поставленої мети.

Інформаційна війна пов’язана з контролем над інформаційною сферою, що передбачає формування та спрямування інформаційних потоків на тактичному, оперативному та стратегічному рівнях, це контроль над джерелами та розповсюдженням інформації. Вона може відбуватися у різних формах (війна у сфері командування та контролю; розвідувальна війна; радіоелектронна війна; психологічна війна; хакерська війна; економічно-інформаційна війна; кібервійна). Ведення інформаційної війни передбачає збір тактичної інформації; перевірку точності інформації; поширення пропаганди та дезінформації з метою деморалізації або маніпулювання опонентом та громадськістю; підривання якості інформації про опонента; позбавлення опонента можливості збирати інформацію тощо. Для досягнення політичних цілей переважно використовується психологічна форма інформаційної війни.

3. Інструментальний арсенал інформаційної війни забезпечує інформаційна зброя. Під останньою розуміється сукупність засобів та методів, що дозволяють викрадати, спотворювати чи знищувати інформацію; обмежувати чи припиняти доступ до неї законних користувачів; порушувати роботу або виводити з ладу телекомунікаційні мережі та комп'ютерні системи, що використовуються у забезпеченні життєдіяльності суспільства та держави. А також інформаційна зброя здатна змінювати свідомість людей, змушує їх неадекватно сприймати реальність, жити у світі ілюзій та робити згубні для себе вчинки. До ключових категорій інформаційної зброї належать: збір, передача, захист, маніпулювання, порушення, деградація та заперечення.

Перераховані вище методи можуть завдати серйозної шкоди воєнно-політичним операціям, що залежать від інформації. Сучасний контекст інформаційного суспільства робить держави та інших політичних акторів особливо у країнах з високорозвиненою інформаційно-комунікаційної інфраструктурою, з одного боку, найбільш дієвими, а з іншого, - найбільш уразливими. Тому аспект контрзасобів має не менш важливе значення.

Для атаки або захисту інформації слід використовувати такі операції: психологічні (використання інформації для впливу на міркування противника); електронна боротьба (заперечує ворогу точну інформацію); військовий обман (вводить противника в оману щодо його можливостей або намірів); фізичне знищення (перетворює накопичену енергію в руйнівну силу); заходи безпеки (заперечує інформацію про військові можливості та наміри); інформаційна атака (прямо пошкоджує інформацію, не змінюючи помітно фізичної одиниці, в якій вона знаходиться).

Інформаційна війна має спиратися на продуману стратегію як загальний план організаційних заходів. При цьому стратегія інформаційної війни має перманентно піддаватися моніторингу, оцінці та рафінуванню, адже її контексту властиві швидкі зміни та модернізація. Стратегія — це загальний план, що охоплює довготривалий проміжок часу, спосіб досягнення важливої мети. Завданням стратегії є ефективне використання наявних ресурсів для досягнення основної мети (стратегія набуває особливого значення, коли наявних ресурсів недостатньо для досягнення визначеної мети). Основні стратегії інформаційної війни: відмова в інформації; обман і мімікрія; порушення та знищення; підривна діяльність.

4. Основними «будівельними» блоками комплексного розуміння теми кібервійни є кіберпростір, кіберсила, кіберстратегія та кібервійна. Сьогодні кіберпростір офіційно занесений до переліку областей, в яких може вестись війна. Він займає п’яте місце після суходолу, моря, повітря та космосу, тому що здатність контролювати, порушувати чи маніпулювати інформаційною інфраструктурою супротивника стала настільки ж визначальною, як перевага кінетичної зброї у визначенні результату фізичних конфліктів. Кіберпростір - це всі комп’ютерні мережі у світі (не лише Інтернет) та все, що вони об’єднують та контролюють за допомогою кабелю, волоконно-оптичного або бездротового зв’язку. Влада, заснована на інформаційних ресурсах, - це кіберсила. У той час як кіберпростір — це сфера, в якій відбуваються кібероперації, кіберсила — це сума стратегічних ефектів, які генеруються

кібероперaціями в кіберпросторі та з нього. Кіберстратегія полягає в розвитку та застосуванні можливостей для роботи у кіберпросторі, інтегрованих та координованих з іншими оперативними сферами, для досягнення або підтримки досягнення цілей за допомогою елементів державної влади. Кіберстратегія ґрунтується на систематичному і структурованому поєднанні цілей (цілей і завдань), засобів (ресурсів і можливостей) і способів (як засоби використовуються для досягнення цілей) з дотриманням належного аналізу та врахуванням ризиків і витрат. Кібервійна - це конфлікт, який використовує ворожі, незаконні транзакції або атаки на комп'ютери та мережі з метою порушити комунікації та інші частини інфраструктури як механізм для нанесення економічної шкоди чи порушення захисту. Серед актуальних тенднецій кібернетичної війни можна виділити: посилення залежності від розвитку аапаратного та програмного забезпечення; зниження ресурсної витратності; домінування нападу над захистом; схильність до тиражування; зменшення вартості входу в кіберпростір тощо.

5. Міжнародний досвід протистояння політичному насиллю в інформаційному просторі підтверджує наявність спільного ворога демократичного світу в інформаційній боротьбі – РФ. Російський підхід до інформаційної війни – це глобальна стратегія, яка включає як кібер-удари, так і інформаційні операції проти більшості демократичних акторів світу (Болгарія, Грузія, Молдова, США, Франція тощо). Російські кампанії інформаційної війни впливали і продовжують чинити вплив на демократії, пропагуючи екстремізм і невдоволення, підтримуючи антидемократичних лідерів, намагаючись похитнути вплив Заходу. Російські стратегії збігаються в багатьох країнах і можуть служити різним цілям. Однак, є три загальні: відновлення російського домінування в пострадянській/імперській сфері впливу; зменшення впливу західних демократичних цінностей, інститутів та систем з метою створення поліцентричної моделі світу; розширення політичної, економічної та військової гегемонії Росії в усьому світі, щоб зміцнити місце РФ як великої держави.

Для досягнення цих цілей Росія покладається на хакерів (групи APT 28, APT 29, Turla тощо), свою все більш потужну розвідувальну спільноту, використання державних ЗМІ (наприклад, Russia Today або RT і Sputnik), ферми тролів і ботів. Хоча Російська Федерація має все більш глобальні прагнення, інформаційна війна використовується, насамперед, для встановлення російського домінування в її колишній зоні впливу, яка включає колишні радянські та комуністичні республіки та території, які раніше входили до складу Російської імперії або перебували під її впливом.

Останніми роками кібер-дії Росії виявлені в 85 країнах, що охоплюють загалом 6 континентів і 16 регіонів світу: Центральна Америка, Центральна Азія, Східна Африка, Східна Азія, Східна Європа, Північна Америка, Північна Європа, Південна Америка, Південно-Східна Азія, Південна Африка, Південна Азія, Південна Європа, Західна Азія та Західна Європа.

6. Сьогодні політико-правовий захист інформації в Україні відбувається з урахуванням зовнішніх і внутрішніх загроз, вирізняється оперативністю та дієвістю, зваженістю та системністю. Державна політика з інформаційної безпеки має стратегічну спрямованість і деталізована продуманими тактичними рішеннями. Лише так можна утримати інформаційну стабільність в середині країни, посилити підтримку України акторами в міжнародному інформаційному полі та захиститися від інформаційних провокацій ворога.

З 24 лютого 2022 року відбувається перманентне оновлення законодавства України з метою посилення інформаційної безпеки (Верховною Радою України прийнято Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції», Закон України «Про внесення змін до деяких законодавчих актів України (щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора), Закон України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності досудового розслідування за "гарячими слідами" та протидії

кібератакам», Закон України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану» тощо.

Загалом аналіз законодавчих та нормативно-правових документів дозволив вичленувати основні принципи державної політики щодо інформаційної безпеки (верховенство права; пріоритет захисту прав і свобод людини, що стосуються інформації; своєчасний і адекватний захист життєво важливих національних інтересів від реальних і потенційних загроз інформаційній безпеці; захист інформаційного суверенітету України; свобода думки, свобода слова і вільне вираження думок і переконань; свобода збору, зберігання, використання та поширення інформації тощо), її ключові напрямки (створення нормативної бази для організації розвитку інформаційного простору та його захисту від зовнішніх загроз та узгодження такої нормативної бази з нормами міжнародного права, вимогами міжнародного співробітництва та стандартами та правилами ЄС; розробка та реалізація ефективної національної інформаційної політики, спрямованої на розвиток національного інформаційного простору та гармонізацію системи контролю та координації серед практиків національної інформаційної політики та експертів з інформаційної безпеки) та загрози (комунікативні та технологічні).

Революція Гідності стала своєрідним тригером протистояння РФ та України у інформаційному просторі, злочинні активності країни-агресора в межах останнього почали активно нарощуватися, що змусило вітчизняні державні структури удосконалювати свій інформаційно-цифровий потенціал задля здійснення гідної відсічі ворожим зазіханням. Аналіз двох ключових аспектів (змістового наповнення інформаційного дискурсу Росії та

технологічного способу його донесення до аудиторії) дозволив виявити особливості інформаційної війни в українських реаліях.

Інформаційна війна Росії проти України провадилася и триває у трьох площинах: у межах власного інформаційного простору для закріплення у свідомості росіян хибних інформаційних патернів щодо українців, нашої держави, її офіційних представників, міжнародної діяльності тощо; у межах українського інформаційного поля з метою дезінформації, формування недовіри громадян до політичної влади, закладання підсвідомих страхів і т. д.; у світовому інформаційному просторі задля поширення неправдивих наративів щодо України. Усі ці активності інформаційного характеру мають політичну мету – шляхом дискредитації української держави та її населення виправдати зазіхання на суверенітет, територію та політичну владу в Україні.

Кібератаки, які використовує Росія проти України, можна класифікувати за трьома типами: DDoS-атаки, пошкодження веб-сайтів та зараження зловмисним програмним забезпеченням шляхом фішингу. Перші два інструменти точніше описуються як кібер-зриви, тоді як останній більш спрямований на кібершпигунство для збору розвідданих і підготовки поля бою до подальших кінетичних наступів або кібератак. Останні можуть чинити тимчасовий збій у роботі банківської та фінансової систем, енергетичної галузі, системах мобільного та стаціонарного зв’язку тощо, що у свою чергу, може негативно відбиватися на життєзабезпеченні населення, координованості дій різних гілок влади, комунікації між громадянами та з громадянами і т. д. Однак, у довгостроковій перспективі вони можуть сприяти удосконаленню вітчизняної системи цифрової та інформаційної безпеки, проактивній позиції держави, міжнародній співпраці у протистоянні агресору, обізнаності населення у технологіях цифрової та інформаційної боротьби, гігієні українських соціальних мереж тощо.

Досвід нашої держави може стати у нагоді для багатьох інших країн, які бажаючи лишатися відкритими та демократичними, мають дбати про безпеку власного інформаційного поля. Зокрема, вони повинні активно намагатися

зміцнити свою позицію, щоб їхня держава не стала жертвою пропагандистських кампаній. Крім того, вони повинні підвищити кібербезпеку державних онлайн-інфраструктур від атак розподіленої відмови в обслуговуванні та пошкодження веб-сайтів. Також покращення кібербезпеки може бути пов’язане з обмеженням залежності від іноземних технологій та наданням рекомендацій приватному сектору щодо того, як реагувати на кібератаки. Демократичні держави повинні уважно стежити за тим, як розвивається україно-російське протистояння у інформаційному просторі, і сприяти заходам зміцнення довіри на міжнародному рівні.