УДК 343.91(477) *DOI: https://doi.org/10.32631/vca.2023.3.56*

Петро Петрович ГАЛУШКО
(Харківський національний університет внутрішніх справ, м. Харків)

ПОЛІТИЧНІ ТА ВІЙСЬКОВІ ФАКТОРИ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ В УМОВАХ ВІЙНИ

Стаття присвячена дослідженню політичний та військових факторів кіберзлочинності в умовах війни. крізь призму комплексної кримінологічної теорії детермінації. Зроблено висновок про те, що традиційні уявлення про злочинність, війну та інформаційне протистояння більше не є адекватними для опису нової реальності, що склалася. Головними детермінантами, тобто причинами, що породили безпрецедентний сплеск та якісну трансформацію ворожої кіберактивності, є політична воля та військова стратегія держави-агресора. Війна створила умови, в яких кіберпростір перетворився на повноцінний театр бойових дій, а кібероперації стали невід'ємним інструментом досягнення військових та політичних цілей. Це призвело до появи гібридної форми державної злочинності, яка нерозривно пов'язана зі збройним конфліктом і не може бути адекватно проаналізована поза його контекстом.

Ключові слова: *кіберзлочинність, кібератака, кібероперація, детермінація, політика, війна, агресія, збройний конфлікт, протидія.*

Постановка проблеми. Війна Росії проти України стала трагічним, але потужним каталізатором для переосмислення безпеки у XXI столітті. Вона продемонструвала, що в епоху цифрової взаємозалежності кіберпростір є невід'ємною частиною будь-якого конфлікту. Майбутнє цивілізованого, мирного використання кіберпростору залежить від здатності демократичних суспільств засвоїти ці уроки та побудувати багатошарову, стійку та інтегровану систему захисту проти рішучих державних супротивників, для яких кіберпростір є лише ще одним полем бою.

Дивлячись у майбутнє, необхідно враховувати нові виклики, що стоять перед Україною. Головний урок, винесений з досвіду майже дворічного протистояння України російській агресії, полягає в тому, що кіберзахист перестав бути суто технічним питанням і перетворився на елемент національної безпеки та загальносуспільної стійкості. У зв'язку з цим поглибленого дослідження потребують військові та політичні фактори детермінації кіберзлочинності.

Проблеми детермінації кіберзлочинності ставали предметом наукової уваги низки дослідників, таких, зокрема, як Д. С. Азаров, Р. В. Бараненко, Л. В. Борисова, М. О. Кравцова, О. В. Манжай, Д. В. Пашнєв, В. В. Топчій, К. О. Черевко та ін. Водночас вплив специфічних політичних та військових факторів на кіберзлочинність не був досліджений та потребує здійснення

відповідного аналізу.

Мета статті полягає у виявленні, описі та поясненні основних політичних та військових факторів детермінації кіберзлочинності в Україні.

Виклад основного матеріалу. Повномасштабне вторгнення російської федерації в Україну 24 лютого 2022 року стало не лише ескалацією восьмирічної збройної агресії, а й каталізатором фундаментальної трансформації глобального ландшафту безпеки. Воно ознаменувало перехід до нової епохи гібридної війни, де кіберпростір перестав бути лише ареною для шпигунства, дезінформації та економічних злочинів, перетворившись на повноцінний театр військових дій[1]. У цьому новому контексті те, що за інерцією продовжують називати «кіберзлочинністю», насправді є невід'ємним компонентом державної військової та політичної стратегії, інструментом для досягнення цілей на полі бою та в геополітичному протистоянні.

Природа, масштаби та еволюція кіберзлочинності, починаючи з лютого 2022 року визначаються, насамперед, політичними та військовими цілями держави-агресора, російської федерації. Цей процес призвів до розмивання меж між діяльністю хакерських угруповань, що спонсоруються державою, традиційною кримінальною активністю, військовими операціями та діями, що за своєю суттю є воєнними злочинами згідно з міжнародним гуманітарним правом. Сама війна виступає головним детермінантом, створюючи як *причини* (стратегічні цілі агресії), так і *умови* (вороже цифрове середовище, використання даних як зброї, мобілізація недержавних суб'єктів) для виникнення та поширення цього феномену.

Тож в умовах міжнародного збройного конфлікту традиційний кримінологічний вокабулар, що послуговується узагальненим терміном «кіберзлочинність» виявляється недостатніми. Він не відображає ключової відмінності між діяльністю фінансово мотивованого кіберзлочинця та діями військовослужбовця ворожої армії, який виконує наказ свого командування, використовуючи ті самі технічні інструменти.

Провідні міжнародні аналітичні центри, такі як Microsoft, пропонують більш диференційований підхід, чітко розмежовуючи три категорії загроз:

1. Кібератаки, що спонсоруються державою (*Nation-state threat attacks*): зловмисні кібератаки, що походять з певної країни та мають на меті просування її інтересів, часто зумовлені геополітичною конкуренцією.

2. Кіберзлочинна діяльність (*Cybercriminal activity*): діяльність, типово мотивована фінансовою вигодою.

3. Операції впливу (*Influence operations, IO*): скоординоване застосування національних можливостей (дипломатичних, інформаційних, військових, економічних) для формування поглядів та рішень іноземних цільових аудиторій[2].

[1] Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression / Microsoft On the Issues. 04.11.2022. URL: https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/

[2] Microsoft Corporation. Microsoft Digital Defense Report 2024 URL: https://cdn-dynmedia-

Повномасштабна війна росії проти України продемонструвала, що агресор цілеспрямовано поєднує всі три категорії в єдину гібридну стратегію. Атаки на державні реєстри, що підпадають під визначення «кіберзлочину», є частиною військової операції, спрямованої на дестабілізацію, а їх висвітлення у пропагандистських медіа стає елементом операції впливу. Таким чином, для адекватного аналізу необхідно перейти від вузького поняття «кіберзлочинність» до ширшого – «ворожі кібероперації», що охоплює весь спектр зловмисної діяльності в цифровому просторі, керованої державою-агресором.

Головною причиною сплеску та якісної зміни ворожих кібероперацій є політичне рішення керівництва російської федерації про ведення повномасштабної агресивної війни та військові стратегії, спрямовані на досягнення її цілей (окупація територій, знищення державності, придушення спротиву). Саме ці стратегічні цілі породжують потребу в кібератаках як інструменті війни.

Умовами, що сприяють реалізації цих причин, є сам стан війни та його наслідки. Аналогічно до того, як війна створює умови для традиційної організованої злочинності в Причорноморському регіоні (незаконний обіг зброї, схеми з гуманітарною допомогою, корупція на тлі змін у митному регулюванні)[1], вона створює ідеальні умови для кібероперацій. До них належать:

– підвищена залежність держави, військових та цивільного населення від цифрових комунікацій та інфраструктури;

– масова міграція населення та створення величезних баз даних переселенців, що стають ціллю для атак;

– психологічна вразливість суспільства, що робить його більш сприйнятливим до дезінформації та операцій впливу;

– поява великої кількості патріотично налаштованих хакерів та волонтерів з обох боків, що розмиває межі між державними та недержавними суб'єктами;

– проліферація даних як зброї, де викрадена інформація використовується для шантажу, розвідки та психологічного тиску [2].

Такий підхід, що базується на комбінуванні теорій детермінації, дозволяє зробити важливий висновок. Традиційні методи боротьби зі злочинністю, що застосовуються правоохоронними органами, такими як Департамент кіберполіції Національної поліції України, розраховані на усунення умов злочинності (соціальних, економічних) та переслідування окремих виконавців у рамках національної юрисдикції. Однак, коли причиною злочинної діяльності є свідома політика іншої суверенної

1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20(1).pdf

[1] Джелілова М. А. Причини та умови організованої злочинності в умовах воєнного стану: регіональний аспект. *Протидія злочинності: проблеми практики та науково-методичне забезпечення*. 2023. № 2. С. 25–35. DOI: https://doi.org/10.32850/sulj.2023.2.2.

[2] Там само.

держави, ці методи стають недостатніми. Причина – стратегічні цілі агресора, блокування можливості реалізації яких знаходиться поза досяжністю національних правоохоронних органів. Це пояснює і те, чому ефективна протидія ворожим кібероперaціям вимагає не лише зусиль кіберполіції, а й комплексного застосування інструментів державної політики: військового кіберзахисту (що здійснюється, наприклад, Держспецзв'язку та СБУ)[1], міжнародних санкцій, дипломатичної ізоляції та, що найважливіше, застосування норм міжнародного гуманітарного та кримінального права. Таким чином, комбінована кримінологічна рамка детермінації пояснює, чому відповідь на кіберагресію закономірно перемістилася з суто правоохоронної у геополітичну, військово-політичну площину.

Політичні цілі російської федерації у війні проти України є першочерговим і найпотужнішим детермінантом, що визначає спрямованість, характер та інтенсивність ворожих кібероперацій. Ці операції є системними, цілеспрямованими, інтегрованим до більш масивної системи військово-політичного протистояння, націлені на досягнення конкретних стратегічних результатів.

За даними Служби безпеки України, лише за початок 2023 року було нейтралізовано майже чотири тисячі кібератак. Переважна більшість цих атак була спрямована на електронні системи центральних органів влади та об'єкти критичної інфраструктури з метою отримання несанкціонованого доступу до державного документообігу та технологічних систем управління. Це свідчить про чітку військову мету: паралізувати державне управління, посіяти хаос, порушити функціонування життєво важливих для суспільства систем та отримати розвідувальні дані в рамках стратегії гібридної війни[2]. Аналітичні звіти підтверджують цю тенденцію, фіксуючи мільйони кібератак на державний сектор, що включають фішинг та дезінформаційні кампанії, які є інструментами політичної дестабілізації.

Аналіз, проведений провідними світовими компаніями, такими як Google та Mandiant, дозволяє виокремити три головні політичні цілі, які держава-агресор переслідує за допомогою кібернетичних та інформаційних операцій[3]. Ця тріада формує стрижень російської гібридної стратегії:

1. Підрив українського уряду та деморалізація суспільства. Ця мета досягається через систематичні руйнівні атаки на державні інформаційні ресурси, веб-сайти міністерств та відомств, банківську систему та критичну інфраструктуру[4]. Дефейсменти (зміна зовнішнього вигляду) урядових

[1] Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 року / Державна служба спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/uk/articles/233

[2] СБУ з початку року нейтралізувала майже 4 тисячі кібератак на Україну. *Укрінформ*. 2023. 26 жовтня. URL: https://www.ukrinform.ua/rubric-society/3778970-sbu-z-pocatku-roku-nejtralizuvala-majze-4-tisaci-kiberatak-na-ukrainu.html

[3] Huntley S. Fog of war: how the Ukraine conflict transformed the cyber threat landscape. // The Keyword : офіц. блог Google.16.02.2023. URL: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

[4] Wahlstrom A., Revelli A., Riddell S., Mainor D., Serabian R. The IO Offensive: Information Operations

сайтів, поєднані з погрозами, мають на меті посіяти паніку та підірвати довіру громадян до здатності держави захистити їхні дані та забезпечити стабільне функціонування.

2. Розкол міжнародної підтримки України. Цей напрям роботи спрямований на союзників України, насамперед країни-члени НАТО. Російські хакерські угруповання проводять агресивні шпигунські кампанії проти урядових та військових структур країн Альянсу, намагаючись отримати розвідувальні дані про обсяги та характер допомоги Україні. Згідно зі звітом Microsoft[1], у певний період 90% російських атак були спрямовані на країни НАТО. Одночасно розгортаються масштабні дезінформаційні кампанії, покликані дискредитувати Україну та її керівництво в очах західної аудиторії. Прикладом є поширення фейкових наративів про нібито продаж Україною західної зброї терористичним угрупованням, таким як ХАМАС, для підриву довіри та припинення військової допомоги[2].

3. Підтримання внутрішньої репресивної політики всередині самої росії, в якій, за слушним зауваженням Ю. В. Орлова, сформувався повноцінний фашистський політичний режим. Так, зокрема, дослідник наголошує на тому, що «сучасний російський фашизм має в своїй основі розгалужений метакомплекс факторів колективного безсвідомого, чільне місця в яких обіймає патерналізм, істерії страху, неврози нав'язливих станів, ресентимент, ворожість до естетично розвинених культурних патернів. Водночас вдалося встановити, що російський фашизм не є ідеологічним. Натомість в першу чергу він є травматичним, а у другу – міфологічним, фальсифіковано-комеморальним, мегалотимно-реваншистським, замкненим у циклосі ХХ ст. Фантазми звільнення від пут культури й поринання у минуле вибудовуються на платформі величі-жертовності, мілітарної етики й естетики, невротичної установки на боротьбу, що фіксується культурою страждання та, разом з тим, табу на дослідження дійсних джерел останнього, фальсифікації причин колективного травмування, вибірково-історичної амнезії»[3].

При цьому, небезпідставно підкреслює Ю. В. Орлов, «патерналізм зумовлює таку рису соціального характеру як конформність. Як і патерналізм конформність в цілому є нормою. Однак при гіпертрофованому, архетипізованому етатизмі й конформність набуває ентропійного значення, що надміру звужує простір для індивідуальності, унікальності, зрештою й свободи як такої. Саме конформність і конформізм є одним з базових

Surrounding the Russian Invasion of Ukraine // Google Cloud Blog : офіц. блог Google. 19.05.2022. URL: https://cloud.google.com/blog/topics/threat-intelligence/information-operations-surrounding-ukraine.

[1] Brut T. Microsoft. Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression. *Microsoft On the Issues*. 04.11.2022. URL: https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/

[2] Watts C. Russian influence and cyber operations adapt for long haul and exploit war fatigue. *Microsoft On the Issues*. 07.12.2023. URL: https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/

[3] Орлов Ю. В. Злочинність і протидія їй в умовах війни: кримінально-правовий та кримінологічний виміри : монографія / Кримінол. асоц. України. Харків : Право, 2023. С. 123.

стовпів багаточисельності й безсловесності підданих по натурі як соціальної бази сучасного російського фашизму»[1]. Конформність же вимагає жорсткої цензури, контролю за поширенням інформації.

Тож «кремль» використовує кібероперації та пропаганду для формування вигідного йому наративу всередині країни. Це включає виправдання агресії, дискредитацію будь-яких альтернативних джерел інформації та створення образу «колективного Заходу» як ворога. Аналіз, здійснений експертами Google, показує, що понад 90% виявлених прихованих інформаційних операцій на його платформах велися російською мовою і були спрямовані саме на внутрішню аудиторію[2].

Поєднання кібератак та інформаційних операцій є наріжним каменем російської гібридної війни. Фактично, умовою успішності інформаційно-психологічних операцій в низці випадків постає успішна кібератака. Така узалежненість дозволяє ворожі інформаційні кампанії (інформаційно-психологічні операції) розглядати в числі умов воєнно-контекстуальної кіберзлочинності. Аналіз конкретних випадків демонструє, наскільки глибоко інтегровані ці два компоненти. Розглянемо окремі з них.

Наратив про «біолабораторії»[3]. Ця дезінформаційна кампанія, розгорнута наприкінці 2021 року, слугувала ідеологічним підґрунтям для виправдання майбутнього вторгнення. Microsoft детально описує її триетапний підхід, що імітує військову операцію:

1. Попереднє розміщення (Pre-positioning): Заздалегідь у публічний простір через маргінальні сайти та акаунти в соцмережах вкидаються фейкові «документи» та наративи. Це аналогічно до попереднього розміщення шкідливого програмного коду в мережі жертви.

2. Скоординований запуск (Launch): У визначений момент, сприятливий для досягнення політичних цілей, запускається масована кампанія з поширення цих наративів через державні та підконтрольні ЗМІ (RT, Sputnik) та мережу ботів.

3. Посилення (Amplification): Проксі-ресурси та «лідери думок» підхоплюють та посилюють наратив, створюючи ефект інформаційної лавини, спрямованої на цільову аудиторію[4].

«Глибокі фейки» (Deepfakes) та психологічний тиск. У березні 2022 року російські спецслужби здійснили комплексну операцію, що поєднувала технічну атаку та психологічний вплив. Було створено та поширено ШІ-згенероване відео («*deepfake*»), де Президент України Володимир Зеленський нібито оголошує про капітуляцію. Поширення цього відео було

[1] Там само. С. 123.

[2] Wahlstrom A., Revelli A., Riddell S., Mainor D., Serabian R. The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine // Google Cloud Blog : офіц. блог Google. 19.05.2022. URL: https://cloud.google.com/blog/topics/threat-intelligence/information-operations-surrounding-ukraine.

[3] Іноземні біолабораторії в Україні: чергові витки роспропаганди / Міністерство цифрової трансформації України ; Центр протидії дезінформації. Київ : Мінцифра, б.д. URL: https://cpd.gov.ua.

[4] Cyber influence operations // *Microsoft Digital Defense Report 2022* / Microsoft. URL: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-cyber-influence-operations

синхронізовано зі зламом та дефейсментом сайту телеканалу «Україна 24» та запуском фейкового повідомлення в рухомому рядку телевізійного ефіру. Ця операція була розрахована на те, щоб посіяти паніку та підірвати волю до спротиву в перші, найважчі тижні вторгнення[1].

Експлуатація сервісу Cameo. Цей випадок демонструє винахідливість та цинізм російських інформаційних операцій. Агенти ГРУ через сервіс Cameo, де можна замовити відеопривітання від знаменитостей, замовляли ролики у американських компаній та музикантів (зокрема, Елайджі Вуда, Діна Норріса, Прісцилли Преслі).[2] Потім ці відео монтувалися, до них додавалися емодзі, посилання та логотипи медіа, і вони поширювалися в соцмережах для просування давнього фейкового наративу про нібито наркотичну залежність Президента Зеленського.

Ці приклади ілюструють фундаментальний зсув у природі загроз. Традиційно кібербезпека (зона відповідальності Держспецзв'язку, кіберполіції) та протидія дезінформації (відповідальність центрів стратегічних комунікацій, прес-служб) існували в окремих підрозділах, організаціях. Однак російська стратегія не бачить між ними різниці. Злам сайту є лише засобом доставки для інформаційної «боєголовки» – фейкового відео. Викрадення даних використовується не для фінансової вигоди, а для підтримки політичного наративу. Це означає, що ефективна оборона більше не може бути суто технічною. Захист від вторгнення є лише першим кроком; не менш важливим є спростування наративу, який це вторгнення мало на меті поширити. Таким чином, успішна протидія вимагає створення нової, інтегрованої моделі оборони, що поєднує технічну стійкість, розвідку, правоохоронну діяльність та стратегічні комунікації в єдиний, скоординований механізм[3].

Політичний детермінант безпосередньо визначає характер та інструментарій технічної атаки. Військові цілі російської федерації є другим ключовим детермінантом, що формує ландшафт кібервійни. Кібероперації не існують у вакуумі; вони глибоко інтегровані у загальний план ведення бойових дій, слугуючи як для досягнення тактичної переваги на полі бою, так і для реалізації ширших стратегічних завдань з виснаження супротивника.

Аналітики компанії Mandiant ідентифікували та детально описали стандартизований, повторюваний сценарій (*playbook*), який використовує ГРУ рф для проведення руйнівних кібероперацій в Україні[4]. Цей сценарій є, по суті, військовою доктриною, розробленою для підвищення швидкості,

---

[1] Зеленський заявив, що президентом бути складно й оголосив капітуляцію України. *Детектор медіа*. 2022. 16 березня 2022 р. URL: https://disinfo.detector.media/post/zelenskyi-zaiavyv-shcho-prezydentom-buty-skladno-i-oholosyv-kapituliatsiiu-ukrainy.

[2] Watts C. Russian influence and cyber operations adapt for long haul and exploit war fatigue. *Microsoft On the Issues*. 07.12.2023. URL: https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/

[3] Smith B. Defending Ukraine: Early Lessons from the Cyber War / Microsoft. URL: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

[4] Black D., Roncone G. The GRU's Disruptive Playbook. *Google Cloud Blog*. 12.07.2023. URL: https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook.

масштабу та інтенсивності атак при одночасному зниженні ризику їх виявлення. Він складається з п'яти основних компонентів:

1. «Життя на краю» (*Living on the Edge*): операція починається з компрометації периметрових пристроїв мережі – маршрутизаторів, брандмауерів, VPN-шлюзів. Ці пристрої часто мають слабший захист і моніторинг, ніж сервери та робочі станції. Отримавши контроль над ними, зловмисники створюють стійкий і важкодоступний для виявлення плацдарм для подальшого проникнення в мережу.

2. «Життя за рахунок землі» (*Living off the Land*): після отримання початкового доступу хакери ГРУ уникають використання унікального, кастомного шкідливого програмного забезпечення. Натомість вони максимально використовують легітимні, вбудовані в операційну систему інструменти, такі як PowerShell, Windows Management Instrumentation (*WMI*) та інші системні утиліти. Це дозволяє їм маскувати свою діяльність під звичайну активність системних адміністраторів, що значно ускладнює виявлення.

3. «Атака на групові політики» (*Going for the GPO*): ключовою тактичною ціллю всередині скомпрометованої мережі є контролер домену та об'єкти групової політики (Group Policy Objects, GPO). Захопивши контроль над GPO, зловмисники отримують можливість одночасно та з найвищими привілеями розгорнути шкідливий код на сотнях або тисячах комп'ютерів у мережі, що забезпечує максимальний руйнівний ефект.

4. «Руйнуй та заперечуй» (*Disrupt and Deny*): на фінальному етапі через скомпрометовані GPO розгортаються деструктивні інструменти. Це можуть бути спеціалізовані програми-вайпери (*wiper*), єдиною метою яких є безповоротне знищення даних (наприклад, *CaddyWiper)*, або фальшиві програми-вимагачі (наприклад, *WhisperGate*), які імітують фінансове вимагання, але насправді також знищують дані, додаючи елемент психологічного тиску та заплутування слідства.

5. «Телеграфування «успіху»» (*Telegraphing «Success»*): паралельно з технічною атакою або одразу після неї, через підконтрольні Telegram-канали та акаунти фейкових «хактивістських» груп поширюється інформація про «успішний злам». Мета цього етапу — посилити психологічний ефект від атаки, створити враження всемогутності російських хакерів та посіяти паніку, незалежно від реального технічного збитку, завданого операцією[1].

Систематичні та скоординовані атаки на критичну інфраструктуру України є найяскравішим проявом військової складової кіберагресії. Звіт Microsoft Digital Defense Report за 2022 рік зафіксував істотні й негативні структурно-динамічні зміни: частка атак на об'єкти критичної інфраструктури зросла з 20 % до 40 % від усіх атак, що спонсоруються

[1] Black D., Roncone G. The GRU's Disruptive Playbook. *Google Cloud Blog*. 12.07.2023. URL: https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook.

державами, і цей ріст прямо пов'язується з військовими цілями росії в Україні[1].

Ключовою особливістю цих атак є їхня тісна координація з фізичними ударами, що демонструє їх вмонтованість до єдиного військового планування.

Висновки. Аналіз політичних та військових факторів кіберзлочинності в Україні в умовах війни, проведений крізь призму комплексної кримінологічної теорії детермінації, дозволяє зробити низку фундаментальних висновків щодо природи сучасних конфліктів. Традиційні уявлення про злочинність, війну та інформаційне протистояння більше не є адекватними для опису нової реальності, що склалася.

Синтез представлених даних підтверджує основний висновок цієї частини нашого дослідження: головними детермінантами, тобто причинами, що породили безпрецедентний сплеск та якісну трансформацію ворожої кіберактивності, є політична воля та військова стратегія держави-агресора. Війна створила умови, в яких кіберпростір перетворився на повноцінний театр бойових дій, а кібероперації стали невід'ємним інструментом досягнення військових та політичних цілей. Це призвело до появи гібридної форми державної злочинності, яка нерозривно пов'язана зі збройним конфліктом і не може бути адекватно проаналізована поза його контекстом.

Агресивна війна росії проти Україні остаточно довела злиття інтересів, підходів гібридної війни. Фізичні, кібернетичні та інформаційні операції більше не є трьома окремими війнами; це три фронти єдиного, інтегрованого конфлікту. Успіх чи поразка на одному фронті безпосередньо впливає на інші. Відтак і протидія кіберзлочинності в умовах війни – задача не автономна. Її реалізація передбачає здійснення глибокої інтегрованості заходів із забезпечення кібербезпеки до структур протидії широкому спектру різнорідних загроз від держави-агресора у поєднанні із функціонуванням системам внутрішньої кібернетичної стійкості, запобігання ординарним кримінальним правопорушенням у кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Джелілова М. А. Причини та умови організованої злочинності в умовах воєнного стану: регіональний аспект. *Протидія злочинності: проблеми практики та науково-методичне забезпечення*. 2023. № 2. С. 25–35. DOI: https://doi.org/10.32850/sulj.2023.2.2.

2. Зеленський заявив, що президентом бути складно й оголосив капітуляцію України. *Детектор медіа*. 2022. 16 березня 2022 р. URL: https://disinfo.detector.media/post/zelenskyi-zaiavyv-shcho-prezydentom-buty-skladno-i-oholosyv-kapituliatsiiu-ukrainy.

[1] Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression. *Microsoft On the Issues.* 04.11.2022. URL: https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/

3. Іноземні біолабораторії в Україні: чергові витки роспропаганди / Міністерство цифрової трансформації України ; Центр протидії дезінформації. Київ : Мінцифра, б.д. URL: https://cpd.gov.ua.

4. Іноземні біолабораторії в Україні: чергові витки роспропаганди / Міністерство цифрової трансформації України ; Центр протидії дезінформації. Київ : Мінцифра, б.д. URL: https://cpd.gov.ua/articles/inozemni-biolaboratoriyi-v-ukrayiniche/

5. Орлов Ю. В. Злочинність і протидія їй в умовах війни: кримінально-правовий та кримінологічний виміри : монографія / Кримінол. асоц. України. Харків : Право, 2023. 252 с.

6. СБУ з початку року нейтралізувала майже 4 тисячі кібератак на Україну. *Укрінформ*. 2023. 26 жовтня. URL: https://www.ukrinform.ua/rubric-society/3778970-sbu-z-pocatku-roku-nejtralizuvala-majze-4-tisaci-kiberatak-na-ukrainu.html.

7. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом 2022 року / Державна служба спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/uk/articles/233.

8. Black D., Roncone G. The GRU's Disruptive Playbook. *Google Cloud Blog*. 12.07.2023. URL: https://cloud.google.com/blog/topics/threat-intelligence/gru-disruptive-playbook.

9. Brut T. Microsoft. Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression. *Microsoft On the Issues*. 04.11.2022. URL: https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/

10. Cyber influence operations // *Microsoft Digital Defense Report 2022* / Microsoft. URL: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022-cyber-influence-operations.

11. Huntley S. Fog of war: how the Ukraine conflict transformed the cyber threat landscape. // The Keyword : офіц. блог Google.16.02.2023. URL: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

12. Microsoft Corporation. Microsoft Digital Defense Report 2024 URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20(1).pdf.

13. Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression / Microsoft On the Issues. 04.11.2022. URL: https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/

14. Smith B. Defending Ukraine: Early Lessons from the Cyber War / Microsoft. URL: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

15. Wahlstrom A., Revelli A., Riddell S., Mainor D., Serabian R. The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine // Google Cloud Blog : офіц. блог Google. 19.05.2022. URL: https://cloud.google.com/blog/topics/threat-intelligence/information-operations-surrounding-ukraine.

16. Watts C. Russian influence and cyber operations adapt for long haul and exploit war fatigue. *Microsoft On the Issues*. 07.12.2023. URL: https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/

Стаття надійшла до редакції 09.12.2023

Petro P. HALUSHKO,
Postgraduate Student
(Kharkiv National University of Internal Affairs, Kharkiv, Ukraine)

POLITICAL AND MILITARY FACTORS OF CYBERCRIME IN UKRAINE IN WAR CONDITIONS

The article is devoted to the study of political and military factors of cybercrime in war conditions. through the prism of a complex criminological theory of determination. The conclusion is made that traditional ideas about crime, war and information confrontation are no longer adequate to describe the new reality that has developed. The main determinants, that is, the reasons that gave rise to an unprecedented surge and qualitative transformation of hostile cyberactivity, are the political will and military strategy of the aggressor state. The war created conditions in which cyberspace turned into a full-fledged theater of hostilities, and cyber operations became an integral tool for achieving military and political goals. This has led to the emergence of a hybrid form of state crime, which is inextricably linked to armed conflict and cannot be adequately analyzed outside its context.

Keywords: *cybercrime, cyberattack, cyberoperation, determination, politics, war, aggression, armed conflict, counteraction.*