CYBER DIMENSIONS OF POLITICAL DISCOURSE

DOI: 10.46340/eppd.2021.8.4.11

Vasyl Tarkin
ORCID ID: https://orcid.org/0000-0002-1754-9046
National University "Odesa Law Academy", Ukraine

THE FIGHT IN CYBERSPACE: INFORMATIONAL WARFARE AND CYBERTERRORISM

Василь Таркін
Національний університет «Одеська юридична академія», Україна

БОРОТЬБА У КІБЕРПРОСТОРІ: ІНФОРМАЦІЙНІ ВІЙНИ І КІБЕРТЕРОРИЗМ

"Information warfare" is a term of the late twentieth century, which means a combination of human or technological actions designed to appropriate, destroy or change information or impose a certain vision of reality. Information warfare is a high-tech form of traditional kinetic warfare but based on extensive computerization and electronification. It is also an armed conflict; however, information-technical and program-mathematical resources act as a weapon. Cyberwarfare can exist both as an independent phenomenon and as an accompanying routine to military action, increasing their chances of success. Information technologies are not only involved as the weapon of modern warfare, but they also have a strong impact on the process of obtaining and storage of intelligence and strategic planning.

The digital revolution and the ability to be a full participant of the modern world is already a part of anthropology: to teach, to inform, to have fun, and to communicate regardless the distance and borders. Global informatization has made the world community, the integrity of which is largely ensured by including through intensive information exchange, more vulnerable – stoppage of information contacts even for a short period of time may lead to a crisis at the national or international level. The transformation of the field of information technology and its irreplaceable nature has turned it from a tool into a goal.

Socio-economic, political, and cultural transformations are inextricably linked to the process of informatization, however, the new way of social functioning and the transition of information to the category of valuable resources led to new challenges, including information warfare and cyberterrorism, the phenomenon of which is of scientific interest.

Keywords: information warfare, cyberterrorism, cyberattack, levels of informational and technical warfare, methods of informational and technical warfare.

Актуальність теми наукового дослідження. Цифровізація впевнено крокує планетою, характеризується зростаючою роллю інформації в усіх сферах життя і діяльності людини, розглядає її як системоутворюючий фактор сучасного суспільства, що активно впливає на стан політичної, економічної, оборонної й інших складових безпеки держави, на можливість виконання її соціальних функцій, задовольняти основні потреби населення, надавати послуги. Водночас, науково-технічна революція породила нові форми конфліктів: інтенсивні, небезпечні, масштабні. У боротьбі за сфери економічного й політичного впливу акцент із застосування фізичної сили усе більше зміщується у сторону прихованих і гнучких форм агресії. Інформаційні війни і кібертероризм – серйозні загрози із пагубним впливом. Ці явища характеризуються складністю ідентифікації джерела агресії, контрольованим, дозованим нанесенням шкоди, непередбачуваністю наслідків і важливим є розуміння картини цих загроз, особливо, на фоні кризи стану наукового світогляду у теоретизації інформаційних війн і кібертероризму, хоча, чимала кількість науковців, і вітчизняних, і зарубіжних конструювали і викладали своє бачення природи цих понять, **серед таких вчених**: Г. В. Пєвцов,

С. В. Залкін, С. О. Сідченко, К. І. Хударковський[1], А. В. Манойло[2], С. П. Расторгуєв[3], Д. В. Кіслов[4]., В. М. Брижко, М. Я. Швець, В. С. Цимбалюк[5], Я. М. Жарков[6], Г. Г. Почепцов[7], М. І. Сенченко[8] та ін. Різні підходи до розуміння, теоретичного осмислення інформаційних війн і кібертероризму через складність і багатомірність цих понять лише поглиблюють плюралізм розуміння як самих категорій, так і їх основних складових.

Мета статті – викладення власного бачення на природу інформаційних, насамперед, інформаційно-технічної війни із виокремленням її форм та методів, кібертероризму, а також порівняльна характеристика цих двох явищ.

Виклад основного матеріалу дослідження. Сьогодні кіберпростір можна порівняти із повноцінним театром бойових дій, на рівні із наземним, повітряним, морським. Цифрова платформа останніми роками все частіше тріщить на різних рівнях – від локального − окремих компаній до фундаментального − об'єктів критичної інфраструктури. Масштаби інформаційних загроз зростають разом із цифровізацією.

У 2005 році Габрієль Вейнман відмітив: «із психологічної точки зору два найбільших страхи сучасності об'єднані терміном кібертероризм…страх перед цією загрозою перебільшено: поки що не зареєстровано жодного випадку кібертероризму, хакерів регулярно приймають за терористів, а кіберзахист надійніший, ніж здається на перший погляд»[9]. А вже у 2021 році питання кібертероризму і кібератак відносяться до глобальних людських проблем, протидія яким стає предметом обговоренням на світовому рівні[10]. Однак, чи можемо ми на разі говорити про **реальність існування** кібертероризму?

Теза зарубіжного дослідника про те, що «хакерів регулярно приймають за терористів» актуальна і досі. Межа між інформаційними війнами і кібертероризмом остаточно не проведена: у наукових роботах критерії розмежування термінів «інформаційна війна» та «кібертероризм» відсутні. В.Ф. Прокоф'єв, ще у роботі 2003 року наголошував, що «термінологія у цій області (*інформаційного протиборства – курсив наш*) не встановилася. Майже кожен із авторів пропонує своє визначення того чи іншого поняття». Науковець визначає «інформаційну війну» як «широкомасштабну інформаційну боротьбу із застосуванням способів і засобів інформаційного впливу на психіку людей, насамперед, на їх індивідуальну і суспільну свідомість, а також на функціонування технічних засобів в інтересах досягнення цілей сторони, яка впливає»[11]. В. Д. Кіслов надає таку наукову експлікацію: «це одна з основних форм конкурентної боротьби

[1] Пєвцов, Г. В., Залкін, С. В., Сідченко, С. О., Хударковський, К. І. (2019). Методичний підхід до формування сценарію проведення інформаційно-психологічного впливу на осіб, що приймають рішення. *Системи обробки інформації, 1 (156),* 74-81; Пєвцов, Г. В., Залкін, С. В., Сідченко, С. О., Хударковський, К. І. (2019). Методичний підхід до кластеризації інформаційних повідомлень в ході протидії інформаційно-психологічним впливам противника. *Наука і техніка Повітряних Сил Збройних Сил України, 2 (35),* 39-46; Пєвцов, Г. В., Залкін, С. В., Сідченко, С. О., Хударковський, К. І. (2019). Особливості формування сценарію проведення інформаційно-психологічного впливу в ході реалізації стратегічних комунікацій. *Наука і техніка Повітряних Сил Збройних Сил України*, *3*, 40-46.

[2] Манойло, А. В. (2003). *Государственная информационная политика в условиях информационно-психологической войны.* Москва: Горячая линия-Телеком, 541.

[3] Расторгуев, С. П. (2002). *Философия информационной войны*. Москва: Московский психолого-социальный институт, 365.

[4] Кіслов, В. (2013). *Інформаційні війни.* Київ: Київський національний торгово-економічний університет, 300; Кіслов, Д. В. (2013). *Сучасні медіа та інформаційні війни*. Київ: МП Леся, 240.

[5] Калюжний, Р. А., Шамрай, В. О. (ред.) (2002). *Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики*. Київ: КВІЦ, 296; Калюжный, Р., Швец, Н. (2002). *Е-будущее и информационное право*. Київ: Інтеграл, 264.

[6] Жарков, Я. М., Дзюба, М. Т., Замаруєва, І. В. та інші (2008). *Інформаційна безпека особистості, суспільства, держави*. Київ: Видавничо-поліграфічний центр «Київський університет», 274.

[7] Почепцов, Г. (2015). *Сучасні інформаційні війни*. Київ: Києво-Могилянська академія, 496.

[8] Сенченко, О. (2015). Інформаційні війни як фактор трансформації соціальних систем. *Вісник Книжкової палати, 9,* 40-46.

[9] Weimann, G. (2005). Cyberterrorism: The Sum of All Fears*? Studies in Conflict & Terrorism, 28:2,* 129-149. <https://www.tandfonline.com/doi/abs/10.1080/10576100590905110> (2021, липень, 14).

[10] Хожаінова, В., Коріновська, А., Рябчук, Ю. (2021). Путін і Байден уперше зустрілися і провели переговори у Женеві. Як це було. *Суспільне|новини* <https://suspilne.media/139778-putin-pribuv-do-zenevi-dla-zustrici-z-bajdenom/> (2021, липень, 16).

[11] Прокофьев, В. (2003). *Тайное оружие информационной войны: атака на подсознание.* Москва: СИНТЕГ, 24.

шляхом використання всіх засобів та технологій інформаційно-комунікаційного, символічного та психологічного впливу на свідомість мас, на суб'єкти та об'єкти конкуруючих суспільств та організацій з метою руйнування ментальності та трансформації їх цінностей та інтересів на користь підпорядкування власним стратегічним інтересам, встановлення геополітичної та геоекономічної гегемонії, домінування, контролю та управління на глобальному чи регіональному рівнях»[1]. Більшість дослідників підтримують таке комплексне бачення інформаційної війни. Ця теорія передбачає розподіл інформаційних війн на два види: інформаційно-психологічну та інформаційно-технічну.

Під інформаційно-технічною війною ми розуміємо будь-який тип інформаційного впливу із застосуванням інформаційної зброї, метою якого є вплив на функціонування інформаційної системи шляхом незаконного доступу до інформаційної системи, здолання системи захисту, обмеження доступу законних користувачів з можливістю подальшого несанкціонованого збору, копіювання, перехоплення, блокування або видалення інформації.

Першим рівнем інформаційно-технічної війни ми вважаємо інформаційно-технічну атаку (кібератаку). Із визначень кібератаки на кшталт «кібератака − це цілеспрямовані дії, які реалізуються в кіберпросторі (або за допомогою його технічних можливостей), що призводять (можуть призвести) до досягнення несанкціонованих цілей»[2] або легального, наданого у ЗУ «Про основні засади забезпечення кібербезпеки України»[3]: «кібератака − спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та / або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та / або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» (п. 4 ст.1) складно зрозуміти чим, кібератака відрізняється від інформаційних операцій, інформаційних кампаній. Між тим, ця різниця, на наш погляд, існує – саме тому ми говоримо про **рівні** інформаційно-технічної війни. Кібератака локальна, обмежена у часі, це одноразовий інформаційний вплив на інформаційну систему. М. Ю. Яцишин зазначає: «кібератаки … за своїм характером не є значними, масштабними та систематичними, не можуть визнаватись кібервійною»[4]. Ми підтримуємо цю тезу: інформаційно-технічна атака може визнаватися першим рівнем інформаційно-технічної війни у разі, якщо таких одиничних атак було декілька, вони завдали істотної шкоди або ж окрема інформаційна атака перейшла на вищий рівень – рівень інформаційної операції і таким чином вона передувала розгортанню більш серйозних дій на інформаційному полі битви.

Інформаційно-технічна атака має певні стадії: розвідка об'єкта – розпізнавання і пошук даних про об'єкт атаки і про ресурси (інформаційну зброю), яка дозволяє її вчинити; сканування – перевірка правильності отриманої у результаті розвідки інформації, спостереження за об'єктом атаки, створення інструментів для проведення атаки; отримання доступу – контроль над атакованим об'єктом, втрата такою системою цілісності, конфіденційності наприклад, шляхом отримання повноважень системного адміністратора і знищення слідів незаконного втручання.

Сьогодні розповсюджені такі види інформаційно-технічних атак: DoS (відмова в обслуговуванні); DDoS (розподілена відмова в обслуговуванні); DRDoS (відмова в обслуговуванні із розподіленим відображенням); зустрічається також SYN-флуд атака, однак, вона визнається «морально застарілою»[5], оскільки уже існують ефективні способи її здолання;

[1] Кіслов, В. (2013). *Інформаційні війни*. Київ: Київський національний торгово-економічний університет, 57.
[2] Дубов, Д. Ожеван, М. (2011). Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. *Аналітична записка: Національний інститут стратегічних досліджень* <http://www.niss.gov.ua/articles/454/> (2021, липень, 09).
[3] *Закон про основні засади забезпечення кібербезпеки України ст.1, 2017* (Верховна рада України). *Голос України*, 208.
[4] Яцишин, М. (2018). Використання сили у кіберпросторі в рамках міжнароднго права. *Інформація і право, 4,* 22-32.
[5] Прокопчук, А., Баранов, А. (2013). Сетевая атака SYN-флуд. *Institutional Repository NTU Dnipro Polytechnic* <http://ir.nmu.org.ua/bitstream/handle/123456789/1881/SYN-FLOOD.pdf?sequence=1&isAllowed=y> (2021, липень, 14).

вилкова (подвійна) бомба. Ці атаки не приводять зловмисника до отримання доступу до інформації у системі і не викликають втрати чи крадіжки даних. Вони блокують роботу мереж і сервісів, що веде до значних витрат.

Інформаційно-технічна війна проводиться за допомогою двох основних *методів*. Першим є метод соціально-технічної інженерії, який одночасно спрямований і на технічні засоби, і на людину, якій ці технічні засоби належать (наприклад, фішинг залежить не лише від хакерських можливостей, але й від уміння змусити жертву довіряти зловмиснику). До *форм* соціально-технічної інженерії відносяться: а) фішингові листи; у загальному, фішинг − спроба виманити особисту інформацію в користувача Інтернету. Зазвичай для фішингу застосовуються електронні листи, оголошення та фіктивні сайти, за дизайном дуже подібні до тих, які часто відвідує користувач[1]. Листи приходять від підприємств, установ, організацій чи окремих осіб, яким жертва довіряє (наприклад, банк, відомі фірми на кшталт DHL, платформи електронної комерції як-от Amazon) із пропозицією перейти за вказаним у листі посиланням, відкрити доданий до листа файл або відповісти на повідомлення. У липні 2021 року було повідомлено про отримання користувачами листів із посиланням на фальшивий веб-сайт Президента України, з якого завантажувався вірус[2]. Відзначимо, що кібервоїн докладає максимум зусиль для правдоподібності: у полі «Кому» жертва може бачити тисячі інших електронних адрес, таким чином, вважаючи, що лист надіслано від організації, із якою вона працює і якій довіряє; використовуються візуальні елементи організації (шрифт, логотип etc.). Однак, дедалі частіше зусилля кібервоїнів спрямовані на те, щоб звести до мінімуму «соціальний» аспект – залежність від довіри користувача. Для досягнення цієї цілі «фішери» використовують: підроблення адресної стрічки URL; атаки за типом «фармінг», метою якого є переправлення жертви із легального веб-сайту на шахрайський прихованим способом; шпигунський фішинг – шпигунське програмне забезпечення, яке виступає у ролі кейлогера, що записує натискання клавіш на клавіатурі і передає своєму розробнику логін/пароль та іншу необхідну інформацію, коли виявляє, що користувач відвідує сайт (банку, магазину etc.), якому довіряє. На відміну від «класичного» фішингу, який може бути швидко виявлений і припинений правоохоронними органами, шпигунський може працювати місяцями, доки жертва не почне розуміти, що безпека її технічних засобів і особистих даних під загрозою. Мета фішингових атак різна: крадіжка особистої інформації, встановлення шкідливого програмного забезпечення, контроль за персональним комп'ютером і т.п.; б) спам-листи – атака, із якою стикаються мільйони людей − невідомі адресату користувачі розсилають небажані листи на різні теми. ЗУ «Про електронні комунікації»[3], який набуде чинності 1 січня 2022 року визначає спам у п. 118 ст. 2 як «електронні, текстові та / або мультимедійні повідомлення, що без попередньої згоди (замовлення) користувачів неодноразово (більше п'яти повідомлень одному абоненту) надсилаються на їхні адреси електронної пошти або кінцеве (термінальне) обладнання, крім повідомлень постачальника електронних комунікаційних послуг щодо надання ним електронних комунікаційних послуг або повідомлень від органів державної влади чи органів місцевого самоврядування з питань, що належать до їх повноважень». Позитивною новелою цього закону стало й те, що ст. 120 «Захист кінцевих користувачів від спаму» «забороняється умисне масове розсилання електронних, текстових та/або мультимедійних повідомлень без згоди (замовлення) кінцевих користувачів (спаму)».

Попри наявність легального визначення зміст поняття «спам», з урахуванням його багатогранності, легше зрозуміти, визначивши основні характеристики: 1) надсилається в електронному вигляді, однак, не обов'язково обмежується електронною скринькою, а, наприклад, може надсилатися за допомогою SMS або месенджерів; 2) особа відправника зазвичай прихована за заголовком листа або вигадана – спамери рідко використовують власні облікові записи, таким чином атаки складніше відфільтровувати і викрити невідомого відправника; 3) електронна адреса або номер мобільного телефону використовується без згоди власника; разом з тим 4) відправник не має діючої адреси або іншого контакту, на який користувач може надіслати повідомлення із вимогою

[1] Литвинова, С. Г., Букач, А. В. (2018). Обачність. Пильність. Захист. Ввічливість. Сміливість: посібник із цифрового громадянства та безпеки. *Міністерство освіти і науки України* <https://nus.org.ua/wp-content/uploads/2018/08/PRESS.pdf> (2021, липень, 18).

[2] Клуб читателей "ГОРДОН" (2021). *Маскировался под сайт президента. Госспецсвязи заблокировала фишинговый сайт* <https://gordonua.com/news/politics/maskirovalsya-pod-sayt-prezidenta-gosspecsvyazi-zablokirovala-fishingovyy-sayt-1562719.html> (2021, липень, 20).

[3] *Закон про електронні комунікації ст.2, 2020* (Верховна рада України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/1089-20> (2021, липень, 27).

припинення розсилання спаму; 5) може містити незаконні (шахрайство, порнографія) елементи або бути спрямованим на встановлення шкідливого програмного забезпечення; 6) розсилається масово, інколи декілька разів (повторно). Метою спам-повідомлення може бути завантаження вкладення користувачем-адресатом чи перехід за посиланням, яке містить шкідливе програмне забезпечення; агресивний маркетинг; шахрайство; продаж особистої інформації.

Характеризуючи соціально-технічну інженерію як метод інформаційно-технічної війни слід відзначити, що професіоналізм кібервоїнів повсякчас зростає, більше того, часто мова йде і про повноцінні злочини, вчинені у кіберпросторі, які складають цілі кримінальні ланцюги – кіберзлочинці об'єднані глобальними мережами діють на міжнародному рівні, їх робота чітка і високоорганізована. Дії кібервоїнів часто бувають структуровані – фішинг і спам «воюють» разом як піхота й артилерія: роль спамера полягає у зборі електронних адрес для створення списку потенційних жертв і розсилання їм спам-листів із закликом відвідати ту чи іншу компанію / організацію / магазин etc.; фішер займається пошуком «вразливих» серверів.

Другий метод − встановлення шкідливого програмного забезпечення. Метою встановлення шкідливого програмного забезпечення може бути: відслідковування і пересилання даних облікового запису (імена користувачів, паролі); зміна, шифрування чи знищення даних; інтеграція у мережу ботів і їх незаконне використання для DDoS-атак; несанкціоноване віддалене керування IT-системою.

Попри те, що функціональні можливості шкідливого програмного забезпечення відрізняються, воно в усіх випадках використовує інформаційно-технічну систему для цілей, на які законний користувач не давав згоди. До видів шкідливого програмного забезпечення, відноситься: 1. Шпигунське програмне забезпечення – повністю невидимі комп'ютерні програми, які встановлюються з метою передачі інформації про користувача третім особам без його згоди. Зазвичай воно використовується для «агресивного» Інтернет-маркетингу – аби дізнатися про звички споживача, його переваги з метою оптимізації цільової реклами, рідше – з метою заволодіння особистими даними для їх незаконного використання. Наявність у IT-системі шпигунського програмного забезпечення знижує продуктивність і якість роботи комп'ютера. Прикладом такого програмного забезпечення є «CoolWebSearch». 2. Програми-вимагачі блокують системи і вимагають викуп за розблокування. Існують різні види програм-вимагачів: а) програма-шантажист – вона не блокує сам жорсткий диск, а блокує доступ до нього; б) програми-вимагачі, які блокують дані, цей вид має великий потенціал нанесення збитків зацікавленим особам, оскільки це шифрування складно здолати, крім того, сплата грошової суми, яка вимагається часто не призводить до розблокування зараженої системи; в) програми-очисники найбільш небезпечні з усіх «вимагачів», адже, у них відсутня функція розблокування і відновлення даних, апріорі, недоступне у системі навіть після сплати грошової суми; дані стають неприданими для використання і знищуються остаточно. Одним із найбільш шкідливих серед програм-вимагачів є програма-вимагач «GandCrab». 3. Програми для крадіжки інформації, такими, наприклад, є AZORult – програма для крадіжки інформації, яка використовує різні цифрові ідентифікатори; njRAT – інструмент віддаленого доступу, який записує натискання клавіш (кейлогінг) і надає третім особам доступ до мікрофону і камери. 4. Шкідливе програмне забезпечення, яке використовується для цілеспрямованих атак на критично важливу інфраструктуру, органи влади і компанії-гіганти, наприклад, Emotet. 5. Рекламне – призначене для того, аби на екрані користувача з'являлося якомога більше реклами. Лише на перший погляд може здатися, що ця реклама потрібна суто для того, аби привернути увагу (а частіше − подратувати користувача) – часто перехід за рекламним посиланням може привести до веб-сайту, що містить шкідливе програмне забезпечення.

Зусилля кібервоїна спрямовані на системне вторгнення, яке може призвести до знищення інформації, незаконного отримання інформації, несанкціонованої зміни даних можуть супроводжуватися фінансовою вигодою.

Теорія кібертероризму виникла на основі теорії тероризму, загальними рисами тероризму і кібертероризму є використання насильства для досягнення поставлених цілей: політичних, релігійних, економічних чи ідеологічних, бажання суспільного резонансу, залучення ЗМІ із метою залякати, викликати тривогу, невпевненість.

«Кіберпростір» не знайшов остаточного концептуального утвердження у наукових працях, але у п. 11 ст. 1 ЗУ «Про основні засади забезпечення кібербезпеки України»[1] міститься його легальне

[1] *Закон про основні засади забезпечення кібербезпеки України ст.1, 2017* (Верховна Рада України). *Голос України,* 208.

визначення: кіберпростір визначається як «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та / або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та / або інших глобальних мереж передачі даних». Поява кіберпростору призвела до того, що у 1980 р. у США було запроваджено термін «кібертероризм». Пізніше, у західній доктрині почали розвиватися теорії, які виокремлювали специфічні ознаки кібертероризму: «це явище відноситься до незаконних атак і погроз таких атак на комп'ютери, мережі, інформацію, що у ньому зберігається з метою залякування, примушування уряду чи населення для досягнення політичних чи соціальних цілей. Окрім цього, аби бути тероризмом, атака повинна приводити до насильства проти людей, власності чи, принаймні завдавати істотної шкоди, викликати страх... серйозні атаки на критично важливу інфраструктуру можуть бути актом кібертероризму залежно від їх впливу»[1]. Проблема розуміння «кібертероризму» пов'язана, у тому числі, із суперечками про те, чи є це явище «самодостатнім», чи це просто частина інформаційної війни, а спеціальні дослідження нараховують 28 різних визначень[2]. Однак, на наш погляд, складність розуміння кібертероризму як окремого явища полягає не лише у тому, що межі між цим та поняттями інформаційних війн, комп'ютерних злочинів часто стерті, а й у тому – наскільки явище кібертероризму взагалі реальне?

З урахуванням неоднозначних, але все ж розроблених концепцій кібертероризм й інформаційні, зокрема інформаційно-технічні війни не можуть визнаватися тотожними поняттями, хоча у них є певні спільні риси. Вказуючи на спільні ознаки двох складних у теоретизації явищ – інформаційно-технічної війни і кібертероризму, по-перше, слід зазначити, що вони відносяться до *загроз у кіберпросторі*. Сфера і ділового, і особистого життя у цифрову епоху перемістилася в Інтернет, а інформаційні війни і кібертероризм ставлять під загрозу його надійність – ці загрози знижують рівень довіри до Інтернету, збільшують потребу у витратах на забезпечення безпеки користування Всесвітньою мережею і технічних засобів, які забезпечують доступ до неї. До інших спільних ознак можна віднести: анонімність; низький рівень виявлення; невеликі ресурсні вкладення (людські, матеріальні і т.д.); можливість досягнення цілей із будь-якого місця, де є Інтернет-покриття; використанні інформаційних технологій; завжди умисні дії − й інформаційна війна, і кібертероризм є спланованими, оскільки, як мінімум, вимагається розробка програмного забезпечення для проведення атаки; спільний збройний арсенал.

Однак, інформаційно-технічна війна і кібертероризм мають відмінні ознаки, які можна розділити за низкою критеріїв: 1. Різний характер: 1) кількість та інтенсивність кібератак швидко зростає, однак, вона 2) може пройти не поміченою потерпілою стороною, а відтак потерпіла сторона 3) не повідомляє про вчинену кібератаку, особливо, якщо вона не завдала фінансових збитків, (у разі вчинення атаки стосовно певної компанії таке неповідомлення пов'язане ще й зі страхом втрати репутації), разом з тим цей вид інформаційних війн залишається великою загрозою для підприємств. На противагу цьому, кібертерорист має політичну, релігійну чи ідеологічну мотивацію, він використовує знання комп'ютерних систем для привернення уваги.

2. Різні суб'єкти: кібервоїн (хакер) прагне задовольнити своє его: отримати визнання в очах своїх колег, задовольнити цікавість; для нього участь в інформаційно-технічній війні може виступати і як перевірка власного інтелекту, і як виклик державам або окремим організаціям, установам, підприємствам або окремим особам шляхом крадіжки інформації, потенційно із метою її подальшого продажу третім особам; або ж, навпаки, виконати конкретне замовлення окремих компаній, переслідуючи мету грошового прибутку, чи навіть іноземних держав, для досягнення ними конкурентної переваги (наприклад, економічної) тощо; метою кібертерориста є шантаж, експлуатація, помста, знищення, він завжди політично, релігійно чи ідеологічно умотивований. За портретом кібервоїн – розумний підліток або особа молодого віку, яка годинами проводить перед монітором, шукаючи нові можливості для кібератак або повноцінних інформаційних війн. Кібертерористів же можна розділити на три види: представники традиційних терористичних груп; «хакери», які виконують замовлення кібертерористів; терористичні держави які стали і «кібертерористичними

[1] Denning, D. E. (2001). Is Cyber Terror Next. *Social Science Research Council* <http://essays.ssrc.org/sept11/essays/denning.htm> (2021, липень, 16).

[2] Дубов, Д. (2014). Кіберпростір як новий вимір геополітичного суперництва. *Національний інститут стратегічних досліджень* <http://old2.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf > (2021, липень, 27).

державами». Можна сказати, що кібертероризм – явище більш жорстоке. Хоча кібервоїни раз за разом демонструють зламування комп'ютерних мереж, викликаючи функціональний параліч системи і фінансові втрати, ця схильність до нанесення істотної шкоди не є доказом того, що вони готові наражати на небезпеку, переслідуючи політичні, релігійні чи ідеологічні мотиви.

3. Різні об'єкти: для кібертероризму важливими є не лише певна інформаційна інфраструктура, але й таке втручання, що дозволить викликати невизначеність у суспільстві, страх, паніку. Для справжнього кібертерориста – інформаційна система – це лише посередник, а не безпосередній об'єкт як у випадку інформаційно-технічної війни. Помилковим вважаємо і зведення кібертероризму до фізичного знищення інформаційного обладнання, програмного забезпечення чи інших носіїв інформації.

4. Різні цілі: метою інформаційно-технічної війни є нанесення шкоди інформаційно-технічній системі, метою кібертероризму – нанесення шкоди суспільству.

Нами уже зазначалося, що кібертероризм – це розвиток **терористичних можливостей**, які забезпечуються новими технологіями, реалізуються у кіберпросторі, це своєрідна «терористична декаль» у віртуальне середовище. Сама концепція тероризму є дуже складною: «ще у 80-х роках XIX ст. А. Шмідт склав список із 109 визначень тероризму з метою узагальнити цей матеріал і вивести загальноприйняте визначення тероризму. Зусилля вченого виявилися марними, тому що після нього ще багато дослідників намагалися зробити те саме, але безуспішно, нові визначення призводили до ще більшої плутанини… Тероризм – це соціальне явище, яке виникає і загострюється на ґрунті соціальної, правової, політичної та економічної нестабільності в державі з метою досягнення певних змін (виконання поставлених вимог) на користь злочинців, шляхом застосування чи погрози застосування насильства, яке проявляється у застосуванні зброї, вчиненні вибухів, підпалів, та інших загально небезпечних дій певною особою чи організованою групою осіб»[1]. Із цього визначення можна констатувати, що тероризм – це 1) акт насильства; 2) має психологічний ефект; 3) призводить до результату у фізичному вимірі, адже, у кіберпросторі неможливі «фізичні результати», це пов'язано із власне природою кіберпростору. Сьогодні не складно говорити про інформаційно-технічну атаку, яка наносить істотну шкоду і впливає на критично важливу інфраструктуру, однак, як і на початку 2000-х можна висувати **лише теорію** кібертероризму, оскільки, досі немає реального прикладу терористичних дій у кіберопросторі, який би підтвердив гіпотезу його існування: атака на сайт Військово-Морських сил України[2], кібертака на майже триста компаній США, вартість шкоди якої оцінили приблизно у 70 млн. доларів[3] і навіть події весни 2017 року, коли Європа опинилася «у полоні» вірусу Petya-A і вірусом в Україні було заражено комп'ютерні системи «Укренерго», «Київенерго», «Епіцентр», «Київстар», Vodafone, Lifecell, канал ATR, аеропорт «Бориспіль», мережа автозаправних станцій WOG, «Укргазвидобування» − це прояви інформаційно-технічної війни, хоч із великими збитками. Інформаційно-технічна війна – поки що **єдиний вид** конфлікту у кіберпросторі.

Терористи використовують різні методи й інформаційно-психологічної війни. Складно не підтримати тезу К. Хармон, висловлену у книзі «Тероризм сьогодні»: «Пропаганда – справжній стандарт терористичної групи»[4]. Зараз, замість листівок і газет, терористи використовують Інтернет. Більшість терористів «переселилися» у так званий DarkNet, надійне шифрування якого дозволяє розповсюджувати терористичну пропаганду, вербувати, наймати нових учасників, однак, і цю діяльність не можна визнати «кібертероризмом», так само, як не можна вважати «кібернаркоманією» факт купівлі, або продажу наркотиків у тому ж DarkNet.

Нечіткі межі між інформаційними війнами і кібертероризмом часто призводять до використання надто емоційних термінів у ЗМІ, так, анотація журналістської статті із заголовком: «Найгучніші хакерські атаки, які сколихнули всю Україну: вражаючі деталі» обіцяє нам дізнатися цікаву інформацію про **«електронний шпіонаж, шахрайство, шантаж та навіть кібертероризм…»**. У тексті справді йшла мова про відключення електроенергії через встановлення вірусу BlackEnergy, масові атаки із Росії і уже загаданий нами вірус Petya A, однак, самі журналісти пишуть про те,

[1] Біленчук, П. Д., Кофанов, А. В., Кобилянський, О. Л. (2009). *Міжнародний тероризм: консолідований аналіз забезпечення безпеки*. Київ: ННІПСК КНУВС, 13-14.

[2] Украинская правда (2021). *Сайт ВМС Украины «лег» из-за хакерской атаки с РФ, портал Минобороны выстоял* <https://www.pravda.com.ua/rus/news/2021/07/9/7300072/> (2021, липень, 19).

[3] МинфинМедиа (2021). *Масштабная хакерская атака 4 июля может стоить сотням компаний в мире $70 миллионов* <https://minfin.com.ua/2021/07/05/67459817/> (2021, липень, 09).

[4] Harmon, C. (2000). *Terrorism Today.* London: Frank Cass Publishers, 55.

що «фахівці назвали це втручання в роботу комп'ютерних мереж чи не найбільшою **кібератакою** за останні роки»[1]. Жоден із названих прикладів не є кібертероризмом, між тим, вішати на кібертероризм ярлик аморфної, повністю безпредметної категорії теж ми вважаємо помилковим. Це явище було, і залишається цілком реальною загрозою, яка, на щастя, досі не реалізувалася, однак, відсутність її реального втілення, не повинна відкидати теоретичне існування.

Справедливим буде відмітити те, що і спеціальні дослідження грішать різного роду пейоративами як от «цей різновид злочинної терористичної діяльності поширився і почав загрожувати загальносвітовому розвитку людства», «спрямований на підрив атмосфери спокою», разом з тим, науковці переважно або уникають наведення конкретних прикладів «загрози загальносвітовому розвитку людства», або викладають концепції інформаційних війн (у тому числі, інформаційно-психологічної, пишучи про вербування і т.д.), або взагалі переходять до описування «вибухів у метро», відходячи від дефініції «кібертероризм – тероризм, що вчинюється у кіберпросторі», яку використовує і вітчизняне законодавство: терористична діяльність, що здійснюється у кіберпросторі або з його використанням (ст. 1 ЗУ «Про основні засади забезпечення кібербезпеки України») хоча вона, на наш погляд, не несе смислового навантаження і навіть, якщо людство зіткнеться із реальним кібертероризмом у майбутньому, робочим політико-правовим механізмом цей конструкт можна назвати із великою долею скептицизму, оскільки наведене поняття містить у собі замкнене коло: «кібертероризм – терористична діяльність», це ще одна громіздка конструкція, що навряд чи знайде своє практичне втілення.

Отже, проведене дослідження дозволяє зробити такі висновки. По-перше, відсутність чітких меж між поняттями «інформаційних війн» та «кібертероризму» створює серйозні перешкоди на шляху остаточної теоретизації. Наука цифрової епохи тільки стоїть на порозі належного осмислення і відходу від фрагментарності розуміння ключових понять інформаційного протиборства. По-друге, з метою більш чіткого розуміння концепції інформаційно-технічної війни, нами було констатовано можливість її стадійного виміру – першою стадією (рівнем) інформаційно-технічної війни ми вважаємо кібератаку, яка буває різних видів. По-третє, під час ведення інформаційно-технічної війни використовується два основних методи – метод соціально-технічної інженерії та метод встановлення шкідливого програмного забезпечення. По-четверте, кібертероризм, на наш погляд, частина політичної міфології, концепції якої розвинені у науці, однак, не знайшли свого відображення у реальності (автори щиро сподіваються, що реалізація тривожних наукових пророцтв так і не відбудеться), а єдиним кіберпросторовим конфліктом є інформаційно-технічна війна.

References:

1. Weimann, G. (2005). Cyberterrorism: The Sum of All Fears? *Studies in Conflict & Terrorism, 28:2,* 129-149 <https://www.tandfonline.com/doi/abs/10.1080/10576100590905110> (2021, July, 14). [in English].
2. Denning, D. E. (2001). Is Cyber Terror Next. *Social Science Research Council* <http://essays.ssrc.org/sept11/essays/denning.htm> (2021, July, 16). [in English].
3. Harmon, C. (2000). *Terrorism Today.* London: Frank Cass Publishers. [in English].
4. Khozhainova, V., Korinovska, A., Riabchuk, Yu. (2021). Putin i Baiden upershe zustrilysia i provely perehovory u Zhenevi. Yak tse bulo. [Putin and Biden met for the first time and held talks in Geneva. As it was]. *Suspilne novyny* [Public news] <https://suspilne.media/139778-putin-pribuv-do-zenevi-dla-zustrici-z-bajdenom/> (2021, July, 16). [in Ukrainian].
5. Prokofev, V. (2003). *Tainoe oruzhye ynformatsyonnoi voiny: ataka na podsoznanye* [The secret weapon of information warfare: an attack on the subconscious]. Moscow: SYNTEH. [in Russian].
6. Kislov, V. (2013). *Informatsiini viiny* [Information wars]. Kyiv: Kyiv National University of Trade and Economics. [in Ukrainian].
7. Dubov, D. Ozhevan, M. (2011). Problemy chynnoyi vitchyznyanoyi normatyvno-pravovoyi bazy u sferi borotby iz kiberzlochynnistyu: osnovni napryamy reformuvannya [Problems of the current domestic legal framework in the fight against cybercrime: the main directions of reform]. *Analitychna zapyska: Natsionalnyy instytut stratehichnykh doslidzhen* [Analytical note: National Institute for Strategic Studies] <http://www.niss.gov.ua/articles/454/> (2021, July, 09). [in Ukrainian].
8. Iatsyshyn, M. (2018). Vykorystannia syly u kiberprostori v ramkakh mizhnarodnho prava [Use of force in cyberspace under international law]. *Informatsiia i pravo* [Information and law], *4*, 22-32. [in Ukrainian].

[1] 24 канал (2018). *Найгучніші хакерські атаки, які сколихнули всю Україну: вражаючі деталі* <https://24tv.ua/nayguchnishi_hakerski_ataki_yaki_skolihnuli_vsyu_ukrayinu_vrazhayuchi_detali_n1079849> (2021, липень, 19).

9. Prokopchuk, A., Baranov, A. (2018). Setevaia ataka SYN-flud [Network attack SYN-flood]. *Institutional Repository NTU Dnipro Polytechnic* <http://ir.nmu.org.ua/bitstream/handle/123456789/1881/SYN-FLOOD.pdf?sequence=1&isAllowed=y> (2021, July, 14). [in Russian].
10. Lytvynova, S. H., Bukach, A. V. (2018). Obachnist. Pylnist. Zakhyst. Vvichlyvist. Smilyvist: posibnyk iz tsyfrovoho hromadyanstva ta bezpeky [Caution. Vigilance. Protection. Politeness. Courage: a Guide to Digital Citizenship and Security]. *Ministerstvo osvity i nauky Ukrayiny* [Ministry of Education and Science of Ukraine] <https://nus.org.ua/wp-content/uploads/2018/08/PRESS.pdf.> (2021, July, 18). [in Ukrainian].
11. Klub chitateley GORDON [GORDON Readers Club] (2021). *Maskyrovalsia pod sait prezydenta. Hosspetssviazy zablokyrovala fyshynhovyi sait* [Disguised as the president's website. Gospestsvyazi blocked the phishing site] <https://gordonua.com/news/politics/maskirovalsya-pod-sayt-prezidenta-gosspecsvyazi-zablokirovala-fishingovyy-sayt-1562719.html> (2021, July, 20). [in Russian].
12. Dubov, D. (2014). *Kiberprostir yak novyi vymir heopolitychnoho supernytstva* [Cyberspace as a new dimension of geopolitical rivalry] <http://old2.niss.gov.ua/content/articles/files/Dubov_mon-89e8e.pdf > (2021, July, 27). [in Ukrainian].
13. Bilenchuk, P. D., Kofanov, A. V., Kobylianskyi, O. L. (2009). *Mizhnarodnyi teroryzm: konsolidovanyi analiz zabezpechennia bezpeky* [International terrorism: a consolidated analysis of security]. Kyiv: NNIPSK KNUVS. [in Ukrainian].
14. Ukrainskaya pravda [Ukrainian Truth] (2021). *Sait VMS Ukrayny «leh» yz-za khakerskoi ataky s RF, portal Mynoborony vystoial* [The site of the Ukrainian Navy «lay down» due to a hacker attack with the Russian Federation, the portal of the Ministry of Defense survived] <https://www.pravda.com.ua/rus/news/2021/07/9/7300072/> (2021, July, 19). [in Russian].
15. MinfinMedia (2021). *Masshtabnaia khakerskaia ataka 4 yiulia mozhet stoyt sotniam kompanyi v myre $70 myllyonov* [A large-scale hacker attack on July 4 could cost hundreds of companies around the world $ 70 million] <https://minfin.com.ua/2021/07/05/67459817/> (2021, July, 09). [in Russian].
16. 24tv (2018). *Naihuchnishi khakerski ataky, yaki skolykhnuly vsiu Ukrainu: vrazhaiuchi detali* [The loudest hacker attacks that shook the whole of Ukraine: impressive details]. <https://24tv.ua/nayguchnishi_hakerski_ataki_yaki_skolihnuli_vsyu_ukrayinu_vrazhayuchi_detali_n1079849> (2021, July, 19). [in Ukrainian].
17. *Zakon pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy, 2017* (Verkhovna Rada Ukrainy) [Law on Basic Principles of Cyber Security of Ukraine (Verkhovna Rada of Ukraine)]. *Holos Ukrainy* [Voice of Ukraine], 208. [in Ukrainian].
18. *Zakon pro elektronni komunikatsii, 2020* (Verkhovna Rada Ukrainy) [Law on Electronic Communications (Verkhovna Rada of Ukraine)] Ofitsiinyi sait Verkhovnoi Rady Ukrainy [Official site of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/1089-20> (2021, July, 27). [in Ukrainian].