УДК 323.23:316.776.23 DOI: 10.17721/2415–88IX.2022.88.202-218

Сунгурова Саломе Романівна
Військовий інститут Київського національного університету імені Тараса Шевченка (м. Київ, Україна)
https://orcid. org/0000–0003-0715–3416
e-mail: sungarova_s@ukr. net

МІЖНАРОДНИЙ ДОСВІД БОРОТЬБИ З ПОЛІТИЧНИМ НАСИЛЛЯМ ЗАСОБАМИ ІНФОРМАЦІЙНОЇ ВІЙНИ

Резюме

Метою роботи є 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.

Досліджено міжнародний досвід протистояння політичному насиллю в інформаційному просторі, який підтверджує наявність спільного ворога демократичного світу в інформаційній боротьбі — РФ. Продемонстровано, що російський підхід до інформаційної війни — це глобальна стратегія, яка включає як кібер-удари, так і інформаційні операції проти більшості демократичних акторів світу (Польща, Болгарія, Словаччина, Грузія, Молдова, США, Франція, Швеція та ін.). Російські кампанії інформаційної війни впливали і продовжують дискредитацію демократичних інституцій, пропагуючи екстремізм і невдоволення, підтримуючи антидемократичних лідерів, намагаючись похитнути вплив Заходу. З'ясовано, що російські інформаційні стратегії збігаються в багатьох країнах і можуть служити різним цілям. Однак, виявлено що є серед них 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. Акцентується, що російська медіа-машина використовує широкий набір інструментів дезінформації,

«фабрики тролів», що призводить до плутанини та ставить під сумнів саме поняття істини.

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

Вступ

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 [1]. 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. Російські лідери розуміли цінність інформації та те, як її можна використати для впливу на маси як вдома, так і за кордоном [2]. Згодом Російська Федерація почала використовувати Інтернет для підвищення ефективності інформаційної війни у недорогий спосіб. У цьому контексті Російська Федерація працює над покращенням своїх можливостей, щоб домінувати в кіберпросторі за кордоном.

Методи дослідження

Методологічним фундаментом дисертаційної роботи став комплекс загальнонаукових та спеціальних методів. 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.

Результати дослідження

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 [4]. 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 [5]. 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 іммігрaції створюють сприятливий грунт для маніпуляцій. Зокрема на ці побоювання були спрямовані російські інформаційні кампанії, щоб вплинути на результати виборів [6]. 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 [7]. 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 [7]. 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 [8]. 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 [8]. 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 медіамашини. 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 [8]. «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 контексті 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. 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 [9]. 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 [10]. 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 [11].

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 [12].

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 [13].

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 розвідані 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. 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 [14]. 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 [15].

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.

Висновки

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 посилань:

1. Золотухін Д. Протидія інформаційній агресії Росії на рівні законодавчих актів: Резолюція Європарламенту. URL: http://bit. ly/2mVqxzW

2. Ожеван М. А. Глобальна війна стратегічних наративів: виклики та ризики для України. Стратегічні пріоритети. URL: http://nbuv. gov. ua/UJRN/sppol_2016_4_6

3. 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/.

4. 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.

5. 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.

6. Російське іномовлення як інструмент маніпулювання громадською думкою у трансатлантичному просторі. НІСД. URL: http://www. niss. gov. ua/articles/1834/

7. 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.

8. 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.

9. 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.

10. Зеленін В. В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандиської війни. Вінниця: Віндрук, 2014. 384 с.

11. Как работает фабрика «кремлевских тролей?» [Електронний ресурс] / Gordon. com [сайт]. — Режим доступу: http://gordonua. com/news/worldnews/Kakrabotaet-fabrika-kremlevskih-trolley-71305.html

12. 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

13. Козлітін В. Д. Основні напрями світових глобалізаційних процесів кінця XX — початку XXI ст., дискусії між глобалістами та антиглобалістами про їх наслідки. Збірник наукових праць. Серія «Історія та географія». 2004. Вип. 17. С. 26–30.

14. 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.

15. 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.

References:

1. Zolotukhin, D. Countermeasures against Russia's informational aggression at the level of legislative acts: Resolution of the European Parliament. URL: http://bit. ly/2mVqxzW

2. Ozhevan, M.A. Global war of strategic narratives: the challenges and risks for Ukraine. Strategic priorities. URL: http://nbuv. gov. ua/UJRN/sppol_2016_4_6

3. 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/.

4. 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.

5. 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

6. Russian foreign language as a tool for manipulating public opinion in the transatlantic space. National Institute of Strategic Studies. http://www. niss. gov. ua/articles/1834/

7. 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.

8. 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.

9. During the war in Ukraine, 20 journalists died: their names were published. https://www. slovoidilo. ua/2022/04/12/novyna/suspilstvo/vijny-ukrayini-zahynulo-20-zhurnalistiv-opublikovano-yixni-imena

10. Zelenin, V.V. (2014). On the other side of the truth: neuro-linguistic programming as a weapon of propaganda warfare. Vinnytsia: Windruk, 384.

11. How does the Trolks from Olgino work? http://gordonua. com/news/worldnews/Kakrabotaet-fabrika-kremlevskih-trolley-71305.html

12. Danylenko, S.I. Regulation and self-regulation of the Internet in the world: stable trends in the establishment of the civil right to communication. Actual problems of international relations. URL: http://nbuv. gov. ua/UJRN/apmv_2011_103%281%29__8

13.. Kozlitin, V.D. (2004). The main directions of world globalization processes of the late 20th and early 21st centuries, discussions between globalists and anti-globalists about their consequences. Series «History and Geography», Issue 17, 26–30.

14. Zinchenko, M.O, Plugova, O.B & Draglyuk O.V. (2017). Information warfare, means of implementation and countermeasures. The informational dimension of hybrid warfare, the experience of Ukraine: materials of the international scientific and practical conference. Kyiv: NDUU, 38–40.

15. Kapshtyk, O.V. (2019). State mechanisms of strategic communications in the security and defense sector of Ukraine: dissertation. PhD of Sciences of State management: 25.00.05. Khmelnytskyi University of Management and Law. Khmelnytskyi, 197 p.

UDC 323.23:316.776.23 DOI: 10.17721/2415–88IX.2022.88.202-218

Salome Sunhurova
Military Institute of the Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)
https://orcid. org/0000–0003-0715–3416
e-mail: sungarova_s@ukr. net

INTERNATIONAL EXPERIENCE OF STRUGGLING WITH THE POLITICAL VIOLENCE BY MEANS OF INFORMATION WARFARE

Abstract

The goal of the work is to study 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 in order to preserve Western democratic values, institutions and systems.

The article examines the international experience of resisting political violence in the information space, which confirms the existence of a common enemy of the democratic world, the Russian Federation, in the information struggle. It has been demonstrated that the Russian approach to information warfare is a global strategy that includes both cyber attacks and information operations against the majority of democratic actors in the world (Poland, Bulgaria, Slovakia, Georgia, Moldova, USA, France, Sweden, etc.). Russian information warfare campaigns have influenced and continue to discredit democratic institutions. They promote extremism and discontent, supporting anti-democratic leaders in an attempt to shake the influence of the West.

It was found that Russian information strategies coincide in many countries and can serve different goals. However, it was found that there are three common goals among them. There are restoration of Russian dominance in the post-Soviet/imperial sphere of influence, reducing the influence of Western democratic values, institutions and systems in order to create a polycentric world model and the expansion of Russia's political, economic and military hegemony throughout the world. Attention is focused on the fact that the Russian media

machine uses a wide range of misinformation tools, « Trolls from Olgino», which leads to confusion and calls into question the very concept of truth.

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

Стаття надійшла до редакції 18.03.22

© Сунгурова С. Р., 2022