ПОЛІТИЧНІ ПРОБЛЕМИ МІЖНАРОДНИХ СИСТЕМ ТА ГЛОБАЛЬНОГО РОЗВИТКУ

DOI 10.31558/2519-2949.2018.2.17
УДК 32:316.444(477)

Андрієвський Т. Г., Харківський національний педагогічний університет імені Г. С. Сковороди

ЦІЛІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ГІБРИДНОЇ ВІЙНИ

У статті отримала розвиток концепція, що російсько-українська гібридна війна має істотний вплив на світовий порядок та міжнародні відносини. Описуються нові цифрові підривні технології, які Російська Федерація використовує під час конфлікту. Серед іншого, робиться акцент на фейкових новинах, пропаганді, втручанні у виборчі процеси, кібератаках, які є по-суті новим видом зброї в війні нового покоління – гібридної війни чи війни інформаційного суспільства.

У статті описуються окремі особливості підривної діяльності Російської Федерації. Серед іншого, наводяться приклади проведення вищезгаданої підривної діяльності, починаючи з кібератаки на урядові сайти Естонії в 2007 році і закінчуючи сучасними проблемами, з якими зіштовхнувся Захід. Зокрема, розкривається роль соціальних мереж в контексті їх впливу на політичні процеси в демократичних державах. Окремо наголошується на можливому втручанні Російської Федерації у хід президентських виборів в США, зокрема, в контексті проведення інформаційних операцій у соціальних мережах Twitter та Facebook. Наводяться результати моніторингу активності фейкових облікових записів, проведеного службою безпеки Facebook.

У статті знаходять свій виклад певні цілі російської агресії та її підривні заходи. Визначено, що головною метою російсько-української гібридної війни на цьому етапі є створення хаосу, підрив цінностей демократичного світу та виховання всебічної атмосфери недовіри та нігілізму. Крім того, стверджується, що агресор використовує самі інститути демократії та їх слабкі сторони як зброю. Пропонується класифікація інформаційних операцій за їх метою в контексті гібридної війни.

Ключові слова: *війна, гібридна війна, Російсько-українська гібридна війна, фейкові новини, пропаганда, підривні технології, інформаційні операції, Twitter, Facebook.*

Постановка проблеми. Російсько-українська гібридна війна триває вже майже чотири роки. Здобутками агресора в цій війні стала анексія Автономної Республіки Крим та утворення в окремих районах Донецької та Луганської областей маріонеткових урядів, що ефективно контролюються російською адміністрацією. Загалом, за попередніми висновками прокурора Міжнародного кримінального суду – цей конфлікт має усі ознаки міжнародного [15, с. 35, абз. 158]. Тобто стає все менше підстав вважати цей конфлікт внутрішньо українським. Це – агресія, міжнародний злочин, що карається світовою спільнотою.

Проте, виникає питання, чи були ці втрати території для України (у пропорційному відношенні до всієї території держави за словами Президента України П. Порошенко втрати складають 7%) ціллю російської агресії? Безумовно, ні. Основна мета російської агресії, на нашу думку – це недопущення виходу України з-під сфери впливу Росії, боротьба проти права України на власний суверенітет та на самостійне вирішення власної політичної долі. Російські геополітичні амбіції, що і є її метою для протистояння, дуже добре пояснюються словами президента Путіна – адже саме він назвав розпад СРСР «найбільшою геополітичною катастрофою XX століття».

Сучасна російсько-українська гібридна війна не має аналогів у світовій історії. Дійсно, окремі елементи вже застосовувалися і раніше, проте комбінація всіх методів, особливо невійськового характеру, кожного дня доповнюють або змінюють концепцію гібридної війни. Основні фронти переносяться з полів боїв у зовсім іншу сферу: економіку, внутрішню і зовнішню політику,

міжнародні відносини. Звісно, історія доводить, що раніше вже саме так і відбувалося, коли війна ставала глобальною для усіх сфер життєдіяльності держави, проте унікальним явищем сьогодення є саме методи і механізми того, як звичайні громадяни (тобто некомбатанти) стають жертвами агресора або ж його зброєю.

Аналіз актуальних досліджень. Проблематика феномену гібридної війни досліджувалася як зарубіжними теоретиками (М. Бонд, В. Герасимов, Ф. Гоффман, Р. Гейтс, Р. Гленн, К. Касапоглу, М. Кофман, Дж. Мак К'юен, М. Роянськи та ін.), так і вітчизняними дослідниками (В. Горбулін, Є. Магда, І. Рущенко, та ін.).

Метою статті є визначення цілей, які переслідує агресор, та методів, якими він планує досягати переваги. Висновки, отримані в ході нашого аналізу повинні допомогти в майбутньому сформувати концепцію ефективної протидії агресії в інформаційному суспільстві а також підготуватися до нових викликів, адже методи, виявлені нами, можуть і будуть застосовуватися не тільки Росією, а й терористичними організаціями, радикальними ісламістами, тощо.

Виклад основного матеріалу. У російсько-українській гібридній війні Україні, на жаль, відведена роль гарячої точки, основному воєнному фронту та полігону для випробування нових засобів і способів ведення війни нового покоління. Використовуючи концепт «російсько-українська гібридна війна» ми опираємося на праці науковців у сфері національної безпеки з Національного інституту стратегічних досліджень України, які одними з перших увели це поняття в науковий обіг [16, с. 17]. Проте сам конфлікт все більше набуває рис глобального протистояння двох кардинально різних за своїми ціннісними орієнтирами світів. Санкції, що накладені на Російську Федерацію світовою демократичною спільнотою за анексію Автономної республіки Крим та вторгнення на Донбас, є звичайним елементом стримування агресора цивілізованим суспільством. Проте для Росії (у розумінні її керівників), всі сторони західного світу, які підтримують санкційний режим проти неї, стають автоматично учасниками конфлікту. Захід повинен зрозуміти, що Росія (за її переконанням) вже давно не веде війну з Україною. Росія воює з усім світом, де не приймають її «цінності».

Санкції самі по собі є деструктивним чинником уповільненої дії з катастрофічними наслідками для російської економіки, а тому для Кремля постає питання виживання держави та збереження діючої моделі управління разом зі своєю політичною верхівкою.

Уникнення деструктивних наслідків санкцій для Росії можливе двома шляхами. Цивілізований шлях передбачає виведення своїх військ з окупованих територій, проведення розслідувань відповідних злочинів, компенсації Україні завданих збитків. Проте аналіз останніх подій підтверджує, що був обраний власне другий, радянський шлях Холодної війни для вирішення проблеми, що полягає в розхитуванні демократичних систем на Заході, послабленні своїх супротивників зсередини, створенні так званого «керованого хаосу» для досягнення повної дестабілізації політичних процесів. За таких умов Росія сподівається розпочати торг за скасування санкцій і попутно зберегти свої «надбання».

Гібридна війна – це війна інформаційного суспільства, нове покоління воєн, коли територію не потрібно захоплювати фізично, а потрібно отримати контроль над свідомістю, думками і прийняттям рішень людьми. [14, с. 165]. Пропаганда, інформаційні та кібернетичні атаки, створення альтернативної реальності в інформаційному середовищі – це саме ті асиметричні дії Росії, які покликані змінити саме світосприйняття людей в демократичних державах.

Якщо Україна вимушена «фізично» стримувати агресію Росії, застосовуючи свої Збройні Сили, то Захід все більше вимушений зустрічати новий тип втручання – інформаційні операції. Так, під інформаційними операціями ми розуміємо втручання державних або недержавних акторів у внутрішню політику держави з метою поширення вигідних інформаційних наративів для агресора шляхом використання пропаганди, дезінформації або інформаційного хаосу. На жаль, саме «діджиталізація» сучасних суспільних процесів та взаємодій є придатним середовищем для таких інформаційних підривних дій. Цифрова глобалізація розмиває фізичні кордони між державами, фактично, порушуючи певний суверенітет держави. І якщо ще декілька десятиліть тому це розглядалося виключно як елемент загального світового прогресу для спрощення комунікацій між людьми, поширення знань, створення нових ринків і нового сектору економіки, то сьогодні ці технології перетворилися на зброю.

Росія хвора на імперський комплекс меншовартості, помилково прагнучи повернути собі статус наддержави, причому не шляхом створення конкурентної економіки, інновацій, спроможної торгівлі, тощо, а шляхом агресивних дій, як це колись робив СРСР. Застосування підривних технологій під час Холодної війни було доволі звичним явищем для сторін ще 50 років назад. Саме

комплекс таких підривних заходів, що включає в себе поширення дезінформації, використання агентів впливу, організацій прикриття, маніпулювання ЗМІ, тощо, добре описаний в аналітичній доповіді ««Активні заходи» СРСР проти США: пролог до гібридної війни» Національного інституту стратегічних досліджень України [13]. Проте Захід виявився неготовим до того, що після розпаду СРСР сучасна Росія вирішить скористатися такими ж заходами тільки вже з використанням сучасних технологій.

Загалом, російська влада спочатку випробувала ці технології на власному суспільстві. Монополізуючи владу над засобами масової інформації, вони вибудовували іншу альтернативну реальність для своїх громадян, де Захід став знову основним ворогом для Росії. Поширюючи державний контроль над соціальними мережами (Вконтакті, Одноклассники), Росія почала застосовувати перші свої фальшиві акаунти і ботів для формування політичної думки в громадян. Монополія на інформацію дозволила позбутися будь-яких політичних конкурентів та нівелювати спроби опозиції на поширення своєї точки зору. Загалом, джерела та розвиток російської цифрової пропаганди добре описаний в монографії С.Сановіча з Нью-Йоркського університету [11].

Сформувавши стабільну недемократичну систему всередині держави, Росія наважилась на використання цифрових технологій за межами країни. Так, в 2007 році Росія застосовує масову хакерську атаку на урядові мережі Естонії [5]. Все це відбувалося на тлі скандалу із перенесенням пам'ятнику радянському воїну, якого в Естонії вважають символом радянської окупації. Далі, такі заходи використовуються під час російського вторгнення до Грузії в 2008 році. Агресія проти України теж готувалася із використанням інформаційних операцій. Не викликає подиву той факт, що Росія використовувала інформаційні атаки перед анексією Криму, але це питання лише зараз починає отримувати розголос на Заході [8]. Так, використовуючи мережу своїх пропагандистських каналів як RT або Sputnik, Росія намагалася поширити хибні думки про внутрішній конфлікт в Україні, показати глядачу на Заході, що Росія це дружня і добра країна, і анексія чужої території не є злочином. Слід зазначити, що питання України, застосування хакерських атак Росією, інформаційні та пропагандистські операції, інша підривна діяльність ще тільки аналізується і вивчається. Це окрема тема великого дослідження.

В силу того, що російська агресія проти України не стала бліцкригом, а санкції повільно наносять удари по економіці держави, Росія почала вдаватися до більш активних дій, де ціллю вже стали уряди західних держав, політичний устрій.

Втручання в процес президентських виборів в США супроводжувався не тільки прямими діями росіян, але, як показує останнє розслідування компанії Facebook, за два роки з акаунтів, які «ймовірно керувалися з Росії», закупили політичної реклами на 100 тисяч доларів США. Внутрішнє розслідування виявило, що 3000 рекламних оголошень та постів було оплачено з 470 акаунтів та сторінок, за якими не стоять реальні люди. Реклама, яку за підрахунками, могли побачити від 23 до 70 мільйонів осіб, не була адресована на підтримку того чи іншого кандидата на президентських виборах у США [7]. Загалом, за останні два роки російську політичну рекламу побачили 126 мільйонів осіб [10]. Зміст постів більше стосувався суперечливих соціальних та політичних послань та зачіпав такі теми, як ЛГБТ, міжрасові стосунки, міграція, право на носіння зброї. Адміністрація Facebook дійсно занепокоєна тим, що соціальна мережа стала елементом політичного протистояння. Проводячи розслідування, вони одночасно шукають шляхи протидії інформаційним операціям. В аналітичній доповіді «Інформаційні операції та Facebook» вказується три основні елементи, на яких концентрується адміністрація:

– цілеспрямоване збирання даних з метою викрадення та, найчастіше, для викриття непублічної інформації, яка може забезпечити унікальні можливості для управління публічним дискурсом;

– створення контенту, неправдивого або реального, безпосередньо оператором інформації або ж шляхом надання інформації журналістам, іншим третім сторонам, у тому числі через фейкові онлайн-особи;

– несправжнє просування, яке адміністрація визначає як узгоджену діяльність неавторизованих облікових записів з метою маніпулювання політичною дискусією (наприклад, заважаючи конкретним сторонам брати участь у обговоренні або посилювати сенсаційні голоси над іншими) [12, с.6].

Сьогодні, Facebook здійснює обережні та неквапливі спроби вдосконалити свою мережу, з метою запобігти вищевказаним ризикам шляхом:

– постійного вивчення та моніторингу зусиль тих, хто намагається негативно маніпулювати громадським дискурсом на Facebook;

– введення інновацій у сферах доступу до облікового запису та цілісності облікового запису, включаючи виявлення фальшивих облікових записів;

– підтримки програм громадянського суспільства щодо медіа-грамотності [12, с.13].

Окремим прикладом використання Росією ботів, що впливають на політичні вподобання громадян інших держав, є Twitter. Акаунт «@TEN_GOP» був дуже помітним «голосом» у американських правих, за яким стежили понад 130 000 осіб, а деякі помічники Трампа робили репости його записів під час передвиборчої кампанії. Коли діяльність цього облікового запису була призупинена у липні 2017 року, то в мережі навіть почалися протести американських правих радикалів, не згодних із закриттям аканту. Але вже в жовтні Twitter підтвердив, що акаунт «@TEN_GOP» був фейковим і керувався російським оператором, пов'язаним із так званою «фабрикою тролів» в Санкт-Петербурзі [9].

Все це є прикладом використання нових засобів для дестабілізації політичної системи з метою підриву довіри громадян до політичних процесів, будь-яких джерел інформації тощо. Є ґрунтовні підозри, що подібні спроби втручання у виборчий процес був здійснений і проти Франції на президентських виборах 2017 року , та під час референдуму щодо виходу Сполученого Королівства з ЄС. Спланові інформаційні операції використовують гру на тих самих гострих темах (мігранти в ЄС, Brexit, світовий тероризм, іслам, права ЛГБТ тощо) утворюють єдину картину хаосу, що покликаний послабити демократію, підірвати віру людей в її цінності [2; 3].

Стосовно України, то сьогодні витрачається багато коштів на фізичне стримування Росії та підтримку армії. А тому інформаційна сфера залишається вкрай вразливою. Так, в політичній площині, в засобах масової інформації, в соціальних мережах в Україні діють актори, які активно просувають нову російську парадигму, що звучить наступним чином: «Ворог не в Кремлі, ворог в Києві». Ці актори використовують гострі і болючі теми для створення точки кипіння всередині держави, для того щоб люди не довіряли суспільним інститутам, для поляризації суспільства. Для таких маніпуляцій використовується будь-який вдалий привід – від проведення аналогу російської акції «безсмертний полк» на День перемоги над нацизмом у Другій світовій війні до використання маніпуляцій щодо мовного питання в освітній реформі, питання платної медицини в медичній реформі тощо. Здійснюються спроби використання української опозиції як «криголаму» української державності як такої. Адже не так давно Генеральною Прокуратурою України були надані матеріали, щодо можливості фінансування «протестних акцій» в Києві українським олігархом-втікачем Сергієм Курченко, що переховується в Росії і який звинувачується в Україні в державній зраді [17] . Всьому цьому спектру заходів особливо важко протистояти, враховуючи той факт, що до початку російської агресії, в Україні постійно працювали російські телеканали, фактично створюючи власну антиукраїнську парадигму, соціокультурна конвергенція погіршувалася з кожним роком, де російська культура намагалася поглинути українських громадян. Саме тому, тоді, коли була вчинена агресія, агресор не сприймався великою кількістю українців як ворог. Окремим питанням є спроби підірвати довіру до України серед її партнерів та сусідів. Окреме погіршення відносин між Україною та Польщею на ґрунті різної історичної пам'яті є якраз сприятливим середовищем для Росії, де вона передбачувано намагатиметься розсварити партнерів та союзників. Так, польські медіа самі публікували інформацію щодо можливості російського фінансування угруповань, що своїми діями та вандалізмом погіршували відносини двох держав [1].

Саме тому фахівці Гаазького центру стратегічних досліджень в своєму аналізі «Всередині Кремлівського будинку дзеркал: як ліберальні демократії можуть протистояти російській дезінформації та внутрішньому втручанню» надають важливий перелік заходів для стримування інформаційної агресії та пропаганди Росії [6]. Серед цих порад можна виокремити такі основні як:

1) інвестування у соціальну медіа грамотність для населення та для окремих специфічних верств (держслужбовці, військові, журналісти, блогери);

2) не боятися закривати російські телеканали за сприятливої можливості, коли вони явно поширюють фейкові новини або пропаганду, що загрожує суспільству;

3) не повторювати російські наративи і пропаганду, використовувати власні позитивні наративи для населення, застосовувати контрпропаганду;

4) не дозволяти Росії використовувати структурні проблеми суспільства – уряд повинен звертатися до цих проблем;

5) ідентифікувати тих політиків, представників громадських організацій тощо, що мають постійні контакти з Росією;

6) витрачати кошти на розвиток аналізу з біг дата для виявлення тих груп населення, що найбільш вразливі для російської дезінформації;

7) розуміти, що Росія веде проти цивілізованого світу політичну, некінетичну війну.

Тому треба визнати, що протидія деструктивним підривним заходам все ж відбувається. Поки в США йде розслідування втручання Росії у вибори, Європейський парламент ще в листопаді 2016 року прийняв резолюцію, в який заявив, що «уряд Росії використовує широкий спектр засобів та інструментів, таких як аналітичні центри та спеціальні фонди (наприклад, «Русский мир»), спеціальні органи («Россотрудничество»), багатомовні телевізійні станції (наприклад, RT) , псевдо новинні агентства та мультимедійні сервіси (наприклад, "Sputnik"), транскордонні соціальні та релігійні групи (...) соціальні мережі та інтернет-тролі, з метою кинути виклик демократичним цінностям, розділити Європу, отримати внутрішню підтримку та створити сприйняття східних сусідів ЄС як держав, що не відбулися» [так звані «failed states» – прим. авт.], закріплюючи таким чином стратегію протидії інформаційній загрозі з боку Росії [4].

Висновок. Таким чином, ми можемо сформулювати **мету** російсько-української гібридної війни, яка полягає **в створенні хаосу, підриві цінностей демократичного світу і культивації всеохоплюючої атмосфери недовіри і нігілізму**. Ця мета поширюється не тільки на Україну, а й на ті держави, що її підтримують. Саму демократію Росія, яка сама не знає демократичних традицій, перетворила на нашого ворога. Використовуючи основні цінності демократії як зброю, агресор домігся того, що свобода слова перетворилася в право на брехню, свобода на отримання інформації – в свободу на поширення фейків, брехні і пропаганди, свобода на мирні зібрання – в право на вуличні зіткнення, а соціальні мережі – на хаотичне зібрання неіснуючих осіб для розпалювання ворожнечі. Підривається сама ідея демократії, піддається сумніву сама можливість вільного, чесного і неупередженого волевиявлення особи.

Саме тому, класифікуючи за метою такі інформаційні операції, ми можемо виділити: 1) операції щодо розколу суспільства всередині держави для її ослаблення або приведення до влади власних кандидатів; 2) операції, для дискредитації держави на світовій арені та для напруження відносин з її сусідами або партнерами; 3) операції з розповсюдження загального інформаційного хаосу для досягнення окремих власних тактичних цілей агресором.

Саме тому ми можемо казати, що за умов активного інформаційного протиборства, коли державу намагаються знищити і захопити зсередини, інформаційні підривні технології мають на меті десоціалізацію особистості. Ця особа не довіряє владі, за яку вона голосувала, не довіряє інститутам демократії, не довіряє медіа, не довіряє сусідам. Втрачаючи власні цінності, така особа починає довіряти фейкам і чужій пропаганді. Особа, вирвана із нормального суспільства, що втратила будь-які ціннісні орієнтири, сама того не бажаючи стає зброєю ворога, а тому слід проводити правильну і виважену інформаційну політику, займатися інформаційною безпекою, інформаційною грамотністю та вчасно реагувати на нові підривні технології та інформаційні пастки.

Бібліографічний список:

1. Andrusieczko P., Poczobut A., Wojtczuk M. Za kasę z Rosji w Polsce przeciw Ukrainie [Електронний ресурс] // Gazeta Wyborcza. – Режим доступу: http://wyborcza.pl/7,75399,21472245,za-kase-kremla-w-polsce-przeciw-ukrainie.html?disableRedirects=true

2. Booth R., Weaver M., Hern A., Walker S. Russia used hundreds of fake accounts to tweet about Brexit, data shows [Електронний ресурс] // The Guardian. – Режим доступу: https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets

3. Daniels L. How Russia hacked the French election. [Електронний ресурс] // POLITICO. – Режим доступу: https://www.politico.eu/article/france-election-2017-russia-hacked-cyberattacks/

4. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)) [Електронний ресурс]. – Режим доступу: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0441+0+DOC+XML+V0//EN

5. Grassegger H., Krogerus M. Fake news and botnets: how Russia weaponised the web. [Електронний ресурс] // The Guardian. – Режим доступу: https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia

6. Jong S. de, Sweijs T., Kertysova K., Bos R. INSIDE THE KREMLIN HOUSE OF MIRRORS. How Liberal Democracies can Counter Russian Disinformation and Societal Interference. [Електронний ресурс] // The Hague Centre for Strategic Studies. – Режим доступу: https://www.hcss.nl/sites/default/files/files/reports/Inside%20the%20Kremlin%20House%20of%20Mirrors_0.pdf

7. Leonnig C., Hamburger T. and Helderman R. Russian firm tied to pro-Kremlin propaganda advertised on Facebook during election [Електронний ресурс] // The Washington Post. – Режим доступу:

https://www.washingtonpost.com/politics/facebook-says-it-sold-political-ads-to-russian-company-during-2016-election/2017/09/06/32f01fd2-931e-11e7-89fa-bb822a46da5b_story.html?utm_term=.de6206fe1b8e.

8. Nakashima E. Inside a Russian disinformation campaign in Ukraine in 2014 [Електронний ресурс] // The Washington Post. – Режим доступу: https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html?utm_term=.f64454e2ed36.

9. Nimmo B. How A Russian Troll Fooled America [Електронний ресурс] // Atlantic Council's Digital Forensic Research Lab Режим доступу: https://medium.com/dfrlab/how-a-russian-troll-fooled-america-80452a4806d1

10. Russia-linked posts 'reached 126m Facebook users in US' [Електронний ресурс] // BBC. – Режим доступу: http://www.bbc.com/news/world-us-canada-41812369

11. Sanovich S. Computational Propaganda in Russia: The Origins of Digital Misinformation [Електронний ресурс] // University of Oxford. – Режим доступу: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Comprop-Russia.pdf.

12. Weedon J., Nuland W., Stamos A. 2017. Information Operations and Facebook [Електронний ресурс]. – Режим доступу: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

13. «Активні заходи» СРСР проти США: пролог до гібридної війни: аналіт. доп. / Д.В. Дубов, А.В. Баровська, Т.О. Ісакова, І.О. Коваль, В.П. Горбулін; за заг. ред. Д.В. Дубова. – 2-ге вид. – К. : НІСД, 2017. – 52 с.

14. Андриевский Т. Гибридная война: сущность и базовые стратегии [Електронний ресурс] / Тимур Андриевский // De securitate et defensione.– 2017. – № 1(3). – с. 158-166. – Режим доступу: http://www.desecuritate.uph.edu.pl/images/De_Securitate_12_Andrewskij.pdf.

15. Отчет о действиях по предварительному расследованию (2016 г.) [Електронний ресурс] // Международный Уголовный Суд. – Режим доступу: https://www.icc-cpi.int/iccdocs/otp/161114-otp-rep-PE-Ukraine.pdf.

16. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. – К. : НІСД, 2017, с. 496

17. Юрій Луценко повідомив, що ГПУ спільно з СБУ виявлено факт фінансування С. Курченком масових акцій протесту у містах України [Електронний ресурс]. – Режим доступу: https://www.gp.gov.ua/ua/news.html?_m=publications&_t=rec&id=220231&fp=60

Andriyevskyy T. G. The purposes of Russian-Ukrainian hybrid war

The article evolves the concept that the Russian-Ukrainian hybrid war has a significant impact on the world order and international relations. New digital undermining technologies that the Russian Federation exploits during the conflict are described. Among others, the emphasis is made on the fake news, propaganda, interference in the election processes, cyberattacks that are a new weapon of the new generation warfare – hybrid war or war of the information society.

The article describes some peculiarities of subversive activity of the Russian Federation. Among other, examples of above-mentioned subversive activities are described: from cyberattacks against government sites in Estonia in 2007 to the current challenges that the West faces. In particular, the role of social networks in the context of their influence on political processes in democratic states is revealed. There is a special emphasis on the possible intervention of the Russian Federation in the process of the presidential election in the United States, in particular, in the context of information operations on social networks such as Twitter and Facebook. The results of monitoring the activity of fake accounts, conducted by the security service of Facebook, are presented.

The article finds out certain goals of Russian aggression and its undermining measures. It was determined that the main goal of the Russian-Ukrainian hybrid war at this stage is to create chaos, undermine the values of the democratic world, and foster a comprehensive atmosphere of mistrust and nihilism. In addition, it is argued that the aggressor uses the institutions of democracy itself and their weaknesses as a weapon. The classification of information operations by their purpose in the context of hybrid warfare is proposed.

Key words: *war, hybrid war, Russian-Ukrainian war, fake news, propaganda, undermining technologies, informational operations, Twitter, Facebook.*