УРОКИ ГІБРИДНОГО ДЕСЯТИЛІТТЯ:

що треба знати
для успішного руху вперед

КИЇВ, 2019

УРОКИ ГІБРИДНОГО ДЕСЯТИЛІТТЯ: ЩО ТРЕБА ЗНАТИ ДЛЯ УСПІШНОГО РУХУ ВПЕРЕД

Публікацію підготовлено на запит Офісу Віце-прем'єр-міністра з питань європейської та євроатлантичної інтеграції України та Урядового офісу координації європейської та євроатлантичної інтеграції в рамках діяльності Платформи Україна–НАТО з вивчення досвіду протидії гібридній війні.

ЗМІСТ

У середині 2015 року з'явилася пропозиція створити Платформу Україна-НАТО з вивчення досвіду протидії гібридній війні. Відповідне рішення було ухвалено вже під час Варшавського саміту НАТО у 2016 році, як один із елементів Комплексного пакету допомоги Україні (Comprehensive Assistance Package). Конференція «Уроки гібридного десятиліття: що треба знати для успішного руху вперед», яка відбулась 7-8 листопада 2018 року за ініціативи уряду України, стала логічним продовженням співробітництва в рамках цієї платформи.

Метою заходу було детально розглянути гібридні засоби ведення війни, вивчити шляхи протидії їм, у тому числі із врахуванням відповідного досвіду України, Грузії, Естонії, Великої Британії, Литви, Польщі, Латвії та інших держав, а також врахувати ризики, що постають перед Україною та державами Заходу.

Мета цієї публікації – підсумувати дискусії, які розгорнулися під час конференції «Уроки гібридного десятиліття», проаналізувати основні напрямки та питання, які обговорювались під час відповідних сесій, та сформулювати рекомендації для посилення співробітництва в сфері протидії гібридним загрозам і розбудови стійкості в Україні та державах-партнерах.

НА ПЕРЕДНЬОМУ КРАЮ ГІБРИДНОЇ ВІЙНИ: ВІД БАЛТИКИ ДО ЧОРНОГО МОРЯ

Гібридна війна не є винаходом Російської Федерації. Але Москва вдосконалила її інструменти та збільшила масштаби їхнього застосування. Випробувавши цілий арсенал методів ведення гібридної війни, Росія фактично демонструє формат війни майбутнього, де інформаційні та кібер-технології, розвідка та політичний вплив «тихої війни», загроза силою та використання бойовиків можуть відігравати більше значення, ніж пряме військове втручання.

У своїй вступній промові Президент України Петро Порошенко зазначив, що *нині нема тих, хто заперечуватиме, що реваншистська політика Кремля проти України стала спільним викликом для євроатлантичної безпеки, як і те, що без сильної України, яка перетворилася на де-факто східний фланг НАТО, не може бути й мови про стабільний євроатлантичний простір*.

За словами Іванни Климпуш-Цинцадзе, Віце-прем'єр-міністра з питань європейської та євроатлантичної інтеграції України, найбільшим викликом сьогодення для демократичного світу є усвідомлення нових гібридних загроз та формулювання спільної дієвої відповіді.

Заступник Генерального секретаря НАТО з питань нових викликів безпеці

Антоніо Міссіролі підкреслив, що *гібридна війна, за своєю суттю, не є чимось новим. Новинкою стала велика кількість інструментів, які зараз доступні для гібридних кампаній*.

Інформаційні атаки, спроби дестабілізації ситуації в середині країни, енергетичний шантаж, повне ембарго і закриття ринків, агресивне нав'язування свого порядку денного через агентів впливу, через агентів в політичній, культурній сфері, розпалювання соціальних конфліктів, вплив через релігійні організації – це далеко не весь російський інструментарій, який, на думку Президента П. Порошенка, нарешті отримав назву гібридного.

А. Міссіролі наголосив, *що ми зможемо подолати гібридні загрози, якщо зробимо три кроки: перший – аналізувати, що відбувається насправді, оскільки першочерговою метою гібридної війни є ввести в оману та заплутати; в ідеалі, жертва не зрозуміє, що з нею відбувається до того моменту, коли вже запізно відповідати ефективно. Це становить проблему для окремих держав, але є ще більшим викликом для Альянсу, де рішення приймаються консенсусом, саме тому НАТО підвищує свої розвідувальні та аналітичні спроможності. Крок два – відповідь. Ми вже краще реагуємо на кібератаки і знаємо моделі гібридних дій, що дозволяє нам швидше боротися з пропагандою. До того ж, ми нарешті почали називати речі своїми іменами. Це не зупинить агресора, але дасть йому зрозуміти, що за будь-яку атаку доведеться платити ціну. Третій крок – це посилення стійкості. Ми повинні думати як захиститися, як мінімізувати негативні наслідки гібридних атак та захистити критичну інфраструктуру. І оскільки більшість інфраструктури у сфері енергетики та комунікацій знаходиться у приватних руках, то ми повинні розвивати приватно-державне партнерство*».

> Ми ніколи не зможемо визначити, що саме є перемогою у гібридній війні. Тому що гібридна війна – це процес; процес, який ніколи не закінчується

Україна почала використовувати термін «гібридна війна» лише у 2014 році, і, як визначив Президент П. Порошенко, лише тому, що у 2008 ми ще не знали, як називати дії Росії в Грузії. Сьогодні, і Україна, і Грузія, на думку Валдіса Затлерса, очільника Латвії у 2007-2011 роках, відчули на собі всі 4 етапи гібридної війни – формування стратегії, розробку операцій, проведення операцій та консолідацію результатів.

І хоча більшість методів зовсім не нові, за словами І. Климпуш-Цинцадзе, те, що раніше слугувало допоміжним фактором у протистоянні (як наприклад, інформаційні атаки), сьогодні стає його основним інструментом. Навіщо завойовувати силою, якщо можна підкорити свідомість?

Ростислав Павленко, директор Національного інституту стратегічних досліджень, визначив, що у політичному

дискурсі демократичних країн й у взаємодії з іншими країнами дуже важливо розуміти, що вчасне виявлення, вчасна спільна протидія допоможуть попередити набагато більшу загрозу й економічні втрати. І. Климпуш-Цинцадзе пояснила, що метою атак ворожих держав (hostile state actors) є не завоювання, а підпорядкування слабших та деморалізація сильних.

На думку, В. Затлерса, ми ніколи не зможемо визначити, що саме є перемогою у гібридній війні. Тому що гібридна війна – це процес; процес, який ніколи не закінчується. Йому заперечує Р. Павленко – *перемогою в гібридній війні можна вважати відмову агресора від ведення цієї війни*.

І. Климпуш-Цинцадзе підкреслила, *що НАТО є наразі єдиною міжнародною структурою, здатною сформувати дієву та адекватну відповідь російській гібридній війні*. При цьому, Президент Порошенко акцентував, *що сьогодні вже Україна має досвід, яким готова поділитися зі світом*.

Заступник Генерального секретаря НАТО А. Міссіролі наголосив, *що гібридна війна і гібридні кампанії є основним викликом для всіх нас, але ми зустрічаємо їх разом, і якщо так і продовжимо, то будемо до них готові*. Голова Верховної Ради України Андрій Парубій у своєму виступі також підкреслив, *що на ці гібридні виклики ніхто не зможе відповісти самостійно. Ця загроза є глобальною, і тому відповідь на неї має бути теж глобальною... Розпочавши агресію проти України, Путін кинув виклик всьому вільному світу.*

Рівень усвідомлення «гібридних» загроз серед членів НАТО та ЄС, а також їх партнерів залишається дуже різним. За останнє десятиріччя Україна та Грузія відчули повну силу поєднання традиційних, конвенційних та неконвенційних дій з боку Російської Федерації. Однак, список країн, які є жертвами гібридних операцій, є набагато ширшим. Передусім, це країни, що перебувають в зоні російських інтересів: країни Балтії, Центрально-Східної Європи та Східного партнерства.

Відповідно до результатів дослідження, проведеного European Values Think-Tank[1] на основі аналізу національних стратегічних документів, звітів та офіційних заяв усіх 28 держав-членів ЄС, з метою підсумувати, як окремі європейські країни реагують на зростаючу загрозу російської підривної діяльності (а саме: державні установи, контррозвідувальне співтовариство і неурядовий (громадський) сектор), – лише 5 країн ЄС (Велика Британія, Швеція, Естонія, Латвія та Литва) знаходяться в групі «А» – тобто повною мірою усвідомлюють загрозу, вживають контрзаходи на рівні уряду та розвідки. Також, за результатами дослідження 2 країни були названі «колаборантами Кремля» – Греція та Кіпр. Вони не чинили жодного спротиву підривній діяльності Росії.

1 "2018 Ranking of countermeasures by the EU28 to the Kremlin's subversion operations". Kremlin Watch Report. European Values Think-Tank. 13.06.2018. https://www.kremlinwatch.eu/userfiles/2018-ranking-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations.pdf

Окрім того, за результатами аналізу, який був проведений у 2018 році консорціумом організацій на чолі з Радою зовнішньої політики «Українська призма», було розроблено Індекс стійкості до дезінформації. Метою цього дослідження стала оцінка рівня стійкості до іноземних, насамперед кремлівських, дезінформаційних кампаній в 14 країнах Східної та Центральної Європи. За всіма трьома показниками (схильність і сприйняття контенту прокремлівських ЗМІ, якість системної реакції та уразливість до прихованої дезінформації) Молдова опинилась в кінці рейтингу. Результати інших країн не такі однозначні, загалом, у групі ризику опинилися Латвія, Білорусь, Україна. Експерти відзначили, що практично у всіх країнах Центральної та Східної Європи відсутні якісні системні відповіді на інформаційні атаки, як і довгострокові національні стратегії боротьби з іноземними дезінформаційними кампаніями.

РОСІЙСЬКА ГІБРИДНА ВІЙНА: КОНЦЕПЦІЯ ТА РЕАЛЬНІСТЬ

Незважаючи на те, що гібридна війна, її інструменти та етапи досить добре описані у академічній літературі, російська агресія в Україні, незаконна анексія Криму та подальші дії на сході України актуалізували це питання на міжнародному порядку денному, поставили нові питання щодо інструментів гібридної війни та нелінійних засобів, до яких вдається Російська Федерація.

Як справедливо зазначає угорський дослідник Андраш Рац, проривом у дискурсі, що стосується гібридної війни та гібридних загроз стало застосування відповідних термінів з боку НАТО.[3] У NATO Review від 1 липня 2014 року представники Альянсу публічно і відверто вказали на те, що новою формою ведення війни стала «гібридна війна».[4]

Невдовзі цей вираз підхопили провідні світові медіа, а під час саміту НАТО в Уельсі у вересні 2014 року було запропоновано вважати «гібридними» засобами «широке коло високоінтегрованих відкритих та прихованих мілітарних, парамілітарних

2 Russian Disinformation Resilience Index. The Foreign Policy Council "Ukrainian Prism". 2018. http://prismua.org/wp-content/uploads/2018/06/DRI_CEE_2018.pdf

3 A. Racz, "Russia's Hybrid War in Ukraine: breaking the enemy's ability to resist", *FIIA Report 43*, 16.06.2015, http://www.fiia.fi/en/publication/514/russia_s_hybrid_war_in_ukraine

4 Hybrid war - hybrid response? *NATO Review*, 01.07.2014, https://www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-crisis-war/EN/index.htm

та цивільних засобів» (п.13).[5] А вже у 2016 році на саміті у Варшаві було вирішено поширити дію статті 5 Вашингтонського договору на атаки проти одного із союзників з використанням гібридних методів: «Альянс та його члени будуть готові протидіяти гібридній війні в рамках колективної оборони. Північноатлантична рада може прийняти рішення про приведення у дію статтю 5 Вашингтонського договору» (п.72).[6] Тоді ж було затверджено і стратегію протидії гібридній війні.

Водночас, варто зазначити, що термін «гібридна війна» вже активно використовувався військовими США та НАТО з 2006 року – стосовно дій Хезболли в ході лівансько-ізраїльського конфлікту.[7] А методи «гібридної війни» активно застосовувались в античні часи, середньовіччя та спецслужбами Радянського Союзу.

Серед авторів детальних визначень гібридної війни почасти згадують Вільяма Немета, Джона Маккюена, Френка Гоффманна та Рассела Гленна. Деякі вважають, що термін «гібридні засоби» походить з праць В. Немета про чеченську війну, у яких він згадує, що під час цього конфлікту дії сторін не обмежувалися полем бою, а стали поєднанням регулярних та нерегулярних методів і їх гнучких комбінацій у ширшому, нелінійному сенсі із застосуванням інформаційних засобів, спрямованих на здобуття переваг над противником.[8]

Для Дж. Маккюена гібридні конфлікти включають повний спектр воєн у їх фізичному та концептуальному вимірах, включно з боротьбою проти озброєного противника, ширшою боротьбою за підтримку місцевого населення, а також за підтримку міжнародної спільноти.[9]

Ф. Гоффманн, у свою чергу, вважає, що гібридні ризики включають засоби різної форми: конвенційні спроможності, нерегулярні тактики і формування, терористичні акти включно з невибірковим насильством та примусом, а також кримінальний безлад і загалом є операційно та тактично керованими і скоординованими задля досягнення синергетичного ефекту у фізичному та психологічному вимірах конфлікту.[10]

---

5 Wales Summit Declaration. NATO Official website. 05.09.2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm

6 Warsaw Summit Communique. North Atlantic Treaty Organization. 09.07.2016, https://www.nato.int/cps/uk/natohq/official_texts_133169.htm?selectedLocale=en

7 D. E. Mason, An Assessment of the 2006 Lebanon-Israeli War. Joint Forces Staff College. 2009, https://apps.dtic.mil/dtic/tr/fulltext/u2/a530150.pdf, або R. Gates, "A Balanced Strategy: Reprogramming the Pentagon for a New Age". *Foreign Affairs*, January/February 2009, Vol. 88, No. 1, pp. 28-40.

8 W. J. Nemeth, "Future War and Chechnya: A Case for Hybrid War". *Monterey Naval Postgraduate School thesis*, 2002, p. 74, http://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf

9 J. J. McCuen, "Hybrid Wars". *Military Review*. March–April. 2008, p. 108, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20080430_art017.pdf

10 F. G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies. December 2007, p. 8. http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Серед першочергових питань, які становлять академічний та практичний інтерес і на які спробували відповісти учасники міжнародної конференції «Уроки гібридного десятиліття: що треба знати для успішного руху вперед», стало питання про ***досвід України як полігону для випробувань гібридних тактик та питання проявів гібридної війни у Європі та Північній Америці.***

Можна погодитися із заступником секретаря Ради національної безпеки та оборони України Олександром Литвиненком, який в своєму виступі зазначив, що *гібридна війна належить до широких та вкрай розмитих понять. Чи не головною ознакою гібридних заходів є складність доведення причетності до них їхніх організаторів і проблематичність їх покарання за вчинені злочини. Іншими словами «их там нет» і «не докажете».*

З наведеними вище визначеннями також перегукуються тези О. Литвиненка про те, що *гібридні засоби – це не стільки пряме порушення правових норм, а й зловживання цими нормами, не стільки пряме застосування сили, але й шантаж, а іноді й блеф різного ступеню відвертості*. Головним об'єктом російських стратегій стала не фізична реальність, а поле її інтерпретації і сенсів. Боротьба точиться не за території, а за мізки і душі людей, що їх населяють.

При цьому, справедливо зауважити, що росіяни повністю підпорядковують військові інструменти політичним цілям. Можна стверджувати, що такий російський підхід ґрунтується на «революційному експансіонізмі»[11] – підході, що поєднує сталі стратегічні цілі Російської Федерації і нові інструменти гібридної війни з радянськими концепціями глибоких операцій, активних заходів і рефлексивного управління.

> Чи не головною ознакою гібридних заходів є складність доведення причетності до них їхніх організаторів і проблематичність їх покарання за вчинені злочини

Таким чином, у російському гібридному підході ми, значною мірою, стикаємось з продовженням застосування радянських методів, які адаптовані до нових політичних реалій. При цьому, як зазначає дослідник Ендрю Данкан, Росія інтегрує всі елементи національної потуги (power) у своїх спробах тиску на державу-ціль, а концепція активних заходів пояснює застосування проксі-сил і різнорідних інформаційних операцій.[12]

11 A. Tsygankov, "From International Institutionalism to Revolutionary Expansionism: The Foreign Policy Discourse of Contemporary Russia", *Mershon International Studies Review*, Vol. 41, No. 2, November 1997, p. 249.

12 A. Duncan, "New 'Hybrid War' or old 'dirty tricks'? The Gerasimov Debate and Russia's response to the Contemporary Operating Environment". *Canadian Military Journal*. Vol. 17, No. 3, Summer 2017. http://www.journal.forces.gc.ca/Vol17/no3/PDF/CMJ173Ep6.pdf

Радник Президента України, перший віце-президент Національної академії наук України В. Горбулін поділився своїми думками про те, що вирізняє гібридний тип війни з-поміж інших. На його думку, *перш за все – високий ступінь невизначеності. Гібридна війна стирає грань між війною та миром, війною та політикою. Розмитість є однією з ключових ознак такої війни. Незрозуміло, хто із ким воює. Виникають труднощі у визначенні сторін конфлікту, а агресор завжди намагається додатково посилити цю невизначеність, весь час змінюючи риторику щодо конфлікту: від «в Україні громадянська війна» до «в Україні Росія воює з Америкою». Але все це заради маскування ключової тези: Росія воює з Україною. Ця невизначеність призводить до ще одного наслідку – ускладнення спроб врегулювання конфлікту дипломатичними методами і це особливо добре видно на практиці Нормандського формату та Мінських угод.*

> Що вирізняє гібридний тип війни з-поміж інших, перш за все – високий ступінь невизначеності

Таким чином, ключовою ознакою сучасної гібридної війни, яка водночас перешкоджає її ідентифікації, є те, що вона розгортається у т.зв. сірій зоні. За висновками Норвезького інституту міжнародних відносин: «гібридна війна розмиває різницю між війною та миром, оперуючи поза межами нашого розуміння війни як насильницького зіткнення сил, та ставлячи під сумнів наше розуміння початку та кінця воєнних дій».[13]

Як, у свою чергу, вказав О. Литвиненко – *ключовим джерелом для російської гібридної війни залишається російська стратегічна культура, наріжними каменями якої є: схильність до гіперреалізму або, іншими словами «Росія – це про силу», широке застосування стратегічного введення в оману, спирання на проксі-структури, а також використання клієнтських держав та суспільств у своїй безпосередній діяльності. Непересічне значення має надзвичайна гнучкість росіян у застосуванні доволі вузького постійного арсеналу засобів при незмінності стратегічних цілей*.

Тези О. Литвиненка про те, що *особливістю російської гібридної агресії виступає її системність, скоординованість операцій з одного центру (хоча далеко не завжди йдеться про жорстке управління, яке, в принципі, залишається базовим російським підходом), але й про використання координації мережевого типу на основі спільних цінностей, ідей і підходів, що притаманні всім виконавцям гібридних заходів*, також перегукуються із західними дослідженнями у сфері гібридних війн. Дослідники одноголосно стверджують: такий підхід став можливим завдяки використанню сучасних інформаційних технологій, насамперед Інтернету та соціальних мереж.

13 "Hybrid warfare – how to counter it?" Norwegian Institute of International Affairs, 07.11.2018. https://www.nupi.no/en/News/Hybrid-warfare-how-to-counter-it

Заступник Міністра закордонних справ України з питань європейської інтеграції Олена Зеркаль у своєму виступі відсилає до праць колишнього глави Пентагону Джеймса Метті́са, який ще у 2005 році зазначав, що гібридна агресія скомпонована з різних елементів. Вона включає в себе організовану злочинність, традиційні конвенційні військові дії, а також тероризм в усіх його проявах, зокрема, кібертероризм, а також використання засобів впливу на масову свідомість.

Гібридний підхід, зокрема російський, базується на виявленні а, подекуди створенні і експлуатації вразливості противника. *Кожне суспільство вразливе по-своєму, але помітні й певні загальні підходи* – додав О. Литвиненко. Але разом з тим, він зазначив: *показово, що найбільш шкідливі практики, що спрацювали в окремих регіонах України, росіянам навіть не вдалось перенести на інші регіони. Саме у цьому виявилась обмежена ефективність російських підходів. У Кремля все вдавалось і вдається там, де вони мають розуміння ситуації, де можуть передбачити реакції, де вони володіють надійною експертизою. При цьому, йдеться не тільки й не стільки про схід України, але й, наприклад, про Сирію.*

Окрім того, на думку заступника Міністра закордонних справ Грузії Лаші Дарсалії, Росія прагне контролювати або, щонайменше, впливати на внутрішні політики держав регіону, підпорядковувати їх російським інтересам. Як зазначають дослідники Ендрю Вільсон та Ніку Попеску, російський вплив подекуди застосовує елементи «м'якої сили». Щоправда, це дуже своєрідне тлумачення цього поняття, оскільки Росія не служить моделлю модернізації і не спонукає до таких позитивних зрушень, як демократизація та інтеграція. Йдеться про те, щоб за допомогою «м'якої сили» змусити інших виконувати російські забаганки.[14]

Росія прагне контролювати або, щонайменше, впливати на внутрішні політики держав регіону, підпорядковувати їх російським інтересам

О. Литвиненко також звернувся до кількох базових підходів, які можна визначити за результатами аналізу російського досвіду: *Росіяни вважають себе незаслужено ображеними Заходом, насамперед – США, і прагнуть реваншу за поразку в «холодній війні». Йдеться про відновлення величі, що лишилась в минулому, чи навіть точніше – про відчайдушний спротив уявним прагненням ліберального Заходу підкорити і знищити Російську Федерацію. Від «Мюнхенської промови» 2007 року* (коли, виступаючи на Мюнхенській конференції з безпеки, російський президент Владімір Путін розкритикував однополярну систему

14 A. Wilson, and N. Popescu. "Russian and European neighbourhood policies compared". *Southeast European and Black Sea Studies*. 2009, Vol. 9, No. 3, p. 319.

міжнародних відносин і натякнув на те, що російська активність на міжнародній арені дедалі більше зростатиме,[15] – і стало зрозуміло, що Росія спробує скоригувати міжнародну ситуацію до російського бачення майбутнього і російських стратегічних цілей, які передбачають відновлення російського статусу супердержави у дво- чи багатополярній системі та спробує відновити російський вплив у світі), *через «зачем нам мир без России» і «государство-полукровку»,*[16] *й аж до «рая для россиян»,*[17] *як наслідок невпевненості у власних силах і прагнення використати останній уявний шанс на виживання.*

Водночас, Л. Дарсалія зазначає, що *діяльність Росії, спрямована проти Заходу, виокремлює Росію як цивілізацію, що не є європейською і, можливо, навіть не є азіатською.*

Не можна заперечити, що у Кремлі, теоретично, можуть уявити світ, у якому Росія втратить статус ключового гравця, і саме цього і бояться. Така непевність викликає принципову реакційність російської зовнішньої безпекової політики, а через це – її емоційний характер. Росія виступає як своєрідний «реакційний революціонер», що підриває світовий порядок, спекулюючи, водночас, принципом легітимності. Саме тому, бажаними союзниками Кремля виступають антисистемні сили в Америці та Європі: і не важливо, ультраправі чи ультраліві. Йдеться також про використання етнічних і релігійних меншин та спекуляцію на темі колективних прав, насамперед, на темі «співвітчизників» за кордоном. Дослідники Мері Коннел та Раян Еванс[18] вказують на те, що для Росії типовим є використання етнічного російського населення як «п'ятої колони» для організації протестів та опору урядам держав, на які спрямована російська агресія. Це, в свою чергу, викликає опір з боку уряду і більшості населення, що призводить до чергового витка ескалації. Таким чином Росія інспірує внутрішні конфлікти.

Понад те, варто згадати, що Росія не обмежує визначення «співвітчизників (росіян)» етнічними росіянами. В. Путін відносить до росіян усіх, хто такими себе відчуває.[19] Розділена російська нація, що встає з колін – постійний рефрен російської пропаганди. Сучасна Російська Федерація перетворює росіян на, де-факто, заручників своєї етнічної належності, незалежно від їхнього громадянства і поглядів.

---

15 "Vladimir Putin speech and the following discussion at the Munich Conference on Security Policy". Kremlin official website. 2007. http://en.kremlin.ru/events/president/transcripts/24034

16 В. Сурков. "Одиночество полукровки". *Россия в глобальной политике*. 09.04.2018. https://globalaffairs.ru/global-processes/Odinochestvo-polukrovki-14-19477

17 Заседание дискуссионного клуба «Валдай». Владимир Путин принял участие в пленарной сессии юбилейного, XV заседания Международного дискуссионного клуба «Валдай». Kremlin official website. 18.10.2018. http://kremlin.ru/events/president/news/58848

18 M. Connel, R. Evans, "Russia's 'ambiguous warfare' and implications for the U.S. Marine Corps". *CNA's Occasional Paper*. May 2015. https://www.cna.org/cna_files/pdf/dop-2015-u-010447-final.pdf

19 M. Wehner, "Goals of Putin, ideology of Russia", *Inosmi*, 05.05.2015. http://inosmi.ru/politic/20160505/236420932.html (in Russian)

Заступник Міністра закордонних справ України Олена Зеркаль окремо вказала і на те, що *Росія повернулась до імперсько-радянської традиції побудови відносин з абсолютною неповагою до міжнародного права, використовуючи при цьому нові інструменти технічного впливу, соціального впливу, якими досконало маніпулює. За її словами, світ, який створювався після Другої світової війни, і відповідний міжнародно-правовий порядок були не готові до відповіді, до відсічі агресії Росії у 2014 році, зважаючи на те, що країни Заходу, як і Україна, базували свої дії і плани виключно на засадах і принципах міжнародного права. У той же час, агресія, яку ми спостерігаємо в Україні, довела, що в сучасному світі конвенційні реакції і конвенційні дії вже недієві, оскільки Росія теж не використовує конвенційні засоби війни*.

Проте, як зазначила О. Зеркаль, *коли в 2014-2015 роках ми говорили, що Україна потерпає від російської агресії, всі намагалися нав'язати нам наратив: «А давайте не будемо говорити, що це агресія. Давайте говорити про те, що це конфлікт. Бажано – внутрішній». Бо виникало занепокоєння щодо того, як це буде сприйнято західними суспільствами, і що може виникнути певний опір зусиллям допомогти Україні. У той період представники МЗС намагалися налагодити постійний діалог з партнерами для того, щоб уникати застосування саме тих термінів і наративів, які були вигідні Російській Федерації, що намагалася уникнути відповідальності, використовуючи усі можливі прогалини у міжнародному праві і, взагалі, усі психологічні моменти, пов'язані з небажанням визнавати можливість загрози.*

При цьому Росія вважала, що вона повністю убезпечена від відповідальності, пов'язаної з агресією. Як постійний член Ради Безпеки ООН, Росія й дотепер захищає своє право на абсолютно безкарну поведінку, хоча при цьому вимушена поступатися своїм іміджем, як це було під час розгляду резолюції зі створення міжнародного трибуналу щодо розслідування за фактом збиття літака рейсу МН17, коли тільки Росія, як країна-парія, використала право вето. Трибунал не було створено.

Не можна заперечити тези О. Зеркаль про те, що *Росія маніпулює не тільки правом, але й свідомістю. Однак, несподівано для Росії, західні суспільства починають усвідомлювати цю маніпуляцію. Те, що відбувається зараз у Голландії – відповідь на постійні вкиди інформації щодо провини України у катастрофі МН17, обвинувачення в тому, що слідство не вживає достатніх заходів для розслідування, що немає підстав вважати, що Росія винна. Нині ці російські тези викликають зовсім іншу реакцію*. Те, що Нідерланди разом з Австралією запросили Росію до консультацій щодо відповідальності Росії як держави за збиття Боїнгу – це великий крок вперед і успіх, адже ще три роки тому ніхто не міг собі уявити, що Австралія і Нідерланди будуть готові звинувачувати Росію як країну.

Так само змінюється усвідомлення в інших країнах, приміром, «справа Скрипалів» стала поштовхом до переоцінки ризиків у Великій Британії і виявила те, що британці теж є не-

захищеними від російської гібридної агресії. І неважливо, де знаходиться країна – вона може стати жертвою гібридної агресії, оскільки росіяни дійсно вірять в те, що вони не будуть притягнуті до відповідальності, і ніхто не зможе використати проти них інструменти міжнародного права, бо вони є недієвими.

> Гібридні конфлікти мають сталу здатність перетворювати географічно локальні та регіональні конфлікти в інформаційно-глобальні

Вартими уваги є тези радника Президента України Володимира Горбуліна, що *гібридні конфлікти мають сталу здатність перетворювати географічно локальні та регіональні конфлікти в інформаційно-глобальні. Недооцінка саме цих їх властивостей може призвести до страшних за своїми наслідками стратегічних помилок. Приклад – анексія Криму. Нині, на п'ятому році війни в контексті мілітаризації півострова достатньо згадати розташування там комплексів С-400 та Іскандер, які можуть нести ядерну зброю. У контексті тих дипломатичних, економічних, військових та інформаційних зусиль, до яких змушена вдаватися дедалі більша кількість держав, стає очевидним, що окупація Криму створила ризики перетворення Чорноморського басейну на зону військового протистояння, отже це вийшло далеко за межі регіональної проблематики.*

Ще один важливий аспект, на який вказав В. Горбулін, полягає в тому, що *окремі прояви поведінки Російської Федерації у форматі гібридних загроз були помітні ще на початку 2000-х. Територіальні зазіхання навколо острова Тузла, відключення газу 1 січня 2006 року, торгівельні обмеження (під час президентства Ющенка їх було близько 40), – все це події одного порядку та однієї логіки гібридного протистояння. Приблизно тоді ж, у 2006 році, відбулась ще одна подія, яка заслуговує на увагу. Раптово в Росії з'явилась велика кількість нових талановитих літераторів, які ніколи не були на війні, але твори яких описували усі складові майбутньої російсько-української війни. Саме ці автори дали символічний старт інформаційно-смисловій війні проти України, яка завершилась очікуваною воєнною компонентою*.

На тлі згадок В. Горбуліна про те, що прояви гібридної війни були помітні задовго до 2014 року й коментарів О. Литвиненка щодо Мюнхенської конференції 2007 року, варто також звернути увагу на те, ***чи вивчила Україна уроки Грузії 2008 року, і як Україна нейтралізує підривні кампанії Росії***.

У цьому контексті слід звернути увагу на слова Лаші Дарсалії. Як і більшість дослідників теми гібридних загроз, він погоджується, що *інструменти, які використовує Росія, не нові, вони використовувалися раніше і були добре розвиненими ще до того, як взагалі з'явилась концепція «гібридної» війни. Інструментарій, який використовує Росія, служить для задоволення її стратегічних інтересів і*

цілей на пострадянському просторі, а основною метою є втримати цей простір принаймні під своїм впливом, якщо не під прямим контролем.

Л. Дарсалія вказав на те, що основою *політики Росії стосовно своїх сусідів є ревізіонізм та реваншизм. Також він погодився з О. Зеркаль у тому, що Росія – це держава, що піддає сумніву загальноприйняті міжнародні норми. Перші сигнали щодо цього мали місце у 2005-2006 роках, коли В. Путін заявив, що розпад Радянського Союзу був геополітичною помилкою, геополітичною трагедією.*[20]

На думку Л. Дарсалії, примітно, що *важливим компонентом російської гібридної агресії є антилібералізм чи путінський консерватизм. Росія послуговується сумішшю православних та консервативних підходів, комуністичних підходів та більшовицьких ідей, уявлень про те, яким чином мав би бути організований світ*. Екстраполюючи грузинський досвід на регіон в цілому, Л. Дарсалія наголосив, що *на пострадянському просторі Росія передусім захищає так звані ексклюзивні сфери впливу. Для цього навіть використовується спеціальний термін, що також має психологічне навантаження – «ближнє зарубіжжя». На цьому просторі, з точки зору Росії, має бути заборонено розширення НАТО та вступ до нього пострадянських держав.*

На думку Л. Дарсалії, *у Грузії Росія переслідує такі інтереси: по-перше, запобігти західному впливу, тобто демократизації країн Південного Кавказу, що сприймається Росією як загроза. По-друге, обмежити стратегічний вплив Сполучених Штатів та Європейського Союзу (такий підхід ґрунтується на концепції ексклюзивних зон впливу). І, по-третє, контролювати енергетичні коридори.*

При цьому Л. Дарсалія наголосив, що *є підстави вважати, що «гібридні» концепції та інструменти використовуються проти Грузії протягом останніх 25-30 років. Це відбувалося не лише у 2008 році і після цього. Лише один приклад – ще у 1992-1993 роках, коли, як багато-хто вважав, у Грузії спалахнув етнічний конфлікт, насправді, відбувалась «гібридна» операція. Вона містила майже всі ті складові, які ми спостерігаємо в Україні: військові найманці, напади на цивільне населення, свого роду «зелені чоловічки», «гуманітарні конвої». І все це здійснювалось під керівництвом Сергія Шойгу [зараз Міністра оборони РФ].*

Заслуговує на увагу також теза про те, що, *перш за все, Росія не хоче встановити у Грузії проросійський уряд. Головна мета Росії – мати слабкий уряд Грузії, тобто дестабілізувати грузинські інституції. Друга важлива мета – демонізація Заходу і західних цінностей за допомогою різних способів і підходів (наприклад, з використанням консервативних угрупувань).*

Один із основних інтересів (і це також важливо в контексті України) – представити Грузію Заходу як ненадійного партнера. Це теж складова «гібридної» війни. Згадка про цей аспект

20 Владимир Путин: "Распад СССР - крупнейшая геополитическая катастрофа века". *ИА REGNUM.* 25.04.2005. https://regnum.ru/news/444083.html

«гібридної» війни важлива з огляду на те, що, як справедливо зауважує військовий дослідник Б. Фрідман, Росія в таких ситуаціях позиціонує себе як той, хто може запропонувати вирішення проблеми, при цьому, намагаючись замовчати той факт, що сама Росія її і спричинила.[21]

Насамкінець, якщо всі ці інструменти виявляються недостатньо ефективними і не досягають дестабілізації, Росія може використовувати окуповані території та конфлікти всередині грузинського суспільства. Як зазначали українські спікери, аналогічний підхід реалізується сьогодні і в Україні.

У свою чергу, В. Горбулін додав, *що ключовим моментом у розгортанні російської гібридної агресії став саме 2008 рік. Тодішня російсько-грузинська війна та відверто квола реакція на неї міжнародної спільноти стала своєрідним вододілом між миром та війною. Вододілом спочатку у регіональному, а потім і у світовому масштабі. Події 2014 року в Україні стали можливими значною мірою саме тому, що у 2008 році міжнародна реакція більше нагадувала події у Мюнхені 1938 року, ніж події у Потсдамі 1945 року.*

Водночас, В. Горбулін критично зауважив, що *гібридна війна перевернула все, що раніше робилось в гуманітарному та інформаційному просторі. Ніколи ще ЗМІ Росії не були настільки інфіковані своєрідним «вірусом сказу». Агресія в інформаційному просторі та конфліктогенність – це той продукт, який Росія активно намагається експортувати не лише до України, але й до Європи і Сполучених Штатів. Для посилення ефекту поширення і підтримки руйнівних наративів, спрямованих проти України та демократичних держав, Росія активно користується перевагами Інтернету, застосовуючи масові атаки у соцмережах (згадаємо Ольгинську фабрику тролів). В Україні для сіяння розбрату і ненависті також використовується вкрай чутлива релігійна тематика.*

Серед проблем, які є похідними від такої діяльності Росії, є той факт, що населення здебільшого не бачить в ній для себе загрози. Відтак непомітно відбувається повернення до війни ідей та смислів, що було притаманно «холодній війні», а в інформаційній та смисловій сфері Україна часто поступається Російській Федерації.

Разом з тим, хоча кожен елемент інформаційної війни, по суті, не новий і використовувався майже у всіх війнах минулого, ситуація стає унікальною через узгодженість і взаємозв'язок цих елементів, динамічність та гнучкість їх застосування. Росія постійно удосконалює свої можливості у цій сфері. Наприклад, нещодавно Кремль підняв питання про необхідність створення Генерального штабу інформаційної безпеки.

Серед основних наративів російської пропаганди проти НАТО є те, що Альянс не захистить навіть країни-члени у разі нападу з боку Росії, не кажучи вже про партнерів, а також, що це саме сили НАТО можуть атакувати

21 B. Friedman, "Fellow travelers: managing savagery and the Gerasimov Doctrine". *The Bridge*. 27.04.2017. https://weaponizednarrative.asu.edu/system/files/library/docs/fellow_travelers.pdf

Росію з території країн-членів, зокрема, і без згоди національних урядів. Відповідно військові бази в країнах Східної Європи та Балтії є прямою провокацією проти Росії, а не захистом від її агресивної політики.

Все це вписується у схеми протиборства, які так полюбляють основні ідеологи та ініціатори гібридної війни, якими В. Горбулін вважає В. Путіна та В. Суркова. І основним питанням на цьому тлі є те, ***які чинники можуть мінімізувати шкоду, заподіяну гібридними атаками?***

Відповідь на це питання спробував дати, насамперед, О. Литвиненко. Він наголосив, що *гібридна війна працює проти розділених суспільств зі слабкими інституціями. У період внутрішньої кризи такі засоби можуть бути дуже ефективними. Протиставити гібридним засобам можна стійкість суспільства, його волю до боротьби за свободу і незалежність, готовність до спротиву, високий рівень взаємної довіри між членами суспільства і до власних інституцій, ефективний сектор безпеки і оборони. Найсуттєвіше значення мають здорове громадянське суспільство і відповідальні медіа.*

О. Зеркаль додала, що, *усвідомлюючи всю обмеженість міжнародного права, необхідно убезпечити себе, використовуючи всі наявні правові інструменти, зокрема такі як: Міжнародна конвенція про заборону фінансування тероризму, Міжнародна конвенція про ліквідацію всіх форм расової дискримінації, Міжнародний суд ООН. Попри те, що судові процеси тривають дуже довго, вони приносять результати. Росія ніколи не сподівалася, що українські інвестори, які втратили власність і свої активи в Криму, зможуть захистити себе з використанням такого інструменту як двостороння Угода про захист інвестицій, але це сталося. І вже є перше рішення [Арбітражний суд у Парижі 26 листопада 2018 року ухвалив рішення задовольнити вимогу про компенсацію збитків "Ощадбанку", завданих унаслідок анексії Росією Криму, на суму 1,3 млрд дол. США плюс відсотки].*[22]

> Застосування гібридних засобів впливу може виступати як підготовчий етап – прелюдія до широкомасштабного застосування військової сили, супроводжувати таке застосування, або, у випадку досягнення політичних цілей, заміняти війну в її традиційному розумінні

Що ж стосується більш широкого контексту і того, чого очікувати далі, якими є подальші цілі Кремля, то тут слушним є твердження О. Литвиненка, що *глибоко зневажаючи демократію і лібералізм як засади цивілізованого*

22 "ОЩАДБАНК" виграв у РФ у міжнародному суді $1,3 млрд компенсації збитків через анексію Криму. 5 канал. 26.11.2018. https://www.5.ua/ekonomika/oshchadbank-vyhrav-u-rf-u-mizhnarodnomu-sudi-13-mlrd-kompensatsii-zbytkiv-cherez-aneksiiu-krymu-181912.html

світу, Кремль усіляко прагне використати їхні особливості для підриву демократичних політичних режимів в Європі і світі. Йдеться, передусім, про втручання у передвиборчі кампанії, беззастережні маніпуляції, інформаційні, психологічні й інші війни.

Особливу увагу треба звернути на традиційні зв'язки Кремля з криміналітетом та на застосування кримінальних методів загалом. Російська мафія не може розглядатися у відриві від новітньої російської держави.

> Росія занурює жертву у хаос, щоб запропонувати вигідне Москві вирішення проблеми

Застосування гібридних засобів впливу може виступати як підготовчий етап – прелюдія до широкомасштабного застосування військової сили, супроводжувати таке застосування, або, у випадку досягнення політичних цілей, заміняти війну в її традиційному розумінні. Як зазначила Г. Шелест: «Фактично гібридні дії можуть бути, як самостійною операцією, де військова сила є лише додатковим важелем для підсилення політичного впливу, так і слугувати в якості першого, підготовчого етапу перед повноцінним та повномасштабним застосуванням військової сили».[23]

Мета гібридних засобів – послабити волю і можливості суспільства-жертви до спротиву, підірвати його здатність до опору й сприяти успішності наступного етапу – військової кампанії. Якщо гібридні методи не досягають бажаних результатів, то можлива ескалація з використанням класичних засобів. Показовими є приклади Сирії і Сходу України. Перехідним етапом до встановлення контролю може виступати повна дестабілізація і занурення жертви у хаос аж до тієї стадії, коли окупація виглядатиме для деяких чи навіть багатьох, як цілком прийнятна ціна за звільнення від безладу і встановлення порядку. У даному випадку, тези О. Литвиненка знову перегукуються з тезами Б. Фрідмана – Росія занурює жертву у хаос, щоб запропонувати вигідне Москві вирішення проблеми.

На думку В. Горбуліна, *немає цілковитої впевненості в тому, що коли нинішня кремлівська влада піде, то боротьба Росії з Україною не продовжиться в усіх її гібридних проявах. Цілі Росії: знищення Української держави та її державності і повернення Росії глобального політичного лідерства у світі. Перша ціль – проміжна, друга – стратегічна. Однак досягти другої без першої – неможливо. Саме тому В. Горбулін вважає, що за умови збереження російської реваншистської політики, Російська Федерація залишатиметься не тільки агресором для України, а й головним детонатором безпекового середовища, випробуванням*

23 Г. Шелест, "Гібридна війна". *Оцінки стратегічного середовища*. Військово-Морські Сили Збройних Сил України. 2018. стор. 41.

на міцність для союзів і альянсів, тестом для НАТО та 5 статті Вашингтонського договору.

Одним з інструментів запобігання найбільш негативним сценаріям можна вважати згаданий Джил Сінклер, стратегічним радником високого рівня Консультативної ради з питань оборонної реформи, *механізм швидкого реагування країн Групи 7 [Великої сімки], який сформує структуру забезпечення солідарності, розподілу інформації та спільну роботу із протистояння загрозам. Роботу над його запуском було розпочато за рішенням саміту в Канаді у 2018 році.* Дж. Сінклер також погодилась з тим, що суспільство має бути більш стійким до зовнішніх впливів та маніпуляцій, і це має стати загальноприйнятим підходом.

Разом з тим, слід розглянути можливість започаткування в Україні механізмів протидії гібридним атакам. На думку В. Горбуліна, такі механізми та координуючі структури мали б спиратися, передусім, на апарат Ради національної безпеки і оборони, і працювати у тісній взаємодії з відповідними структурами НАТО, Групи 7 тощо. Поза тим, першочерговим завданням для України є реформування сектору безпеки та оборони, включаючи реформування прокуратури, Міністерства внутрішніх справ, Служби безпеки України та розвідки.

Слід також врахувати досвід і максимально підвищити стійкість державних інституцій, а також стійкість суспільства і його поінформованість щодо загроз, з якими стикається держава.

ТРАНСАТЛАНТИЧНЕ СПІВРОБІТНИЦТВО: КОНСОЛІДОВАНА ВІДПОВІДЬ НА СПІЛЬНІ ЗАГРОЗИ

Російська агресія проти України запустила процес руйнування системи європейської та трансатлантичної безпеки. Гібридні дії Кремля проти України та інших регіональних держав підривають стабільність у просторі від Балтії до Чорного моря, створюють серйозний виклик миру та безпеці в регіоні. За словами Анатолія Петренка, заступника Міністра оборони України з питань європейської інтеграції, *аналіз поточної ситуації свідчить, що військова складова гібридної війни, аж ніяк не зменшується. Крим перетворюється не лише на велику військову базу Росії, але й на центр для поширення впливу РФ далеко за межами Чорного моря.*

Водночас наслідки подібної деструктивної поведінки мають більш широке значення: методи та стратегії Кремля активно переймають інші авторитарні режими. Фактично, у су-

часному світі формується новий вид глобального протистояння – світова гібридна війна, що ведеться у межах єдиного глобалізованого простору на фронтах, утворених лініями розподілу між зонами стабільності і безпеки, між раціональним порядком, де вагу має закон і міжнародне право, та сферою ірраціонального, соціально-політичного хаосу, де панують емоції і домінує право сильного. Результат цієї війни матиме екзистенційне значення для світу.

> Поки НАТО збирається захищати «будинок», Росія працює з його мешканцями. Гібридні загрози спрямовані на персональне сприйняття кожного, викривлення цього сприйняття та заохочення заангажованості

Одне із найважливіших питань останнього десятиріччя – ***як перейти від реактивних до проактивних підходів у протидії спільним загрозам?*** Перехід можливий лише після усвідомлення та уніфікації природи спільних гібридних загроз. На жаль, наразі вони неоднаково сприймаються різними акторами міжнародної системи.

Гібридна війна Москви, яку та веде проти Західного світу, це унікальний феномен через неспроможність ліберально налаштованих політиків зрозуміти її справжні цілі, а відтак знайти адекватну стратегію реагування. Причому вплив реалізовується таргетовано до тих країн та суспільств, які Москва хоче ситуативно використати або «розхитати». Треті країни, за таких умов, здебільшого не відчувають прямої загрози або прямого впливу, а відтак є індиферентними або нейтральними до них.

Більшість європейських країн дуже вузько розуміють гібридні виклики як такі. Вони вкладають їх у парадигму найбільш поширених дій Москви: в інформаційній площині (пропаганда), у кіберпросторі (кібератаки, які в майбутньому можуть стати предметом застосування статті 5 Вашингтонського договору НАТО) та в економіці (Північний потік-2). На думку багатьох експертів, на цьому вичерпний перелік російських загроз закінчується, а сама природа гібридних загроз класифікується як така, що хоче «зруйнувати, підпалити спільний дім».

На думку колишнього голови Військового комітету НАТО Кнуда Бартелса, *найбільша загроза йде не зі Сходу чи Південного Сходу, вона може прийти від нас самих, від нашої неспроможності порозумітися щодо цілої низки питань. Гібридна війна використовує усі виміри державної влади, щоб нав'язати свою волю іншій державі, натискаючи на найслабші точки розвитку й досягаючи результатів. Фактично, цей тип війни передбачає, що першою лінією оборони стає саме суспільство.*

Під час конференції «Уроки гібридного десятиліття» заступник Генерального секретаря НАТО Антоніо Міссіролі наголосив *на необхідності побудови стратегії*

стійкості (resilience) для держав-членів НАТО, що допоможе зробити «спільний дім» вогнетривким. Проблема лише в тому, що Москва давно не переймається конструкцією «спільного дому» європейців, її не цікавлять «стіни», «вікна» й «дах». Поки НАТО збирається захищати «будинок», Росія працює з його мешканцями. Гібридні загрози спрямовані на персональне сприйняття кожного, викривлення цього сприйняття та заохочення заангажованості.

Особливий акцент Кремль робить на молоді – через операції психологічного впливу, непрямі дії, соціальні медіа (пропаганда вже не обмежується Facebook і йде в Instagram). Піддаються впливам й люди старшого віку, оскільки російські меседжі «заходять» через традиційні цінності, мораль і етику, церкву (в тих країнах, де це можливо), проплачених експертів громадської думки, мозкові центри й авторитетні ЗМІ. І може статися, що одного чудового ранку хтось рішуче «підпалить будинок» зсередини. Москва виробляє та експортує достатньо «сірників», намагаючись посіяти розбрат, розділити ЄС та НАТО, культивуючи нетолерантність, ненависть, ворожість, національний егоїзм, «змащуючи» все це відчуттям страху, використовуючи риторику «підвищення ставок» і ядерного залякування. Крім того, за словами Мікко Кіннунена, посла з питань гібридних загроз МЗС Фінляндії, *цілями гібридної агресії є посягання на верховенство права, свободу слова, а також демократичні вибори, легітимність яких поставлена під питання. Проблемами також є викривлення реальності у ставленні до мігрантів, формування відрази до іноземців шляхом поширення фейків*.

Гібридна війна викривлює суспільні уявлення про значення подій, створює суперечливі версії того, що відбувається. Конфлікт інтерпретацій має потужну руйнівну силу, якій слід навчитися протистояти. Для цього необхідно зрозуміти загальні механізми створення та впровадження гібридних впливів. Гібридна війна – це також апелювання до низинних, первісних почуттів та емоцій людей. Гнів, страх, відторгнення чужого, агресивність. Москва використовує найгірші людські почуття, збуджує їх та виводить на такий рівень, аби вони витіснили кращі – толерантність, милосердя, доброзичливість.

Українські й іноземні експерти на конференції відзначали симптоматику гібридних загроз, але залишили без відповіді головне запитання: як можна уможливити проактивні дії. Так, усі погоджуються з необхідністю демотивації агресора задля його стримування. Кнуд Бартелс зауважив, що *гібридна війна має стати занадто дорогою для росіян. В цьому полягає сенс запровадження санкцій та обмежень*. Але гібридна війна на те й гібридна, що її дії переважно непрямі й не мають руйнівних наслідків для миру чи економічного добробуту тут і зараз. Як можна демотивувати агресора не робити те, чого він «не робить»?

Росія продовжує «піднімати ставки» на Донбасі, зокрема на Азовському морі, яке раніше було символом миру і дружби між державами. Для Росії Україна стає повноцінним полігоном для відпрацювання технологій

непрямого впливу, застосування яких важко довести. «Іхтамнєт», шантаж, блеф, контроль над людьми, а не територіями – ось простий набір інструментів Москви, який активізується напередодні виборів 2019 року в Україні. Але дестабілізація України не є самоціллю для Кремля. За словами народного депутата України Ірини Фріз, *мета діяльності українських депутатів на міжнародних майданчиках полягає в донесенні значення російської загрози для всього цивілізованого світу й застереження, що наступними цілями гібридної агресії Росії стануть країни ЄС.*

Щоб проактивно реагувати на гібридну війну Росії, трансатлантичній спільноті потрібно навчитися передбачати неочевидні наслідки, створити систему змістовних індикаторів, що попереджатимуть про наявність проблеми, щось на кшталт системи раннього попередження. Як зазначив К. Бартелс, *треба навчатись стримуванню, необхідними є відповідні військові можливості*. Серед ефективних інструментів мінімізації агресивної спроможності Росії – економічні санкції, зменшення залежності ЄС від РФ (передусім в енергетичній сфері), а також дипломатична взаємодія.

Проактивні заходи – це профілактика та попередження ризиків. Саме з цією метою був створений у Фінляндії Європейський центр протидії гібридним загрозам, що функціонує під егідою ЄС та НАТО. Це приклад синергії та активної дії на захисті інтересів Західного світу. Разом з тим, на думку заступника Міністра закордонних справ Литовської Республіки Дарюса Скусявічуса, *треба посилювати межі стримування гібридної війни. Необхідні нові проекти в рамках діяльності команди швидкої кібервідповіді, спільної відповіді на втручання у виборчі процеси*.

Проте, говорячи про інструменти гібридної війни, європейці часто тактовно уникають необхідності називати джерело небезпеки – агресивну поведінку Росії, ототожнювати її дії з агресією. Понад те, часто лунають думки про певну «втому Європи від України». Зазначене варто розуміти, в першу чергу, як втому від очікувань, повільних реформ в Україні, а також як втому деяких від впливу антиросійських санкцій на економіки тих країн, що їх впроваджують. Перевантаженість європейських країн власними кризами (Брекзіт, мігранти, праві популісти) призводить до бажання звести агресивну політику Росії до суто проблеми україно-російських відносин.

За сучасних темпів розвитку «національного егоїзму», неможливості дійти консенсусу для рішучих кроків у відповідь, через різну оцінку й аналіз ризиків, під загрозою опиняється саме існування такої організації колективної безпеки як НАТО. Рада Безпеки ООН вже перетворилась на майданчик «глибокого занепокоєння», а платформу ОБСЄ намагаються використовувати як інструмент для маніпулятивного викривлення фактів. Москва рухає «червоні лінії», і саме ЄС та НАТО повинні зупинити подібні дії Кремля. Лише після цього можна буде говорити про ефективні проактивні заходи на національному рівні.

Останні декілька років постає також питання, чи потрібне нам трансатлантичне співробітництво з питань протидії гібридним загрозам, чи можна лише обмежитись європейською співпрацею?

Оскільки феномен світової гібридної війни не знає кордонів, реагувати на нього треба акцентованими глобальними діями. Західний світ – це не лише Європа та Північна Америка, але й Австралія, Японія, Південна Корея та інші держави світу, що розділяють демократичні цінності. Але особлива роль все ж історично покладена на США як неформального багаторічного лідера західного ліберального світу. За словами Посла М. Кіннунена, *після Другої світової війни в Європі зберігається значна присутність США, але якщо ситуація зміниться – це становитиме загрозу*. Стратегія національної безпеки США, опублікована наприкінці 2017 року, визначає Росію супротивником США.[24] Однак це не означає, що Вашингтон буде будувати «стіну» та автоматично солідаризуватись з Україною.

Якщо для України Росія вже давно стала головним подразником та ворогом, то США готові «в'язати» супротивника переговорами та діалогом. Безапеляційна конфронтація часів холодної війни, з точки зору Вашингтону, веде в нікуди, загрожуючи світу ядерною війною. Тому сьогодні єдиний потужний союзник України буде до останнього намагатись знайти компроміс, уникнути ескалації. Подібна поведінка – не замирення агресора та не подвійна гра наших партнерів, а здоровий глузд. Тому Києву варто якнайшвидше легалізувати залучення Вашингтону до переговорного процесу з врегулювання конфлікту на Донбасі (зараз США залучені лише у форматі зустрічей К. Волкера з В. Сурковим) та у питання деокупації Криму.

> Щоб проактивно реагувати на гібридну війну Росії, трансатлантичній спільноті потрібно навчитися передбачати неочевидні наслідки, створити систему змістовних індикаторів, що попереджатимуть про наявність проблеми, щось на кшталт системи раннього попередження

Потенціал для цього достатній. США дедалі глибше розуміють природу та масштаб загрози від Росії. Як показав досвід виборчих кампаній в США у 2016 та 2018 роках, проблема втручання не обмежується континентами. Потрібен не лише трансатлантичний, але й глобальний підхід до вирішення проблеми. Але передусім трансатлантичний, оскільки головна

24 A New National Security Strategy for a New Era. The White House. 18.12.2017. https://www.whitehouse.gov/articles/new-national-security-strategy-new-era/

мета гібридної війни Росії полягає в критичному послабленні Заходу та його цінностей. НАТО має реагувати відповідно.

Кнуд Бартелс з цього приводу зауважив, що *перебудова структури військового командування НАТО почалась після саміту в Уельсі в 2014 році. У 2018 році було відновлено Другий флот США в Північній Атлантиці, зона відповідальності якого охоплює Балтійське море. Це пряма реакція Вашингтону на загрозу ескалації в регіоні. Так само, як й реалістичні дії президента США Д. Трампа – вимога підвищення витрат на оборону європейських країн*.

Проте К. Бартелс скептично ставиться до спроможності ефективно використати НАТО у протидії гібридним викликам. Передусім через *найбільшу загрозу Заходу – неспроможність зібратись разом і не ховати обличчя*.

Гібридна війна стосується повсякденного життя мільйонів людей через феномен «патерналістів», що стимулює прихід до влади красномовних популістів та представників антисистемних рухів. На думку деяких експертів, деструктив переважає над конструктивом, ірраціоналізм – над раціональною поведінкою.

Вразливість західних демократій полягає у відірваності базових ліберальних цінностей від реалістичної політики. Ціннісне бачення світу, властиве постбіполярній добі, поступається перед агресивним поверненням *Realpolitik* під тиском викликів і загроз, кількість та масштаб яких є безпрецедентним. Теперішнє покоління лідерів західного світу, виховане в традиціях лібералізму та гуманізму, не завжди може адекватно реагувати та відповідати на сучасні виклики, внаслідок чого шанс на владу отримують популісти, марксисти та націоналісти, діяльність яких не обмежена ціннісними орієнтирами ліберального світу. На останніх і робить ставку Кремль.

Протистояти цій силі поодинці не вийде – треба об'єднувати зусилля. Як зауважив Д. Скусявічус: *трансатлантична спільнота – ідеальна структура для спільної взаємодії*.

Гібридна війна неможлива без військового компоненту, тому постає питання чи готові армії НАТО та України протидіяти та бути стійкими до такого типу загроз?

Гібридна війна неможлива без військової компоненти. Хоча стійкість, яку випробовують на міцність інструментарієм гібридної агресії, значно частіше стосується суспільства, економіки або політикумів, аніж безпосередньо армії та правоохоронних структур.

Очевидно, що армії країн НАТО не повністю сьогодні готові до відбиття гібридної війни. Проблема не лише у військових доктринах, але, передусім, в політиках та політичних рішеннях. Продовжуються дискусії всередині Альянсу щодо того, що є достатньою формою агресії для застосування статті 5 Вашингтонського Договору? Чи реально отримати консенсусне рішення стосовно неочевидного факту нападу (кібератаки або використання «зелених чоловічків»)?

Російська агресія виявила слабкі місця в системі оборони Альянсу на сході Європи, позначила рівень вразливості на його південно-східному фланзі. Анексія Криму і подальша підвищена військова активність РФ в акваторії Чорного моря створила додаткові безпекові загрози для країн-членів і країн-партнерів НАТО, сформувавши плацдарм для поширення впливу Росії у напрямку Середземномор'я і Близького Сходу. Особливі побоювання пов'язані з країнами Балтії, що мають у своєму складі російські меншини, до яких Москвою може бути застосовано «право на захист співвітчизників».

Власне й самі армії країн-членів Альянсу знаходяться на різному рівні підготовки. Східний фланг значно більш спроможний, аніж південний, й необхідно долати існуючий дисбаланс. Але для цього потрібне розуміння стратегічного концепту із врахуванням когнітивної безпеки. Як зазначив М. Кіннунен, *аби зрозуміти один одного, свої потреби, взаємний зв'язок – країнам-членам треба посилити взаємодію, зокрема, в рамках гібридної платформи.*

Перед подібними викликами постають й Збройні сили України. Як підкреслив А. Петренко: *«Стійкість армії до невійськових загроз є однією з вимог оборонної реформи, що зараз впроваджується в нашій державі».* Для захисту держави потрібне поєднання цивільного та військового потенціалу. Окрім цього, на думку заступника Міністра, зважаючи на отриманий військовий досвід, Україна має різко нарощувати потенціал ВМС, приймати на озброєння ракетні комплекси, розбудовувати інфраструктуру на лівобережній та південній Україні, оскільки з радянських часів вона була здебільш зосереджена на «зовнішньому» західному кордоні.

За словами А. Петренка, *Україну до форсованого розвитку оборонного потенціалу спонукає наявність 29-ти батальйонно-тактичних груп Збройних сил Російської Федерації, розташованих уздовж спільного кордону та готових до наступу. Натомість, мілітаризований Крим є центром впливу РФ далеко за межами регіону, а агресія на Азові – інструментом тиску*.

> Стійкість армії до невійськових загроз є однією з вимог оборонної реформи, що зараз впроваджується в нашій державі

Вагомим викликом для України, що відзначає А. Петренко, є *цикл оборонного стратегічного планування – від Стратегії національної безпеки до Комплексного огляду сектору безпеки та оборони. Піраміда стратегій, що прописана ухваленим в червні 2018 року Законом «Про національну безпеку», вибудовується на американський манер і прив'язана до президентських виборів. Протягом 6 місяців після обрання новий президент має представити свою Стратегію національної безпеки, на основі якої формуються всі*

інші документи стратегічного планування. Діалог в рамках взаємодії України з НАТО має практичну цінність, адже, де-факто, Україна є країною східного флангу Альянсу, що відбиває військову агресію.

Внаслідок політики останніх років, коли панувала думка щодо відсутності загрози великої війни, зменшилася спроможність країн-членів НАТО вести повномасштабну конвенційну війну з високою інтенсивністю бойових дій. Йдеться не тільки про зменшення військового потенціалу та навичок ведення відповідних бойових дій військовими, але також про брак усвідомлення повного спектру наслідків такої війни з боку громадськості і політичних еліт країн НАТО.

Водночас, у НАТО дійшли висновку, що дії Москви потребують багатовимірних відповідей[25] – і в царині міжнародного права, і на оперативно-тактичному рівні, і в площині пошуку нових концептуальних підходів для підтримки трансатлантичної безпеки. Відбувається формування нових засад діяльності НАТО, спрямованих на активне стримування агресивної політики Кремля. Усвідомлення необхідності розробки комплексу заходів для стримування агресора є життєво важливим для того, щоб не допустити реалізації сценарію повномасштабної війни у Європі. Відколи Росія здійснила незаконну анексію Криму у 2014 році, а на південному фланзі з'явились нові виклики безпеці, зокрема, безжальні напади з боку ІДІЛ й інших терористичних угруповань на кількох континентах, НАТО ініціювало найбільш масштабне зміцнення колективної оборони з часу завершення «холодної» війни. Наприклад, було втричі збільшено чисельність Сил реагування НАТО, створено сили надзвичайно швидкого реагування, так звані підрозділи «Вістря списа» у складі 5 000 військовослужбовців, а також здійснено розгортання багатонаціональних бойових груп на території Естонії, Латвії, Литви і Польщі. До того ж НАТО нарощує присутність на південно-східному фланзі Альянсу, центральним елементом якої є багатонаціональна бригада, що базується в Румунії. Альянс також активніше запроваджує місії патрулювання повітряного простору над Балтійським і Чорним морями. Триває розбудова військового потенціалу «першої лінії», зокрема, спільної системи спостереження, розвідки і рекогносцировки. На Варшавському саміті у липні 2016 року держави-члени НАТО визнали кіберпростір новою зоною оперативних дій та зобов'язались вжити заходів задля вдосконалення захисту мереж, місій і операцій.

НАТО, як ключовий елемент європейської та євроатлантичної безпеки, адаптується до змін у безпековому середовищі, модифікує ключові підходи своєї діяльності, особливо щодо стримування Москви. Якщо донедавна Альянс більше зосереджував свою діяльність за межами Європи, то через зростання російської військової загрози, зона ризиків знову зміщу-

25 "A 'comprehensive approach' to crises". North Atlantic Treaty Organization. 26.06.2018. https://www.nato.int/cps/ie/natohq/topics_51633.htm

ється до європейського континенту. Ключова країна Альянсу, США, змушені знову повернути зовнішньополітичну увагу до Європи і відновити свою традиційну роль гаранта європейської безпеки.

Європейський Союз також одночасно посилює власну безпекову складову та розвиває співробітництво з НАТО. 2016 став роком перегляду партнерства ЄС з НАТО. Під час саміту НАТО у Варшаві високопосадовці двох організацій підписали Спільну декларацію із закликом "надати новий імпульс і нову сутність стратегічному партнерству між НАТО і ЄС".[26] Варшавська декларація НАТО-ЄС 2016 року визначила сім пріоритетних сфер співробітництва (гібридні загрози, оперативне співробітництво, кібербезпека, оборонні спроможності, оборонна промисловість та дослідження, координація навчань, розбудова можливостей у сфері оборони та безпеки) та два блоки реалізації заходів. Перший блок із 42 заходів був опублікований в грудні 2016 року, а другий блок із 32 заходів – через рік.[27]

Протидія гібридним загрозам є одним з основних пріоритетів порядку денного співробітництва ЄС-НАТО. Обидві організації вже встановили міжінституційні контакти, спрямовані на вивчення гібридних загроз та обмін відповідною інформацією, наприклад, співробітництво між секцією гібридного синтезу ЄС, відділенням гібридного аналізу НАТО (EU Hybrid Fusion Cell, NATO Hybrid Analysis Branch) та центрами передового досвіду НАТО в країнах Балтії. Цю співпрацю було згодом інституціалізовано через заснування у Гельсінкі в 2017 році Європейського центру передового досвіду з протидії гібридним загрозам. Цей випадок цікавий тим, що дана організація не є структурою ЄС чи НАТО, а була заснована та фінансується країнами-учасницями двох організацій.[28]

Зі свого боку, Альянс готується до оборони у разі потенційного військового або гібридного нападу РФ на країни Балтійського регіону. Саме в рамках стратегічного концепту стримування і оборони з'явилася програма посилення передової присутності Альянсу на східному та південному напрямках. Чотири багатонаціональні батальйони, які були розгорнуті в Литві, Латвії, Естонії та Польщі під керівництвом Великої Британії, США, Канади та Німеччини, демонструють трансатлантичну єдність та утверджують принцип колективної оборони.

Поступово зростає усвідомлення, що поряд з викликами і загрозами для країн Балтії та Північної Європи, різко зросли і продовжують зростати ризи-

26 Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organisation. EU official website. 08.07.2016. https://www.consilium.europa.eu/media/21481/nato-eu-declaration-8-july-en-final.pdf

27 М. Миронова. "Співробітництво ЄС-НАТО: перспективи автономнішої Європи?". *UA: Ukraine Analytica*, Issue 4 (14), 2018 http://ukraine-analytica.org/the-eu-nato-cooperation-perspectives-for-more-autonomous-europe/

28 М. Миронова. "Співробітництво ЄС-НАТО: перспективи автономнішої Європи?". *UA: Ukraine Analytica*, Issue 4 (14), 2018. http://ukraine-analytica.org/the-eu-nato-cooperation-perspectives-for-more-autonomous-europe/

ки для Чорноморського регіону. Якщо донедавна можна було говорити про Чорне море як переважно внутрішній простір НАТО, включений у зону його відповідальності, то сьогодні парадигма сприйняття змінюється, аби не допустити перетворення Чорного моря на «Російське внутрішнє море».

> Мета Росії – гранично послабити міжнародну взаємодію, дозволити національному егоїзму та суверенітету восторжествувати над багатостороннім інституціональним співробітництвом

Актуальні стратегічні пріоритети НАТО – це стримування й оборона,[29] а також поширення стабільності та зміцнення безпеки за межами Альянсу, що передбачає підвищення значення відносин НАТО з країнами-партнерами на східному та південному флангах. Альянс продовжує реалізовувати програму заходів, спрямованих на допомогу цим країнам у розбудові міцніших оборонних інститутів та підготовці власних спроможних збройних сил.

Міжнародна координація необхідна для ефективного протистояння гібридним загрозам. Саме тому, мета Росії – гранично послабити міжнародну взаємодію, дозволити національному егоїзму та суверенітету восторжествувати над багатостороннім інституціональним співробітництвом. Поодинці країни ЄС та НАТО слабкі, разом – міцніші.

Разом з тим, як зазначив Посол М. Кіннунен, поєднання *двох рівнів реакції на гібридні впливи – національного та міжнародного, досі залишається серйозним викликом. Для України, яка не є членом НАТО, це питання стоїть ще гостріше.* Прикладом налагодження подібної міжнародної взаємодії є діяльність центрів передового досвіду НАТО. Як відзначив Дарюс Скусявічус, в *Литві діє Центр з питань енергетичної безпеки, у Латвії – стратегічних комунікацій, в Естонії – кібернетичної безпеки, у Фінляндії – Центр протидії гібридним загрозам під егідою ЄС та НАТО.* Але, на думку литовського високопосадовця, треба задіяти й багатосторонні формати в рамках ЄС, наприклад потенціал Східного Партнерства.

Як зауважив Кнуд Бартелс: *Перша лінія оборони – саме суспільство: міцна демократія, ефективне управління, правоохоронні органи (довіра до них) та підзвітність*. В Європі гібридні впливи вже досягли певних результатів, підтвердженням чого є зростання негативного ставлення до мігрантів та іноземців (зокрема, «заробітчан»-українців). Визнаючи наявність проблеми викривлення суспільної свідомості через спекулятивні пропагандистські впливи та фейки, Бартелс все ж

29 Warsaw Summit Communique. North Atlantic Treaty Organization. 09.07.2016. https://www.nato.int/cps/uk/natohq/official_texts_133169.htm?selectedLocale=en

відмічає, що *«зелені чоловічки» пробуджують нас, повертають до реальності. Саме тому ми побачили саме таку [жорстку] реакцію в Каталонії – Іспанія вивчила українські уроки.* Європейські суспільства мають навчитись ефективно протидіяти спробам внутрішньої дестабілізації та попереджати їх. Міжнародна координація має торкнутись питання відповідного навчання журналістів, лідерів думок, державних службовців – вони повинні навчитись розрізняти правду та брехню, фахово розбиратись в ситуації таким чином, аби кордони та мовне середовище не породжували їх упередженість.

Але передусім, Кнуд Бартелс, як колишній голова Військового комітету НАТО, наголосив на потребі координації військових зусиль: *Наступна війна буде іншою, не такою як раніше. Ми не знаємо якою вона буде, але маємо готуватись до неї. Для цього ми проводимо навчання разом з партнерами, не соромимось відпрацьовувати малоймовірні сценарії. Перший день на полі битви буде несподіванкою для всіх. Тож не вивчайте перемоги, вивчайте поразки*.

К. Бартелс бачить *істотні вразливості армій країн ЄС та НАТО, які пов'язані з відсутністю взаємної сумісності озброєння, виробництво якого потребує оптимізації*. Він називає це «домашнім завданням» трансатлантичної спільноти, слушно відмічаючи, що *нам не потрібно багато гелікоптерів різних моделей і виробників, нам потрібна велика кількість пілотів, що зможуть на них вправно літати.*

Традиційно важливою залишається координація дипломатичних зусиль зі стримування гібридних впливів. Посол М. Кіннунен відзначив, що *трагедія в Солсбері об'єднала нас, змусила задуматись, як попередити подібні дії в інших країнах. Дипломатична реакція на інцидент продемонструвала солідарність країн Західного світу. Однак подібна жорсткість, загалом, є нетиповою для європейців*. Це, в свою чергу, створює нові можливості для Росії.

Проводимо навчання разом з партнерами, не соромимось відпрацьовувати малоймовірні сценарії. Перший день на полі битви буде несподіванкою для всіх. Тож не вивчайте перемоги, вивчайте поразки

Ще однією важливою сферою для міжнародної координації зусиль є комплексний аналіз факторів, що підживлюють пропаганду та забезпечують агресору інформаційну перевагу. Як відзначив Д. Скусявічус, *Ми маємо розуміти, до яких сфер апелює пропаганда, конкретні схеми дії інформаційної атаки. Й діяти на випередження – давати власну точку зору, формувати власні наративи.*

Аналіз поточної ситуації на світовій геополітичній арені свідчить про подальше зростання активності Москви в напрямку руйнування вибудованої протягом десятиліть системи безпеки шляхом реалізації спецопера-цій як військового, так і гібридного

(інформаційного, політичного, безпекового) характеру. Ефективно протидіяти зазначеним впливам можливо лише за умови переходу від реактивних до проактивних підходів у протидії гібридним загрозам. Оскільки метою ревізіоністської політики Росії є послаблення Заходу, демократичні країни трансатлантичного регіону мають об'єднатись для формулювання спільної відповіді, що має обов'язково включати військовий компонент. Міжнародна координація у відповідь на гібридні загрози також має стосуватись таких сфер компетенції як економіка, фінанси, суспільство, медіа, кіберпростір, дипломатія тощо.

Гібридна війна в ширшому європейському контексті створює передумови для повномасштабної конвенційної війни. Ризики євроатлантичній безпеці продовжують зростати після 2014 року. Тож точна оцінка гібридних загроз стає життєво важливою для забезпечення мирного майбутнього.

РОЛЬ РОЗВІДУВАЛЬНОЇ СПІЛЬНОТИ У ГІБРИДНІЙ ВІЙНІ

Розвідувальні служби відіграють важливу роль в забезпеченні міжнародної діяльності держав, а також у плануванні та проведенні військових операцій. Намагання отримати якомога більше інформації стосовно потенціалу союзників та противників, а також їх намірів є одним з класичних інструментів держави. Проте, зміни, які відбулися в характері конфліктів на межі XX та XXI століть, вплинули на зміст діяльності розвідувальних служб та арсенал їх дії.

Таємна активність розвідки найкраще відповідає суті гібридної війни, яка не обмежується міжнародними конвенціями та правилами ведення війни, не має початку і кінця. Саме тому необхідне нове бачення ролі розвідки як джерела гібридних загроз і одночасно, як одного з інструментів протидії цим загрозам.

За останні роки в Україні ухвалена низка законодавчих актів та стратегічних документів, спрямованих на реформування розвідувальних органів, серед яких Закон України «Про національну безпеку» та Стратегія національної безпеки та оборони України. Остання, зокрема, передбачає реформу розвідувальних органів, цілями якої є «пріоритетний розвиток розвідувальних спроможностей України, забезпечений на основі узгодженого функціонування розвідувальних органів» (ст.4.4).[30]

30 Указ Президента України Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпекиУкраїни», Parliament of Ukraine. 26.05.2015. https://zakon.rada.gov.ua/laws/show/287/2015

Ухвалена Національна розвідувальна програма на 2016-2020 рік. Крім того, в Річній національній програмі Україна-НАТО на 2018 рік визначені основні середньострокові цілі та завдання на рік.[31] Проте, Закон про розвідку так і не був розглянутий Верховною Радою у 2018 році, як це передбачалося, що уповільнює темпи реформування спецслужб. Ефективність реформ залежить також і від чіткого розуміння завдань, які стоять перед розвідувальною спільнотою в умовах гібридної війни Росії проти України, чому й мало сприяти обговорення під час сесії «Роль розвідувальної спільноти у гібридній війні» конференції «Уроки гібридного десятиліття» 7-8 листопада 2018 у Києві.

Російська розвідувальна стратегія: минуле та сьогодення

Економічно Росія значно поступається провідним державам світу, зокрема, російський ВВП у 10 разів менше ВВП Китаю (за іншими даними – в 14 разів) і трохи більший від ВВП Іспанії. Тож Росія може стати великою, лише послаблюючи своїх противників – США, ЄС, НАТО, Україну. Як нагадав в цьому контексті Ігор Смешко, голова Служби безпеки України в 2003-2005 роках, *довжина рук розвідки завжди обмежується політичною волею вищого керівництва*.

Специфіка розвідувальної тематики створює декілька пасток під час їх публічного обговорення. З одного боку, успішність багатьох російських розвідувальних операцій створює уявлення про надзвичайну важливість цієї сфери в умовах гібридної війни. З іншого боку, закритий характер діяльності розвідувальних органів створює умови для різноманітних маніпуляцій, до яких можуть вдаватися всі сторони, зокрема (чи в першу чергу), самі спецслужби, щоб надати своїй діяльності більшої ваги, і відповідно отримати доступ до ресурсів.

> Необхідне нове бачення ролі розвідки як джерела гібридних загроз і одночасно, як одного з інструментів протидії цим загрозам

На думку Марка Лайла Гранта, постійного представника Великої Британії в ООН (2009-2015) та радника Прем'єр-міністра Великої Британії з питань національної безпеки (2015-2017), *російська розвідка не має власної стратегії діяльності, натомість вона втілює в життя стратегію президента Росії Владіміра Путіна... У Росії недостатньо інструментів «м'якої сили» для того, щоб досягти своєї мети, натомість є «жорстка сила» – влада, армія, які слугують для підтримки стратегії, що впроваджується російською розвідувальною спільнотою.*

31 Указ Президента України Про затвердження Річної національної програми під егідою Комісії Україна – НАТО на 2018 рік. President of Ukraine official website. 28.03.2018. https://www.president.gov.ua/documents/892018-23882

З цією тезою можна погодитися лише частково. З одного боку, російські спецслужби поступово починають грати більш самостійну роль в різних країнах світу. З іншого, Росія має певні інструменти «м'якої сили», які вона може застосовувати принаймні стосовно частини населення держав, які колись входили до складу СРСР, а це кілька мільйонів громадян. Серед них:

а) ностальгія за радянськими часами: «величчю держави», соціальними гарантіями радянського часу (безкоштовна освіта та медицина, можливість безкоштовно отримати житло та інше), ілюзія рівності тощо. Ці явища розповсюджені переважно серед людей віком за 50 років, досить вагомої групи з огляду на тенденцію старіння населення європейських та пострадянських країн.

б) протиставлення «російського порядку» (усталеність влади та чітка ієрархія прийняття рішень) «демократичному безладу» (часта зміна керівників на посадах, деконцентрація процесу прийняття владних рішень, неможливості «знайти правду» у влади);

в) експлуатація настроїв та фобій російськомовного населення у колишніх радянських республіках, їхньої неготовності або небажання інтегруватися в життя нових держав.

Крім того, Росія зберігає привабливість і для певних прошарків населення в країнах Європи, перш за все, як антиглобалістична сила або руйнівник нинішнього ліберального глобального порядку, а також через сентименти до «великої руської культури».

Відмінність стратегії російської розвідувальної спільноти, зокрема, прагнення Росії підірвати потенціал своїх противників простежується і в характері кібератак. Так, за оцінками М. Лайла Гранта, *Китай здійснює більше кібератак, ніж Росія. Однак кібератаки Китаю сконцентровані на здобутті економічної розвідувальної інформації, інтелектуальної власності, промисловому шпіонажі, у той час як російські кібератаки більше спрямовані на порушення процесу функціонування критичної інфраструктури, послаблення демократичних інституцій*. Тож у короткостроковій перспективі, на думку М. Лайла Гранта, загрози з боку Росії більш серйозні.

Важливою особливістю роботи російських спецслужб є відсутність обмежень у їхній діяльності. Вони застосовують різноманітний арсенал методів: вбивства (справа Скрипаля), державний переворот (приклад Чорногорії), окупація території (український Крим).

У оприлюднених свідченнях Директора національної розвідки[32]США Дена Коутса перед комітетом Сенату у справах розвідки в січні 2019 року, Російська Федерація зазначається серед загроз майже в кожному розділі – кіберзагрози, онлайн-операції

32 D. R. Coats, Statement for the Record "Worldwide Threat Assessment of the US Intelligence Community". United States Intelligence Community. 29.01.2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

впливу та втручання у вибори, зброя масового знищення та ядерне нерозповсюдження, контррозвідка, вороже використання космосу, регіональні загрози тощо.

Окремо зазначено, що очікується, що «російські спецслужби будуть спрямовувати свої дії проти Сполучених Штатів, намагаючись зібрати розвідувальну інформацію, підточити американську демократію, підірвати національну політику США та зовнішні відносини, а також посилити глобальну позицію та вплив Москви».[33]

За словами представника Об'єднаного відділу розвідки і безпеки НАТО Хав'єра Бейлона, *відвертість та неприхованість, які місцями межують з аматорством, є характерними рисами дій російської розвідки. Приклад – кібератака на Всесвітнє антидопінгове агентство (WADA), після якої залишилося безліч свідчень, які вказували на причетність до цієї операції російських спецслужб. Успіх операції важив більше, ніж ризик викрити себе. Але, варто зазначити, що відчуття «аматорства» з'являється тільки після того, як виконавці «схопленні за руку». Оскільки в більшості попередніх випадків ніхто не ловив російські спецслужби «на гарячому», то їхню тактику можна було вважати доволі ефективною.*

Водночас, існують відмінності у діяльності розвідувальних органів у різних регіонах. Ігор Смешко наголосив, що *для країн Заходу російська розвідувальна активність стала певною несподіванкою. З 1991 року в розвідувальних службах західних країн відбулося згортання «російського» напряму, скорочення кадрів, які займалися проблематикою Радянського Союзу. Так, у Великій Британії після окупації Криму відверто визнали, що їхня розвідувальна спільнота, Міністерство закордонних справ не були готові до того, що Росія піде не демократичним шляхом.*

> Китай здійснює більше кібератак, ніж Росія. Однак кібератаки Китаю сконцентровані на здобутті економічної розвідувальної інформації, інтелектуальної власності, промисловому шпіонажі, у той час як російські кібератаки більше спрямовані на порушення процесу функціонування критичної інфраструктури, послаблення демократичних інституцій

У свою чергу, Х. Бейлон підкреслив, що *в кожному з регіонів, де діє російська розвідка, її діяльність має свою специфіку. Сусідні країни найбільше піддаються прямим агресивним діям з боку Росії, зокрема, Україна є полем випробування новітніх тактик. Ре-*

33 D. R. Coats, Statement for the Record "Worldwide Threat Assessment of the US Intelligence Community". United States Intelligence Community. 29.01.2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf , p. 14

гіон Західних Балкан відкритий для непрямих дій з боку Росії. Так, в центрі уваги НАТО опинилася Колишня Югославська Республіка Македонія, де російські спецслужби застосовували весь арсенал: соціальні мережі, пропаганду, місцевих агентів тощо. У країнах Заходу – Великій Британії, Франції, Іспанії, за оцінками експертів, вплив російських розвідслужб менш агресивний, але не менш ефективний. Він здійснюється переважно через пропаганду, нав'язування певних наративів, втручання у політичний процес, зокрема, із застосуванням кібератак та соціальних мереж. Останнім часом з'явилися і випадки участі в масових заворушеннях у європейських країнах військовослужбовців Головного розвідувального управління,[34] які прибувають під виглядом уболівальників або туристів.

> Оприлюднення інформації щодо причетності російської розвідки до гучних справ можна вважати вдалим прикладом асиметричної відповіді на загрозу

Яскравим прикладом дій російської розвідки на Західних Балканах можна назвати і спробу державного перевороту у Чорногорії, який планувалося здійснити у жовтні 2016 року, щоб перешкодити вступу цієї країни до НАТО.

М. Лайл Грант зазначив, що *оприлюднення інформації про причетність офіцерів ГРУ РФ до замаху на Сергія Скрипаля є свідченням того, що у країнах Заходу, зокрема Великій Британії, добре усвідомлюють гібридні загрози. Те ж саме стосується і реакції на кібератаки на Всесвітнє антидопінгове агентство (WADA). Раніше уряди вважали за краще не оприлюднювати інформацію стосовно причетності тієї чи іншої країни до кібератак. Однак діяльність російської розвідки стала настільки зухвалою, що інформацію про її дії було вирішено відкрити для громадськості. Існує подвійна вигода від оприлюднення цієї інформації. По-перше, це можливість змінити позицію урядів країн, які не хотіли вірити, що за цим стоїть Росія (а саме Владімір Путін). По-друге, йдеться про приниження та висміювання Президента Путіна, оскільки дії його розвідки виглядають дуже аматорськими.*

Можна лише додати, що оприлюднення інформації щодо причетності російської розвідки до гучних справ можна вважати вдалим прикладом асиметричної відповіді на загрозу.

На думку Євгена Марчука, Прем'єр-міністра України (1995-1996) та Секретаря Ради національної безпеки і оборони (1999-2003), *проблеми, які виникли у відносинах між Україною та Угорщиною, Україною та Польщею зумовлені значною мірою роботою відповідних спецслужб Російської Федерації*. Сьогодні вони займаються не лише добуванням інформації, а й

34 Офіційна назва – Головне управління Генерального штабу Збройних Сил Російської Федерації.

мають завдання виконувати такі операції, які за своїм ефектом не поступаються військовим.

Підтвердженням цього є провокації проти Товариства угорської культури в Ужгороді, офіс якого двічі намагалися підпалити у лютому 2018 року. Виконавцями нападу були двоє польських громадян, яких згодом затримали правоохоронці. За інформацією Агентства внутрішньої безпеки Польщі, метою провокації було погіршення українсько-угорських відносин. Організатором нападу виявився відомий своїми проросійськими поглядами німецький журналіст Мануель Оксенрайтер, який у свою чергу, працює консультантом депутата німецького парламенту Маркуса Фронмайера з ультраправої партії «Альтернатива для Німеччини».[35]

Можна погодитися і з тезою Є. Марчука про використання демократичних інститутів для послаблення демократичних режимів. Як приклад, існування опозиції є нормальним явищем у демократичному суспільстві. Водночас, так звана «доктрина Герасімова»[36] передбачає трансформацію незгоди в протиріччя, протиріччя – в конфлікт, а конфлікту – у громадянську війну. Окремим елементом є *використання російських олігархів для фінансування спецоперацій, у той час як в Україні деякі олігархи стають виразниками російської позиції, відповідно відбувається трансформація політики телеканалів, які фінансуються через олігархів.*

Незважаючи на те, що розвідувальні операції мають точковий характер, вони зачіпають інтереси всього суспільства країн, у яких вони здійснюються, – зазначив М. Лайл Грант. *Наприклад, замах на вбивство Скрипаля агентами ГРУ РФ за допомогою отруйної речовини призвів до загибелі сторонньої людини. Те ж саме можна сказати і стосовно інших операцій російської розвідки, зокрема, кібератак проти Всесвітнього антидопінгового агентства (WADA), кампанії дезінформації під час референдуму щодо виходу Великої Британії з ЄС або виборів президента США, коли дії розвідок зачепили мільйони людей.*

У сьогоднішніх умовах кожна людина може стати об'єктом як кібератак, так і звичайного тероризму. Відповідно, уряди не можуть взяти на себе всю відповідальність за безпеку своїх громадян, особливо під час кібератак. Тож кожен має самостійно вживати заходи, аби убезпечити себе від цих явищ. Таким чином, за організацію протидії відповідає не лише розвідка, але й все суспільство і кожен громадянин.

Окремо варто підкреслити, що сьогодні до участі в спеціальних операціях закордоном (в Україні, Сирії,

35 У Німеччині відкрили справу проти організатора підпалу спілкиу горців в Ужгороді. *Європейська правда*. 18.01.2019.
https://www.eurointegration.com.ua/news/2019/01/18/7091725

36 В. В. Герасимов, "Ценность науки в предвидении". Военно-промышленный курьер. 2013. № 8 (476). https://www.vpk-news.ru/articles/14632 та M. Galeotti, "I'm Sorry for Creating the 'Gerasimov Doctrine'. *Foreign Policy*. 05.03.2018.
https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine

Польщі, Німеччині, Угорщині, ЦАР, Венесуелі, США) залучаються не тільки відповідні державні структури, але і ширше коло гравців, зокрема, приватні військові компанії, парамілітарні групи, політичні рухи і партії, окремі активісти і медіа-персони, які діють в інтересах тієї чи іншої спецслужби або структури сектору безпеки Російської Федерації. Парадоксальним чином розмивається і гібридизується не тільки зовнішній фронт і спосіб дій розвідок за межами РФ. Ефект від їх діяльності переноситися на територію самої Росії. При цьому, розвідувальна і підривна діяльність спецслужб РФ за кордоном сприймається їх очільниками як джерело прибутків і конкурентна перевага у внутрішньополітичній боротьбі. Таким чином ми спостерігаємо загострення боротьби спецслужб і дотичних гравців за ресурси і доступ до політичної влади. Такі особливості мають враховуватися українським розвідувальним співтовариством у виробленні механізмів протидії гібридній агресії.

> Однією з цілей гібридних атак є дискредитація розвідки і взагалі спецслужб в очах як суспільства, так і політичної еліти країни

Зауважимо, що однією з цілей гібридних атак є дискредитація розвідки і взагалі спецслужб в очах як суспільства, так і політичної еліти країни. Закритий характер їхньої діяльності спрощує це завдання. З огляду на це, важливим завданням є підвищення авторитету спецслужб, зокрема непрямими методами. Можна згадати, що авторитет російської розвідки, яка є спадкоємицею радянських спецслужб, створювався десятиліттями переважно за допомогою літератури та кінематографу. Сучасна Росія продовжує цю традицію. Це той випадок, коли міфологія переплітається з історією і стає неподільною. Україна не має таких власних традицій розвідки, так само, як і практики їх просування.

Роль розвідки у протидії гібридним загрозам

Учасники сесії «Роль розвідувальної спільноти у гібридній війні», в першу чергу, підкреслили необхідність належного аналізу та прогнозування загроз, визначення трендів, що входить до пріоритетних функцій будь-якої розвідки. Питання прогнозування загроз вимагає сьогодні якісно нових підходів до професійної підготовки та підвищення кваліфікації співробітників розвідслужб, а саме:

а) потрібно зважати на існування різного типу загроз (економічних, політичних, інформаційних), що вимагає від співробітників розвідслужби широкого спектру знань, розуміння специфіки політичних, економічних процесів тощо;

б) необхідно поглибити спеціалізацію співробітників по країнах (регіонах), яка б, у свою чергу, передбачала б певне коло знань, зокрема, володіння мовою країни (або однією з мов

країн регіону), базові знання щодо історії, політичного устрою, економіки, етнічних та конфесійних особливостей країни;

в) має існувати гнучка система заохочення співробітників розвідслужб щодо підвищення кваліфікації та знань.

У контексті першого пункту Є. Марчук та І. Смешко також наголосили на необхідності співпраці з експертним середовищем, неурядовими організаціями. В Україні сьогодні існує розвинена мережа неурядових організацій, які здійснюють аналіз та прогнозування загроз у політичній, економічній, інформаційній та соціальній сферах. Характерним є наведений Є. Марчуком приклад, коли розробники нової Морської доктрини передбачили можливе загострення ситуації в Азовському морі через російську блокаду. Однак ключовими моментами для налагодження продуктивної взаємодії залишаються:

а) мотивація неурядових організацій та експертів, які залучаються до здійснення аналізу, результатами яких будуть користуватися спецслужби;

б) залучення неурядових експертів до підготовки або підвищення кваліфікації представників спецслужб (наприклад, для підвищення медіаграмотності).

Протидія ворожій пропаганді, ідентифікація засобів масової інформації, які розповсюджують наративи, властиві ворожій пропаганді, комерційних структур, чия діяльність підриває основи національної економіки, виявлення зв'язків з організованою злочинністю, зокрема міжнародною, є наступним завданням розвідки та контррозвідки, на думку І. Смешка. Важливо також посилювати взаємодію між розвідувальними службами. Як зазначив Х. Бейлон, *незважаючи на закритість розвідувальної інформації, розвідувальні служби можуть бути відкритими для співпраці у питаннях боротьби з пропагандою, організованою злочинністю та ін.* У цьому контексті актуальною є ідея І. Смешка щодо створення євроатлантичної групи експертів високого рівня з питань розвідки та дослідження елементів гібридної війни, до якої пропонується залучити фахівців у сфері розвідки, національної безпеки, колишніх посадовців, які мають досвід та знання, представників недержавних установ.

> Проводити гібридні наступальні акції не менш важливо, і в той же час не менш важко та небезпечно, ніж військові операції

Є. Марчук підкреслив, *що проводити гібридні наступальні акції не менш важливо, і в той же час не менш важко та небезпечно, ніж військові операції. Уже зараз експертне середовище повинне пропонувати органам влади не тільки технології протидії оборонного характеру, а й гібридні наступальні акції.*

Запит на наступальну тактику щодо Росії висуває на перший план три ключові питання:

а) необхідність взаємодії з неурядовими організаціями та експертами з міжнародних відносин, які можуть інформувати закордонних колег про ситуацію в Україні та дії Росії під час участі у публічних заходах (конференціях, круглих столах тощо);

б) потреба у формуванні агентурної мережі та мережі агентів впливу (це можуть бути як громадяни України, так і закордонні громадяни), завданням яких має стати вивчення суспільних настроїв у цільових країнах, розповсюдження необхідної для України інформації в засобах масової інформації зазначених країн, співпраця з політичними колами. У цьому контексті особливого значення набувають питання матеріального та морального стимулювання агентури, оскільки відсутність належних стимулів стримує залучення нових агентів. Слід пам'ятати, що агент, якщо він не є професійним працівником розвідувальної служби, часто має йти всупереч власним переконанням, громадській позиції, жити подвійним життям, ризикувати якщо не власним життям, то принаймні, свободою. Саме тому він повинен, залежно від користі, яку він приносить Україні, мати право на належну матеріальну компенсацію.

в) поглиблення «російських» досліджень, а саме: вивчення політичних, економічних, соціальних, етнічних, конфесійних, екологічних проблем сучасної Росії для виявлення вразливих місць.

Крім того, на думку колишнього секретаря РНБО Є. Марчука, *якщо б нам, насамперед Україні, вдавалося б так розвінчувати спецоперації, як у випадку з Солсбері, щоб в результаті ставала б відома достовірна, документальна інформація про те, хто і як здійснив спецоперацію, тоді ми б могли сказати, що ми починаємо ефективно протидіяти гібридним технологіям цієї негібридної війни.*

Російські розвідувальні служби відіграють провідну роль у здійснені «гібридної війни» проти України, застосовуючи для цього весь «гібридний» інструментарій: дезінформація, кібертероризм, підтримка незаконних військових угруповань, безпосередня участь у проведенні військових операцій (окупація Криму), підтримка опозиційних до чинної влади політичних сил, провокування акцій громадянської непокори.

Українські розвідувальні служби виявилися неготовими до російської агресії, адже протягом всього періоду незалежності Росія не розглядалася як потенційний противник. Військова розвідка і відповідний підрозділ Прикордонної служби швидше адаптувалися і почали відновлювати свої спроможності, отримавши чіткий запит від керівних органів і розуміння наявних загроз.

Не менш активно російські розвідувальні служби діють проти західних країн, спрямовуючи свої зусилля на послаблення їхніх політичних інституцій. Працюючи проти західних демократій, вони використовують переваги демократичного устрою для його ж послаблення, наприклад,

свободу слова для розповсюдження фейкових новин. Підтримка радикальних антиєвропейських течій та організацій, втручання у виборчий процес та у референдуми (щодо виходу Великої Британії з ЄС, референдум у Нідерландах щодо Угоди про асоціацію України з ЄС), підбурювання до сепаратизму та протестних настроїв через соціальні мережі, й інші заходи – все це свідчить про те, що «гібридна» активність Росії виходить далеко за межі пострадянського простору. У послабленні демократичних держав Росія бачить шлях повернення собі провідної ролі, в першу чергу, у Східній Європі, й на міжнародній арені загалом. До подібного повороту подій західні країни (дипломатичний корпус та розвідувальна спільнота) були неготовими, що змушує їх зараз фактично «з нуля» формувати систему протидії «гібридним» загрозам.

Водночас, досвід останніх років свідчить, що російські спецоперації теж мають низку слабких місць. Викриття причетності російської розвідки до замаху на С. Скрипаля, кібератаки на Всесвітнє антидопінгове агентство (WADA) й ряду інших акцій, швидше за все, були зумовлені неготовністю російських служб діяти в умовах інформаційного суспільства, коли певна частина даних несекретного характеру знаходиться у відкритому доступі (бази реєстраційних даних, соціальні мережі, сайти організацій тощо). Без сумніву, керівництво російської розвідки зробить висновки з цих провалів, і будуть вжиті заходи, аби зробити участь російських спецслужб більш прихованою та уникнути у майбутньому подібного публічного розголосу. Однак показовим є те, що вже не допомагає навіть дипломатичний статус розвідників, свідченням чому є публічне вислання з Греції російських дипломатів (розвідників), які підбурювали до протестів проти угоди з Північною Македонією,[37] що відкривало останній шлях на вступ до ЄС та НАТО.

Необхідність протистояти «гібридним» загрозам з боку Росії вимагає сьогодні докорінної перебудови діяльності розвідувальних служб, зокрема, посилення координації їхніх дій, збільшення фінансування, оптимізації та більш ефективного використання наявних ресурсів, зміну підходів до професійної підготовки співробітників національних розвідувальних служб, посилення співпраці з розвідувальними службами країн-членів НАТО та з експертним середовищем.

37 P. Wintour, "Greece to expel Russian diplomats over alleged Macedonia interference". *The Guardian*. 11.07.2018. https://www.theguardian.com/world/2018/jul/11/greece-to-expel-russian-diplomats-over-alleged-macedonia-interference

КІБЕРВІЙНИ НОВОЇ ЕПОХИ: УСВІДОМЛЕННЯ ЗАГРОЗИ ТА ПРОТИДІЯ[38]

Кіберпростір є п'ятою сферою ведення бойових дій, поряд із традиційними «земля», «повітря», «море» та «космос», у якій дедалі більш активно діють відповідні підрозділи збройних сил провідних держав світу,[39] та, водночас, є джерелом постійних загроз. Під атакою опиняються державні інституції, критична інфраструктура, ЗМІ. Кібератаки можуть впливати на виборчий цикл цілих держав, маніпулювати суспільною думкою, підривати довіру до демократичних інституцій як таких. І якщо ключовою характеристикою сучасної гібридної війни є невизначеність, амбівалентність, то саме у кіберпросторі з його динамічною природою вона розкривається найповніше. Як зазначив Марек Щигель, Посол з особливих доручень з питань викликів безпеці Міністерства закордонних справ Польщі, *ми звикли, що існує чітке однозначне визначення миру чи війни, але у випадку кібероперацій розмивається лінія між цими поняттями. Існують тривалі кібероперації поза межами визначення збройного конфлікту. Але, у той самий час, ми не можемо назвати поточну ситуацію «кібер-миром», це так би мовити, «кібер-немир».*

У тексті під поняттям «кібербезпека» (КБ) у більшості випадків розуміємо: конфіденційність, доступність, цілісність, – без урахування теоретичних напрацювань про «кіберпростір» як театр бойових дій. Такий спрощений підхід започаткований авторами звіту Security Sector Reform in Ukraine,[40] підготовлений корпорацією RAND у 2016 році.

Інформаційна безпека (ІБ) та кібербезпека (КБ) будуть вживатися як синоніми, що є звичайною практикою для документів НАТО. Важливо однак пам'ятати, що до ІБ військових об'єктів та до об'єктів критичної інфраструктури можуть ставитися підвищені вимоги, як до систем АСУ ТП (Автоматизована система керування технологічним процесом, SCADA). Коротко цю відмінність можна описати так: «Як правило, до звичайних інформаційних систем (ІС) ставляться вимоги підтримання внутрішніх та зовнішніх зв'язків, належної продуктивності, застосування безпечних механізмів автентифікації та авторизації, та трьох основних принципів ІБ: конфіденційності, доступності та цілісності. Особливістю систем АСУ ТП (SCADA) є підвищені вимоги до на-

38 Більшість спеціальних термінів вживаються в тому значенні, що прийняте для службового спілкування в арміях НАТО.

39 Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», ст.2. 2016. National Security and Defence Council of Ukraine. http://www.rnbo.gov.ua/documents/417.html

40 Security Sector Reform in Ukraine. RAND. 2016. https://www.rand.org/pubs/research_reports/RR1475-1.html

дійності, роботи в режимі реального часу, здатність працювати в умовах надзвичайних ситуацій».[41]

Першими питаннями, на які відповідали учасники сесії «Кібервійни нової епохи», стали: Яким чином кібератаки адаптують до конкретних цілей та регіонів? Які уроки можуть бути засвоєні з останніх хвиль кібератак?

Голова Державної служби спеціального зв'язку та захисту інформації України Леонід Євдоченко зазначив, що *кількість кібератак стрімко зросла із початком військової агресії проти України.* У свою чергу, заступник голови Служби безпеки України Олег Фролов застеріг, *що суцільна інформатизація суспільства призвела до збільшення кількості кібератак та збільшення їхнього впливу на різні сфери діяльності суспільства; завдяки кібератакам агресору вдається досягати військово-політичних цілей без великого кровопролиття і руйнувань.*

Він підкреслив, *що засоби здійснення кібератак адаптуються для потреб і завдань інформаційно-психологічної війни проти України. Наприклад, під час президентських виборів у 2014 році внаслідок атаки на інтернет-ресурси Центральної виборчої комісії було на короткий час оприлюднено фальшиве зображення з підробленими результатами підрахунку голосів; цього було достатньо для створення інформаційного приводу у ворожих медіа, які намагалися підірвати довіру до справжніх результатів підрахунку голосів.*

Заступник голови СБУ наголосив, що гібридна війна, розгорнута Росією проти України, скоординовано здійснюється в інформаційному та в кібернетичному просторі, при цьому поширюються тези антиукраїнської пропаганди, робляться спроби дискредитувати Україну перед іноземними інвесторами та дезорієнтувати український бізнес; ускладнити постачання та виробництво озброєння та військової техніки для Збройних Сил України; ускладнити торгово-економічне співробітництво з Україною; порушити господарські відносини у сфері видобування, постачання та розподілу енергоресурсів для України, підірвати енергетичну незалежність.

> Ми звикли, що існує чітке однозначне визначення миру чи війни, але у випадку кібероперацій розмивається лінія між цими поняттями

Для ефективного ураження українських цілей російські військові розвідники та підконтрольні їм хакери постійно адаптують кібернетичну зброю зі збереженням спадковості у розвитку. Ланцюжок дій нападників вкладається у відому модель послідовних кроків (KillChain): (1) розвідка уразливостей; (2) розробка засобів атаки; (3) доставка; (4) експлуатація уразливостей; (5) інсталяція шкідливого програмного забезпечення

41 R. Krutz, Securing SCADA systems. John Wiley & Sons, 2005.

(ШПЗ); (6) зовнішнє керування; (7) застосування ШПЗ для кібер-шпигунства, або кібер-тероризму.

Наголошуючи на існуванні характерного профілю діяльності групи кібер-терористів, О. Фролов зазначив, що можна з достатньою вірогідністю стверджувати, що певні атаки проти України були здійснені так званою APT28, яку пов'язують з військовою розвідкою РФ. За словами О. Фролова, *кібератаки на інформаційні системи державних установ та об'єкти інфраструктури України мали ознаки складних багатокрокових високоефективних операцій організованих угрупувань типу Advanced Persistent Threat (APT), що вказує на свідоме ураження російськими спецслужбами та хакерами життєво важливих та значимих цивільних об'єктів.*

> Суцільна інформатизація суспільства призвела до збільшення кількості кібератак та збільшення їхнього впливу на різні сфери діяльності суспільства

Відповідно до доповіді розвідувальної спільноти США «Worldwide Threat Assessment», опублікованої в січні 2019 року та представленої на розгляд комітету Сенату з питань розвідки: *Росія використовує кібер-шпигунство, вплив та погрози проти США і наших союзників. Москва продовжує бути дуже сильним і ефективним супротивником, інтегруючи кібер-шпигунство, напад і операції впливу для досягнення своїх політичних і військових цілей. Москва зараз готує основи для проведення кібератак, щоб мати можливість порушити роботу або нашкодити цивільній та військовій інфраструктурі США під час кризи, а також становить значну кіберзагрозу*.[42] Конкретним прикладом такої діяльності у доповіді наведено втручання в електромережі України у 2015 та 2016 роках.

Кібератаки на українські державні та недержавні об'єкти нескладно адаптувати, оскільки переважна більшість програмного забезпечення в Україні є неліцензійною і не підтримується розробниками через оновлення. Застосування антивірусів не вирішує цієї проблеми, створює ілюзію безпеки і вводить користувачів в оману.

Заступник голови Служби безпеки України навів приклад атаки, здійсненої в червні 2017 році ШПЗ NotPetya. 75% уражень від цієї атаки припало саме на Україну, адже доставку ШПЗ зловмисники замаскували під оновлення програми для підготовки української податкової звітності; така тактика називається атакою через ланцюжок постачання (supply chain). Іншу атаку восени 2017 року, за інформацією СБУ, їм вдалося відвернути завчасно, ще на етапі підготовки.

42 D. R. Coats, Statement for the Record "Worldwide Threat Assessment of the US Intelligence Community". United States Intelligence Community. 29.01.2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf, pp. 4-5

Водночас, Посол М. Щигель, відзначив велику складність атрибуції (визначення державної або територіальної приналежності) атакуючої сторони. Анонімність, використання найманої робочої сили, чи застосування «зомбованих» раніше мережевих вузлів та робочих станцій ще більше ускладнює встановлення приналежності нападників.

Гучним викриттям стала заява уряду Великої Британії від 4 жовтня 2018 року про причетність російської військової розвідки до низки масштабних кібератак останніх років.[43] Заступник директора з питань безпеки та оборони Служби комунікацій Уряду Великої Британії Генрі Колліс зазначив, *що уряд його країни співпрацював зі своїми колегами з інших країн та вивчив їхній досвід, зокрема, Естонії. Близько десяти років тому (у 2011 році) підхід Великої Британії до організації захисту в кіберпросторі було змінено і нова концепція отримала назву «Поєднання»: безпекові, дипломатичні та економічні заходи почали комбінувати разом; здійснювати заходи послідовно, і координувати взаємодію на рівні Секретаріату з національної безпеки (СНБ), щоб досягти єдиної мети та реалізувати державну стратегію.*

Посол М. Щигель відзначив *відносну ефективність заходів з викриття приналежності атакуючої сторони та оприлюднення даних про агресора для зменшення кількості загроз або навіть для впливу на поведінку агресора. Велика Британія* та Нідерланди продемонстрували восени 2018 приклад такого викриття агресивних дій Росії.

> Базуючись на досвіді атак 2014 року, Україна усвідомлює необхідність максимально захистити бази даних державного реєстру виборців і єдиної інформаційно-аналітичної системи «Вибори»

Кібератаки є також ключовим елементом так званого зовнішнього втручання у виборчий процес. Йдеться як про спроби вплинути на електоральні симпатії виборців через оприлюднення в Інтернеті компрометуючої інформації про кандидата, отриманої у результаті хакерської атаки (вибори у США та Франції), так і про атаки на виборчу інфраструктуру (вибори в Україні). Л. Євдоченко розповів, що базуючись на досвіді атак 2014 року, Україна усвідомлює необхідність максимально захистити бази даних державного реєстру виборців і єдиної інформаційно-аналітичної системи «Вибори», а також усіх інформаційних ресурсів Центральної виборчої комісії України. Те саме стосується персональних даних виборців.

43 "UK exposes Russian cyber attacks". Foreign & Commonwealth Office. 04.10.2018. https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks?fbclid=IwAR3J-7YDfy-2DiagKRC7Jx1qn_YvKlFxF5mXG5auAh_RHijo98B290B_Z7w

Виконавчий віце-президент зі зв'язків з державними органами CybExer Technologies Мерле Майгре також наголосила, що кібербезпека є невід'ємним елементом безпеки виборів. При цьому, будь-які цифрові способи голосування повинні розглядатися з точки зору загальновизнаних стандартів відкритості, рівності та таємності. У контексті виборів, кібернетична безпека також повинна передбачати стратегічні комунікації, щоб забезпечити довіру громадськості до технології.

О. Фролов наголосив, що набутий досвід свідчить про комплексний вплив в інформаційному та кібернетичному просторі, а багатовекторність антиукраїнської пропаганди, де кібератаки відіграють допоміжну роль в інформаційних операціях, підтвердили необхідність розробки системного підходу, щоб протистояти такій комплексній агресії. Для посилення спроможності держави до оборони необхідно розвивати співробітництво з ЄС та НАТО, а також з країнами-партнерами на двосторонньому рівні.

Водночас, посилення спроможності України до оборони від кіберзагроз є важливою для всього євроатлантичного простору. Посол М. Щигель у своїй доповіді *зазначив принципову річ:* кіберзагрози не мають чітко окреслених меж, вони усі є транскордонними. Зважаючи на взаємопов'язаність, яка існує у сучасному глобалізованому світі, атака на одну країну впливає на інші країни. Йдеться про побічні та віддалені наслідки кібератак, оскільки у багатьох випадках атакуюча сторона не може або не хоче контролювати подальше поширення ШПЗ після атаки (внаслідок вірусного механізму поширення або внаслідок розповсюдження програмного коду ШПЗ).

Посол наголосив, що останніми роками ефективність кібератак зросла за рахунок кращої організації та скоординованості дій нападників. При цьому, як зазначила М. Майгре, технології постійно змінюються, відповідно постійно змінюються засоби нападу та засоби захисту. Ціллю кібератаки може стати військовий або цивільний об'єкт, де можуть бути застосовані однакові технології, відповідно, й уразливості будуть ті ж самі.

М. Майгре, яка очолювала Центр кібербезпеки НАТО у Таллінні, зробила стислий огляд історії атак на державні інтернет-ресурси, включаючи досвід Естонії (2007), коли вперше, у відповідь на кібератаку на державні інституції, до іншої держави було застосовано економічні санкції з метою асиметричної відповіді агресору. Для Естонії атаки 2007 року означали оголошення кібервійни з боку Росії.

В умовах гібридної війни, коли агресором стає держава, або підтримувані нею хакерські групи, виникає питання балансу сил у кіберпросторі. Протистояти подібній кіберагресії не можна лише силами однієї держави. Центр у Таллінні здійснив значну дослідницьку роботу і випустив відомий «Талліннський посібник» (The Tallinn Manual),[44] присвячений тому, як дер-

44 "Tallinn Manual on the International Law Applicable to Cyber Warfare". NATO Cooperative Cyber Defence Centre of Excellence. 2013. https://ccdcoe.org/tallinn-manual.html

жави можуть поширювати на кіберпростір існуючі міжнародні правила поведінки та усталювати нові традиції здійснення державної політики в кіберпросторі.

У сфері кібербезпеки термін «гібридний» позначає приховане застосування сили засобами, що прямо не заборонені міжнародними конвенціями і не підпадають під ознаки конвенційних засобів ведення збройного конфлікту, проте мають руйнівний вплив та інші ознаки акту агресії. Відповідно, сторона-жертва має право на застосування до агресора «сили» у відповідь. Подібна позиція визначається і в розділі 14 «Застосування сили» у «Tallinn Manual 2.0.» (2017).[45]

Важливим питанням залишається **розбудова ефективних механізмів стримування та стійкості до кіберзагроз.**

Г. Колліс підкреслив, що дієва протидія та попередження агресії неможлива без достатньої гнучкості та швидкості у прийнятті рішень. Адже *супротивник, з яким ми маємо справу, не зв'язаний моральними принципами та порушує загальновизнані норми міжнародного права, що ще раз довели події у Солсбері. Супротивник достатньо гнучкий у своїх діях (досить швидко адаптується), непередбачуваний та при цьому наполегливий у досягненні своїх агресивних цілей. Зокрема, це стосується тактики внесення та поглиблення протиріч між різними групами у суспільстві.*

Велика Британія будує свою кібербезпеку на усвідомленні того, що *нова епоха кібервійни вимагає дій на рівні урядів, які повинні теж бути гнучкими і адаптуватися. Належне управління сектором кібербезпеки означає застосування таких нових способів та засобів управління, які дозволять не відставати від супротивника. Британський експерт з кіберезпеки був однозначним: потрібно розробляти системи, які швидко змінюються; які постійно виявляють та закривають вразливості у великому масштабі, а також автоматично відновлюють системи після атаки. Лише такий новий підхід забезпечуватиме стійкість.*

Супротивник, з яким ми маємо справу, не зв'язаний моральними принципами та порушує загальновизнані норми міжнародного права

Державна стратегія кібербезпеки Великої Британії була оприлюднена у листопаді 2011 року. Головні тези стратегії: захищати власні об'єкти, стримувати агресорів та розвивати спроможності власного захисту (defend, deter and develop, 3D). Г. Колліс пояснив, *що їхньому уряду вдалося реалізувати стратегію завдяки тому, що постійно вдосконалювався процес управління. У діяльності*

45 "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations". NATO Cooperative Cyber Defence Centre of Excellence .2017. https://www.cambridge.org/ua/academic/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition?format=PB

державних інституцій послідовно запроваджувалися три принципи: координація (між державними інституціями, між державами-партнерами та державно-приватне партнерство), співробітництво та розвиток спроможностей (coordination, cooperation, capacity building, 3C). Впровадження кожного з цих принципів потребувало ресурсів, зусиль і часу. У 2015 році було створено Національний центр з кібербезпеки, який поєднав такі функції, як управління, оцінювання, визначення загроз, комунікація та координація. Центр добуває і вибірково ділиться з партнерами розвідувальною інформацією, а також відомостями про загрози. Для виконання цих завдань була створена національна система автоматичного сповіщення про загрози (Threatomatic).

> Операційна кібербезпека повинна підтримуватись технічними засобами та навчанням персоналу

Однак слід пам'ятати, що найбільш вразливим місцем кожної системи є людина. М. Майгре підкреслила важливість обізнаності користувачів з правилами кібергігієни. Операційна кібербезпека повинна підтримуватись технічними засобами та навчанням персоналу. За інформацією Олега Дерев'янка, співзасновника Kyiv Cyber Academy, *в Естонії понад 50% громадян обізнані про кіберзагрози. Це один із найвищих показників у світі. М. Майгре розповіла, що в Естонії кібергігієна викладається з раннього шкільного віку; дітей навчають правилам дотримання приватності та безпечної поведінки у мережі. Таким чином розвивається довіра до держави, у дітей не виникає негативних емоцій стосовно застосування інформаційних технологій.*

Г. Колліс наголосив на *важливості освітньої системи, котра буде готувати достатню кількість фахівців, що дасть можливість розуміти, оцінювати і долати кіберзагрози в майбутньому; скажімо, через 30 років.* За словами представника уряду Великої Британії, підготовка фахівців є критично важливою: *спочатку навички, а потім інструменти. Технології та засоби можуть бути дорогими, проте вони мають недостатню ефективність, якщо люди неправильно або неефективно їх застосовують. Координація передбачає підготовку фахівців з кібербезпеки для держави і для усіх секторів економіки*.

Важливим питанням залишається законодавча та інституціональна база для протидії та виявленню кіберзагроз. Голова Державної служби спеціального зв'язку та захисту інформації України Л. Євдоченко зазначив, що впродовж останніх двох років Україна здійснила низку важливих кроків для побудови національної системи кібербезпеки, зокрема, *було розроблено відповідну нормативну базу*. Водночас, голова ДССЗЗІ наголосив на важливості державно-приватного партнерства для підвищення відповідальності громадян та бізнесу за національну кібербезпеку. Леонід

Євдоченко згадав про заходи з модернізації CERT-UA (Computer Emergency Response Team of Ukraine)[46] та початок створення Єдиного контуру кібербезпеки України. *У цій моделі, на додаток до існуючих центрів кібербезпеки, передбачено створення і взаємодію відомчих центрів реагування на загрози та інциденти в сфері інформаційної безпеки.* На його думку, на сьогодні українські сили навчилися захищатися від кібератак.

Існує нелегальний ринок програмного забезпечення для здійснення кібератак, так само існує попит на пошук нових уразливостей. Обидва сценарії пов'язані із реальними загрозами для інформаційних систем, потребують міждержавної та міжвідомчої кооперації, налагодження системи обміну відомостями про загрози. Важливо, що у цьому напрямку почали працювати і суб'єкти забезпечення кібербезпеки України. Ситуаційний центр забезпечення кібербезпеки СБУ запровадив практику підключення до платформи MISP-UA об'єктів критичної інфраструктури та розробників популярного в Україні програмного забезпечення (наприклад, компанію LinkosGroup – розробника Me.Doc) та узгодження спільних дій через підписання меморандумів.

У рамках співробітництва Україна-НАТО заплановано розширення мережі ситуаційних центрів на основі платформи MISP-UA. Окремо варто згадати співпрацю в рамках Трастового фонду Україна – НАТО з питань кібербезпеки. Перший етап цього фонду завершився і одним з результатів став початок розбудови мережі ситуаційних центрів кібербезпеки (зокрема новий ситуаційний центр СБУ). Наразі продовжується консультації щодо наступного етапу.

У рамках співробітництва Україна-НАТО заплановано розширення мережі ситуаційних центрів на основі платформи MISP-UA

Посол М. Щигель вважає, що *настав час для розробки спеціального режиму санкцій, який може бути застосований у відповідь на кібератаки. З цією метою можна розвивати уже існуючі механізми застосування санкцій. Така можливість розглядалася ще у червні 2017 року, коли було прийняте рішення про колективну відповідь усього Євросоюзу на кібератаки щодо кожної держави-члена, включаючи атаки державних і недержавних зловмисників.*

Враховуючи транскордонний характер сучасних кіберзагроз, О. Фролов підкреслив, що *одним з ключових елементів протидії кібератакам на критичну інфраструктуру є налагодження дієвих механізмів міжнародної взаємодії, що забезпечать оперативний обмін інформацією, проведення спільних розслідувань, удосконалення механізмів взаємної правової допомоги, обміну кращими практиками у сфе-*

46 Computer Emergency Response Team of Ukraine. https://cert.gov.ua

рі кібербезпеки. Наприклад, в 2017 році було проведено перші командно-штабні навчання із захисту критичної інфраструктури (із залученням фахівців центрів передового досвіду НАТО та американських дослідників), де питання кібербезпеки були одним з 4-х базових сценаріїв.

> Настав час для розробки спеціального режиму санкцій, який може бути застосований у відповідь на кібератаки

Важливим аспектом протидії кіберзагрозам та вибудовування політики в цій сфері є формування позиції щодо **залучення так званих кібервійськ** та ролі недержавних анонімних помічників. Думки щодо цього питання різняться. Одні стверджують, що держава може забезпечувати лише кіберзахист та дбати про попередження загроз, однак інші вважають, що ефективний захист має включає можливість проводити і власні кібератаки. Так, наприклад, в Естонії після атак 2007 року у рамках Естонської Ліги оборони (сили резервістів) було створено кіберпідрозділ. До його складу входять лише три постійні офіцери та сотні цивільних волонтерів, які у разі надзвичайної ситуації в кіберсфері готові стати на захист національної безпеки держави.[47]

Водночас, на думку голови Державної служби спеціального зв'язку та захисту інформації України, *Стратегія кібербезпеки України має оборонний характер.*

М. Майгре, в свою чергу, зазначила, що *неможливо захиститися від кіберзагроз на належному рівні без розуміння як працює кібератака. Крім того, у кіберпросторі є дуже багато засобів, які є придатними як для наступальних, так і для оборонних дій. Ми маємо вибудовувати свої системи захисту та випробовувати їх під час спроб втручання, проникнення та інших видів тестування, наближених до реальності. Ці наступальні навички необхідно розбудовувати спеціалістам з кібербезпеки.*

Навряд чи можна розділити оптимізм щодо спроможності військових сил і засобів, котрі зазвичай застосовуються для «тестування на проникнення, оскільки набору самих процедур і технік не достатньо для здійснення ефективних сучасних кібератак, котрі у більшості випадків включають тактичні ходи, «обманні маневри», елементи соціальної інженерії та скоординовані дії груп зловмисників із вузькою спеціалізацією.

Воєнна доктрина України[48] (п.19) передбачає, що підготовка сил оборони України орієнтується на ведення ними як оборонних, так і контр-наступальних та наступальних дій. Згідно з цим, розробляються програми та плани бойової і оперативної підготовки, бойові статути і настанови Збройних

47 D. Blair, "Estonia recruits volunteer army of 'cyber warriors'". *Telegraph*. 26.04.2015. https://www.telegraph.co.uk/news/worldnews/europe/estonia/11564163/Estonia-recruits-volunteer-army-of-cyber-warriors.html

Сил України. У Стратегічному оборонному бюлетені, затвердженому у 2016 році, визначено Оперативну ціль 1.5. «Удосконалення системи кібербезпеки та захисту інформації» – «Очікуваний результат: в Міністерстві оборони України, інших складових сектору оборони створено підрозділи з кіберзахисту, протидії технічним розвідкам, впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC».[49] Однак, нам поки не відомо про можливу готовність атакуючих сил і засобів в кіберпросторі. Таким чином, на сьогодні завдання сил оборони України у кібервійні зводиться до підтримання належного рівня інформаційної безпеки на об'єктах критичної інфраструктури та критичної інформаційної інфраструктури.

Що стосується ролі недержавних акторів у забезпеченні національної системи кібербезпеки, то відомі випадки, коли вони допомагали виявити критичні вразливості. Однак наявна система суб'єктів забезпечення кібербезпеки України залишається негнучкою та мало враховує думку громадськості. У багатьох випадках виявлені активістами вразливості залишаються без уваги і без вирішення. Варто зазначити, що існує також загроза використання активістів для досягнення негативних цілей. Так, заступник голови СБУ О. Фролов звернув увагу на *застосування агресором для інформаційного протиборства ворожої резидентури під прикриттям «незалежних» блогерів або «незалежних» експертів.*

У контексті розвитку приватно-державної співпраці у сфері кібербезпеки цікавим є досвід Великої Британії, де було створено платформу партнерського обміну інформацією про кібербезпеку (Cyber Security Information Sharing Partnership, CiSP).[50] З часом вдалося досягти довіри між учасниками, і підприємства почали ділитися інформацією з урядом на умовах анонімності.

> Неможливо захиститися від кіберзагроз на належному рівні без розуміння як працює кібератака

Українським структурам слід врахувати низку конкретних рекомендацій з посилення сектору кібербезпеки України, що містяться у згаданому вище звіті корпорації RAND.[51] Зокрема, у звіті зазначено, що наявний розподіл

48 Указ Президента України Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України». President of Ukraine official website. 2015. https://www.president.gov.ua/documents/5552015-19443

49 Указ Президента України Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України». Parliament of Ukraine. 06.06.2016. https://zakon.rada.gov.ua/laws/show/240/2016#n10

50 Cyber Security Information Sharing Partnership (CiSP). National Cyber Security Center. 27.09.2016. https://www.ncsc.gov.uk/cisp

51 Security Sector Reform in Ukraine. RAND. 2016. https://www.rand.org/pubs/research_reports/RR1475-1.html

повноважень та відповідальності у секторі кібербезпеки України, незадовільна координація між суб'єктами забезпечення кібербезпеки призводить до розпорошення зусиль, сил та засобів та перешкоджає досягненню стратегічних цілей. Наприклад, недооцінюється роль та значення Національного банку України, особливо щодо підвищення обізнаності та поширення кращих практик та стандартів інформаційної безпеки серед фінансових установ та бізнесу. Також важливою є роль Центру кіберзахисту НБУ (CSIRT-NBU), що забезпечує оперативне реагування та обмін інформацією між усіма суб'єктами банківського ринку та правоохоронними органами в режимі реального часу.

Європейські країни поки що знаходяться на різному рівні готовності до відбиття кібератак та забезпечення національної кібербезпеки, однак серед них вже є усвідомлення критичності загрози, необхідності спільних зусиль через транскордонний характер проблеми, розуміння важливості обміну інформацією між країнами, зміцнення власної стійкості (в першу чергу, критичної інфраструктури). Гнучкість для швидкого реагування на загрози, розвиток приватно-державного партнерства, а також активна дискусія щодо необхідності покарання кіберагресора на міжнародному рівні – залишаються пріоритетними питаннями порядку денного.

ІНФОРМАЦІЙНА ВІЙНА ТА ОПЕРАЦІЇ ВПЛИВУ

Інформаційна війна та операції впливу сьогодні є одними з основних знарядь ведення гібридної війни. Іноді навіть спостерігаються випадки підміни цих понять. Хоча «гібридних» інструментів, засобів та методів набагато більше, а їхній вплив розповсюджується на значну кількість сфер функціонування держави і суспільства, саме інформаційні атаки є тим інструментом, який більш за все вражає суспільство та частіше стає відомим загалу.

Як визначив Вадим Черниш, Міністр з питань тимчасово окупованих територій і внутрішньо переміщених осіб України, *Росія – це не держава з розвідувальними і спеціальними органами, це спеціальні органи і служби з державою. Тому там всі цивільні агенції працюють на виконання завдань, ціллю яких є дестабілізація та вплив на цільові країни й суспільства.* У рамках попередньої сесії був наведений приклад російського іномовного телеканалу Russia Today, який фактично є інструментом інформаційної війни і бюджет якого є в кілька разів більшим за бюджет Служби безпеки України.

Водночас, Яніс Сартс, директор Центру передового досвіду НАТО зі стратегічних комунікацій у Ризі, зазначає, що *ми схильні до двох помилок. Перша – це говорити, що Росія «на голову вище нас». Так, в них були певні досягнення, але були і серйозні провали. Друга помилка – це думати, що ми все знаємо. Це призведе до того, що наступного разу ми будемо захоплені зненацька.*

Одним з пріоритетних завдань на шляху вивчення інформаційної загрози як складового елементу гібридної війни та розробки інструментів протидії їй є чітке визначення цілей, на які ці загрози спрямовані. Важливо ідентифікувати, **які сегменти суспільства є найбільш вразливими до інформаційних операцій зовнішнього впливу**, – це дозволить глибше розуміти стратегію і тактику супротивника й ефективно йому протидіяти.

За словами головної радниці і старшої директорки Національного демократичного інституту в Україні Мері О'Хейген, *результати проведеного Інститутом дослідження демонструють кореляцію між рівнем вразливості до російських інформаційних атак та несприйняттям ідеї гендерної рівності. Вона зазначила, що російська пропаганда весь час намагається експлуатувати тему гендерної рівності, при цьому намагаючись демонізувати саме слово «гендер».* За словами М. О'Хейген, *ці ж люди демонструють вразливість до інших типів атак, спрямованих, наприклад, проти представників ЛГБТ-спільноти, що дозволяє говорити про певну інтерсекціональність [перетин різних форм та систем пригнічення, домінування або дискримінації] цільової аудиторії, яка, ймовірно, також демонструватиме несприйняття етнічних меншин, представників інших релігійних вірувань тощо*. Втім, така інтерсекціональність є обмеженою, оскільки значною мірою спирається на використання певного набору стереотипів та інструменталізацію цінностей, базою для яких є просування нетолерантності.

Ми схильні до двох помилок. Перша – це говорити, що Росія «на голову вище нас». Так, в них були певні досягнення, але були і серйозні провали. Друга помилка – це думати, що ми все знаємо. Це призведе до того, що наступного разу ми будемо захоплені зненацька.

Окрім того, як зазначив керівник Могилянської школи журналістики Євген Федченко, *якби, наприклад, ви дивилися лише російське телебачення, ви би цілими днями слухали про те, що Заходу як сутності взагалі не існує.* Це дозволяє ідентифікувати два інші сегменти населення, потенційно більш вразливого до інформаційних атак з боку Російської Федерації. Зазначені сегменти принаймні частково перетинаються між собою:

- старше покоління, яке звикло до російських медіа, і може сприймати їх як складову частину особистісного культурного коду;
- російськомовне населення.

Останній пункт вимагає роз'яснення. Використання у повсякденному спілкуванні будь-якої мови логічно приводить до бажання споживати медіаконтент цією ж мовою, що більшою мірою ставить російськомовне населення під інформаційний удар. Як свідчить дослідження «Мовна складова гібридної війни», проведене С. Осначем, «якщо середній індекс РРП [результативності російської пропаганди] по Україні – 26 одиниць, то для україномовних цей індекс дорівнює лише 15 одиницям, натомість для російськомовних – 38 одиницям».[52] Такі дані не мають бути застосовані з метою дискримінації російськомовного населення, але вказують на необхідність більш інтенсивних освітніх кампаній та превентивних заходів, спрямованих саме на цей сегмент соціуму.

> Існування значної частки «невизначених» є такою ж загрозою для стійкості суспільства перед інформаційними впливами, як і велика кількість тих, хто вірить в російський наратив

Член парламенту Великої Британії Стюарт Макдональд відмітив, що дуже часто *маніпулятивні матеріали можуть бути розташовані тільки у російськомовній версії газети чи сайту, що підкреслює принцип інструменталізації медіа-простору.*

Ще одним сегментом суспільства, який є потенційно більш вразливим до операцій впливу, є аудиторія, яка ще не визначилась і не має чіткої позиції стосовно ряду ключових питань, які маркують довіру чи недовіру до запропонованого Росією дискурсу. Як відзначила М. О'Хейген, існування значної частки «невизначених» є такою ж загрозою для стійкості суспільства перед інформаційними впливами, як і велика кількість тих, хто вірить в російський наратив. Подібна невпевненість провокує апатію, зростання почуття втоми та незахищеності, які створюють сприятливий ґрунт для зовнішнього втручання у суспільні та політичні процеси через послаблення здатності соціуму до опору. Для досягнення цієї цілі агенти впливу наповнюють медіа-простір великою кількістю конфліктних повідомлень та наративів, прагнучи не стільки переконати аудиторію змінити точку зору, скільки спровокувати її до відмови від будь-якої позиції взагалі. Метою в даному випадку є те, щоб об'єкт впливу нарешті сказав: «я ніколи не дізнаюся правди, є різні пояснення, і я не хочу взагалі про це говорити». Таким чином людина відмежовується від проблемних питань, прагнучи позбутися відчуття постійної фрустрації та невпевненості.

Така спрямованість на поширення дезінформації та непевності через велику кількість конфліктних повідомлень

52 С. Оснач. "Мовна складова гібридної війни". Vox Populi. Червень 2015. http://www.vox-populi.com.ua/rubriki/politika/movnaskladovagibridnoievijniavtorosnacsergij

може бути характерною рисою дезінформації у порівнянні з пропагандою, яка полягає передусім в агресивному використанні мас-медіа для просування однієї точки зору. **Виділення відмінностей між такими поняттями як «дезінформація», «пропаганда» та «неправильна інформація»** (англ. misinformation), як і специфіка їхнього використання, заслуговує на більшу увагу і подальше вивчення. Можна запропонувати гіпотезу, що пропаганда розрахована на споживання російськими глядачами і виробляється здебільшого для внутрішнього медіа-ринку, який відносно легко контролювати; тоді як дезінформація є асиметричною інформаційною зброєю, покликаною внести розбрат та сум'яття у зовнішньому інформаційному середовищі, і таким чином, є продуктом, що виробляється на медіа-експорт. Втім, така гіпотеза потребує підтвердження чи спростування в результаті ґрунтовних досліджень.

Україна знаходиться на передовій інформаційного фронту, а тому структурні особливості її аудиторії є важливими для дослідження «механіки» російського інформаційного впливу. Разом з тим, слід наголосити, що інформаційні атаки калібруються відповідно до особливостей кожної аудиторії, наявності доступу до певного медійного ресурсу.

Юкка Саволайнен, директор Групи з вивчення вразливостей та стійкості Європейського центру передового досвіду з протидії гібридним загрозам, наголосив, *що демократія кожні чотири роки дає чудові можливості для ворогів. Потенційно, будь-які вибори в країнах членах ЄС та НАТО можуть перетворюватися на тест щодо того, залишатися чи ні в цих структурах. Є країни, у яких підтримка ЄС та НАТО коливається на рівні 50%, тому можуть з'являтися політичні інтереси провести референдум щодо виходу з цих міжнародних організацій.*

> У 2017 році проводилось дослідження, метою якого було виявити, хто у соціальних мережах поширює інформацію про Балтійські країни російською мовою. У латвійському та естонському сегменті Twitter 85% подібного контенту виробляли саме боти, а не люди

Особливо актуальною інформаційна загроза є для Балтійських країн через територіальну близькість до Росії та значний відсоток російськомовного населення. Держави колишнього соціалістичного табору розглядаються російською політичною елітою як легітимний простір для експансії, що сприймається як повернення до «законного» status quo радянської моделі. Як відзначив директор Центру стратегічних комунікацій НАТО в Ризі Я. Сартс, *у 2017 році проводилось дослідження, метою якого було виявити, хто у соціальних мережах поширює інформацію про Балтійські країни*

російською мовою. У латвійському та естонському сегменті Twitter 85% подібного контенту виробляли саме боти, а не люди. Практично, люди взагалі не були задіяні у цих розмовах. Це свідчить про те, що населення згаданих країн є ціллю потужних операцій впливу на регіональному рівні.

Інформаційний простір кожної з держав, що становить собою ціль для таких операцій, має власні характерні особливості, що ускладнює виведення універсальних критеріїв визначення потенційно вразливих груп населення – хоча активне просування вищезгаданих меседжів, заснованих на ідеї нетолерантності, є надзвичайно поширеним. Але видається можливим говорити про існування базового принципу, за яким відбираються такі групи населення. Як зазначив дослідник російської дезінформації, британський журналіст Едвард Лукас, «вони шукають економічне, соціальне, демографічне, лінгвістичне, регіональне, етнічне – будь-яке джерело розділення»,[53] і використовують такі лінії соціальних зламів, штучно їх підсилюючи.

Оскільки навіть найбільш гомогенне суспільство матиме низку проблемних питань, можна стверджувати, що методологія операцій впливу робить їх досить ефективними у будь-якому середовищі. Особливості цільової аудиторії беруться до уваги, але не змінюють основного принципу, за яким діють агенти російського інформаційного впливу.

Соціальні медіа надають широкі можливості для такого впливу і різного роду маніпуляцій з декількох причин. Так, Міністр з питань тимчасово окупованих територій В. Черниш наголосив *на технологічних особливостях функціонування соціальних мереж, які зменшують здатність аудиторії до критичного осмислення отриманої інформації. За його словами, часу, який зазвичай іде на перегляд стрічки новин, достатньо для того, аби сформувати сильну емоційну реакцію, а не на зважений аналіз.* Зауважимо, що саме орієнтація на емоційну складову, зокрема й на використання гучних заголовків, якими обмежується значна кількість читачів, є одним з основних принципів створення «фейків».

Поширення повідомлень на онлайн-платформах відбувається також за принципом «ланцюгової розсилки», згаданої заступницею директора European Values Think Tank Андреа Міхалковою, що дозволяє донести бажану інформацію до мільйонів користувачів.

Кінцевою метою маніпуляцій громадською думкою та поведінкою є тиск або коригування державної політики у певній країні. За словами В. Черниша, *російська влада активно використовує системи, націлені на вивчення простору в цільовому суспільстві* – такі системи, початково застосовувались у комерційній сфері у Російській Федерації, і пізніше були модифіковані та включені до

53 Opinion Video Series "Operation Infektion". Russian disinformation: from Cold War to Kanye. Episode 2. *New York Times*. 12.11.2018. https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html?fbclid=IwAR2USgPoZkcTZZ1P1d_nUKH8V3hX1VIDXCuP6O661kSzFcxAYyvUR9G3RII#two

політичного інструментарію. Наразі, наголосив В. Черниш, *Адміністрація Президента Російської Федерації і практично кожне силове відомство має подібний продукт, який використовує для вивчення ситуації.*

Під вивченням ситуації розуміється активний моніторинг настроїв населення, виявлення проблем та потенційних ліній соціальних зламів, згаданих вище. Далі інформація обробляється і, за принципом product placement, «повертається у цільовий простір». На необхідних меседжах робиться акцент, проблеми, що можуть призвести до дестабілізації ситуації в державі зсередини, посилюються. Втручання в алгоритми роботи медіа дозволяє розширити коло циркуляції такої специфічним чином обробленої інформації.

Отже, відповідно до цілей конкретної операції впливу на основі зібраних даних створюються відповідні повідомлення, які надалі розповсюджуються через експертів, через власників та/або менеджмент телеканалів та через неурядові організації, активістів та лідерів думок. У подальшому інформація набуває більшого розголосу, потрапляючи у простір соціальних медіа та стаючи темою обговорення у телешоу та в новинах. У результаті здійснюється інформаційний тиск на населення, маніпуляція суспільними настроями з метою дезорієнтації, підсилення апатії та зневіри у суспільстві, що, у свою чергу, може призвести до зміни курсу державної політики.

Заступник Міністра інформаційної політики України Дмитро Золотухін відзначив, що *російську інформаційну модель можна також порівняти із «серіалом», у якому існують загальні метанаративи, які поділяються на більш конкретні «сезони» (наприклад, тематика буцімто наявного зв'язку між Україною та ІДІЛ), кожен з яких має окремі «епізоди», тобто окремі фейкові повідомлення. Йдеться про одну з ключових рис російської дезінформації – схильність до постійного повторення меседжів, які необхідно закріпити у цільовому суспільстві.*

Одна з ключових рис російської дезінформації – схильність до постійного повторення меседжів, які необхідно закріпити у цільовому суспільстві

У цьому контексті варто згадати, що провідні російські медіа знаходяться під державним контролем. Так, телеканал «Россия 1» повністю належить державі, що у випадку Російської Федерації не передбачає вільної редакторської політики. Ключовими акціонерами каналу «НТВ» є державна компанія «Газпром», яка також інтенсивно використовується російською владою для досягнення зовнішньополітичних цілей, та компанії олігарха Ю. Ковальчука, одного з близьких партнерів В. Путіна. Відповідно до спільного дослідження Естонського центру Східного партнерства та Українського кризового медіа-центру, російські приватні медіа, які мали б демонструвати вищий рівень незалежності, виявляють

тенденції до повторення тих самих ключових повідомлень, часто у той же спосіб та з використанням тієї ж самої термінології, що і федеральні ЗМІ. Це ставить їх теоретичну незалежність під сумнів.[54]

Телебачення за своєю структурою є більш зручним для централізованого управління у випадку авторитарної держави, ніж інтернет-ресурси чи соціальні медіа. Втім, на практиці інформаційні операції у мережі не менш ефективні, ніж через традиційні медіа. Переважна більшість основних новинних ресурсів, які російська влада використовує для поширення дезінформації та пропаганди, мають свої сторінки на популярних веб-сайтах, таких як Youtube, Twitter, Facebook тощо. У такий спосіб можна встановити певний зв'язок між повідомленнями, що просуваються на російському телебаченні, та такими ж за смисловим навантаженням повідомленнями, що масово поширюються у соціальних мережах за допомогою «тролів» та «ботів».

Варто зауважити, що така широка медіа-присутність робить спроби України обмежити поширення дезінформації надзвичайно складними: практично всі програми, що можуть бути промарковані як «рупори Кремля», викладають відповідні матеріали на своїх сторінках у загальний доступ, часто у прямому ефірі. Ще більш потужно інформаційні операції здійснюються через такі мережі як «Вконтакте» та «Одноклассники». Як під час відкриття конференції відзначив Президент України П. Порошенко, *вже через декілька місяців після їх заборони надійшли підтвердження, що згадані ресурси знаходились під впливом ФСБ.*

Можна говорити про ще одну роль соціальних мереж, яка стає ключовою з урахуванням централізованого управління такими аккаунтами, – створення штучного інформаційного дисбалансу. Позитивні новини та точка зору, яка суперечить меті операцій інформаційного впливу, опиняються у меншості, що допомагає підсилити сумніви та дезорієнтацію в аудиторії. Як було згадано вище, саме на поширення таких настроїв орієнтується дезінформація.

Враховуючи, що доволі значна частка населення в силу різних раніше розглянутих причин є вразливою до інформаційного впливу, виникає питання: **як ефективно протидіяти такому деструктивному зовнішньому впливу і водночас зберегти свободу слова?** Насамперед, варто зазначити, що збереження свободи слова як однієї з базових цінностей демократії є надзвичайно важливим не тільки в контексті розбудови успішної демократичної держави, але і для боротьби з агресором. На думку М. О'Хейген, *Росія була б дуже щаслива, якби Україна відмовилась від ідей демократичного майбутнього.* Така відмова включила б Україну до ціннісної парадигми, яку активно просуває Росія і експансивну суть якої розглянуто нижче.

54 "Image of European countries on Russian TV". *Estonian Center of Eastern Partnership and Ukraine Crisis Media Center Report*. May 2018: http://ucmc.org.ua/wp-content/uploads/2018/02/TV-3.pdf

Якуб Каленський, член робочої групи «East Strat Com» Європейської служби зовнішньої діяльності у 2015-2018 роках, підкреслює, що *ми [європейці] маємо багато інструментів, які дозволяють вести боротьбу з дезінформацією, не обмежуючи права на свободу слова. Наприклад, законодавство проти «мови ненависті» або проти поширення хибної тривоги (false alarm stories).*

Ряд держав вже застосовує **законодавчі обмеження для боротьби з дезінформацією та маніпуляціями. Так,** в Україні, окрім блокування вже згаданих російських соціальних мереж, Національна рада з питань телебачення та радіомовлення у 2014 році обмежила трансляцію 77 російських каналів. Як було згадано під час дискусії, *Литва також має закон, за яким можна припиняти трансляцію певних телеканалів.* Наприкінці січня 2019 року Національна рада щодо електронних медіа Латвії на три місяці заборонила трансляцію телеканалу «РТР-Россия» через розпалювання ненависті до громадян України.[55]

Фактично країни постають перед дилемою. З одного боку, наражаються на критику з боку ОБСЄ щодо обмеження свободи слова, а з іншого, такі заходи довели свою ефективність для національної безпеки. Однак, враховуючи, що країни Балтії, як і Україна, продовжують на щоденній основі ставати мішенями деструктивних інформаційних атак, очевидно, що суто у юридичній площині вирішити таке питання неможливо.

Цьому сприяє також той факт, що медіа-сфера, а разом з нею і способи використання старих та нових медіа для маніпуляцій громадською думкою, стрімко змінюється і розвивається . В. Черниш зазначив, *що більшість відповідних міжнародних законодавчих актів були написані тоді, коли кіберпростір не набув ще сучасного вигляду, і, відповідно, у юридичній площині існує певна «біла пляма» стосовно протидії операціям впливу з використанням нових медіа. Необережність у діях може призвести до звинувачень у порушенні прав людини і громадянина, що, у свою чергу, може і, скоріш за все, буде використано Російською Федерацією для завдання додаткових репутаційних втрат.*

Більшість відповідних міжнародних законодавчих актів були написані тоді, коли кіберпростір не набув ще сучасного вигляду, і, відповідно, у юридичній площині існує певна «біла пляма» стосовно протидії операціям впливу з використанням нових медіа

Іншою перешкодою на шляху протидії операціям впливу, яка б не порушувала встановлених прав і свобод, є складність розрізнення, до чиєї компетенції

55 "Latvian broadcast regulator hits Russian channel with 3-month ban". *Latvian Public Broadcasting.* 31.01.2019. https://eng.lsm.lv/article/culture/culture/latvian-broadcast-regulator-hits-russian-channel-with-3-month-ban.a307942/

відносяться подібні операції. Як відзначив В. Черниш, *якщо за інформаційною атакою було виявлено представника Головного управління ГШ РФ (ГРУ), то очевидно, що такий випадок належить до компетенції військових. Але чітко ідентифікувати виконавців та організаторів не завжди можливо, зазвичай доводиться мати справу з посередниками, що суттєво ускладнює проведення розмежувальної лінії, за якою можлива відповідь військовими методами.*

На російському телебаченні Захід згадується у негативному світлі близько 25 разів на день – для порівняння, бренд «Coca-Cola» має лише 6 випусків своєї реклами на тих самих телеканалах

Невизначеність підсилює також той факт, що Росія активно використовує певний ряд цінностей, специфічним чином переосмислених та інтерпретованих, для просування свого порядку денного, що накладає свій відбиток на сфери, які взагалі важко піддаються будь-якому політичному регулюванню і, теоретично, мають бути від нього вільними – переважно це масова культура та релігія.

Сформульоване М. О'Хейген питання, *як цінності можна перетворити у зброю,* є надзвичайно актуальним, особливо зважаючи на те, що саме за ціннісною орієнтацією визначається один із сегментів потенційно більш вразливої до впливу аудиторії – люди, які негативно ставляться до концепції гендерної рівності, захисту прав меншин, як було згадано вище. Але для того, щоб знайти відповідь на таке питання, необхідно спочатку визначити, про які саме цінності йдеться.

Показовим є той факт, що у розробці та просуванні своїх наративів, російські агенти впливу часто спираються на меседжі зі знаком «мінус», активно експлуатуючи протиставлення російських та західних цінностей. Перші, часто називають традиційними, хоча на практиці йдеться про цінності, які мають штучно сконструйований характер.

Як свідчить дослідження Групи з аналізу гібридних загроз УКМЦ, російські медіа створюють різко негативний образ європейських країн та Сполучених Штатів Америки, дегуманізуючи рядових європейців, змальовуючи США як основного ворога Росії, представляючи життя у Європі як небезпечне і нестабільне. Важливе місце у цьому образі займає теза про аморальність та ціннісний занепад європейського суспільства.[56] Відбувається «атака на словник, що використовується» і здійснюється підміна понять, у результаті чого такі слова, як демократія, свобода тощо наповнюються негативним змістом, а демократичні та ліберальні цінності дискредитуються. Любов Цибульська, керівниця

56 "Image of European countries on Russian TV". *Estonian Center of Eastern Partnership and Ukraine Crisis Media Center Report.* May 2018: http://ucmc.org.ua/wp-content/uploads/2018/02/TV-3.pdf

згаданої вище аналітичної групи, навела такі дані: *на російському телебаченні Захід згадується у негативному світлі близько 25 разів на день – для порівняння, бренд «Coca-Cola» має лише 6 випусків своєї реклами на тих самих телеканалах*.

При цьому, повідомлень та наративів, які не будуються на критиці західних цінностей чи, радше, того, що після смислових маніпуляцій під ними мається на увазі – вкрай мало. Національний демократичний інститут спробував з'ясувати, що мається на увазі під російськими цінностями. Дослідження показало, що у 36-ти фокус-групах, проведених у південних та східних регіонах України, найбільш популярною відповіддю на це питання стало «нічого». Окрім цього варіанту, учасники опитування включили до набору російських цінностей такі поняття як «родина», «велика держава», «православні», «традиція», «Путін», «імперія», «нафта» тощо. Але наявність такого великого вакууму як «нічого» свідчить про те, що основним смисловим пластом так званих російських цінностей в даному випадку є критика західного ліберального світогляду, – це, у свою чергу, демонструє їхній утилітарний характер.

Водночас, відповідно до того ж дослідження NDI, західні цінності, в першу чергу, асоціюються з такими поняттями як «свобода», «культура», «верховенство права», «розвиток» та «рівність».

Зважаючи на відсутність позитивного, смислового наповнення російського ціннісного наративу, який базується виключно на принципі протиставлення, такі штучно сконструйовані цінності, що мають соціополітичне застосування, можна назвати анти-цінностями. Додатковим підтвердженням є швидка реакція на актуальні процеси у сфері культури та намагання їх експлуатувати. Як було відзначено під час конференції, *у процесі отримання Українською православною церквою автокефалії почала з'являтися велика кількість фейків та маніпуляцій відповідної тематики*. Отже, негативний наратив може вибудовуватись ситуативно, що свідчить про інструментальну природу таких анти-цінностей.

Ще одним прикладом такого інструментального підходу є експлуатація тематики, пов'язаної з ЛГБТ-спільнотою, що корелюється із визначеною вище вразливістю певних сегментів населення до російського інформаційного впливу. Д. Золотухін продемонстрував результати дослідження, згідно з яким *російська сторона особливо активно застосовувала негативну риторику, пов'язану з ЛГБТ-спільнотою у 2012-2013 роках у зв'язку з прийняттям рішення про підписання Угоди про асоціацію між Україною та Європейським Союзом. Таким чином, спираючись на відповідний набір анти-цінностей, медіа були спрямовані на максимальне віддалення українських споживачів відповідного контенту від структур ЄС.*

У підсумку, мета полягає у тому, аби експлуатувати і підірвати віру в зміни, популяризувати нетолерантність до інших людей. Мері О'Хейген погодилася, що *внаслідок активного використання таких меседжів, вразлива*

до них частина аудиторії починає негативно сприймати євроатлантичні структури, що і можна вважати метою просування такого набору антицінностей.

Можна додати, що на внутрішньому медіа-ринку Росії вони мають дещо іншу роль: глибоко вкоренити несприйняття західного способу життя та шкідливих для автократичної традиції цінностей, що йому характерні, а також обґрунтувати необхідність консолідації суспільства навколо єдиного лідера, як відповідь на загрозу агресивного зовнішнього середовища.

> Продукція російської масової культури нерозривно пов'язана з консервативним, антизахідним світоглядом і також просуває «офіційні» наративи

Дещо більшої уваги потребує актуальне **питання церковних відносин** і дослідження того, як саме певний симбіоз між російською політичною елітою та Російською православною церквою використовується в операціях впливу. Очевидним здається той факт, що консервативна російська церква є зручним майданчиком для просування згаданих вище анти-цінностей, але більш чітке розуміння механізмів та специфіки такого просування може виявитися корисним у боротьбі з дезінформацією. Так само на увагу і додаткове вивчення заслуговує питання сучасної масової культури та її використання в рамках інформаційного впливу. На базовому рівні можна говорити про те, що продукція російської масової культури нерозривно пов'язана з консервативним, антизахідним світоглядом і також просуває «офіційні» наративи. Наприклад, кінематографічна продукція в недемократичному політичному контексті має великий потенціал до нав'язування певного порядку денного, при чому нав'язування непрямого. Це додатковий канал впливу на аудиторію, яка ще не визначилася зі своєю позицією або вже перебуває у стані дезорієнтації та апатії, в якому її необхідно утримувати і надалі.

Певний сегмент населення, вразливий до інформаційних атак, дотримуючись принципу «не цікавитись політикою», може уникати перегляду новин та/або політичних ток-шоу і соціальних медіа, що використовуються для просування необхідних наративів, але при цьому споживати інший медіа-контент, такий як фільми та телесеріали. Саме тому, подальшого вивчення потребує те, як саме медіа-продукція такого формату може використовуватись для інформаційних атак та маніпуляцій громадською думкою.

Реакцією на використання анти-цінностей як інструменту інформаційного впливу, відповіддю на просування російських наративів взагалі має бути створення та укріплення власних цінностей. Як зазначив пан Сартс, *необхідно розбудовувати свої власні наративи та ідентичність, і потім певним чином модифікувати їх*

відповідно до реакції Росії на наратив, який вибудовуєте ви. Важливо не дозволяти їм вибудовувати свій наратив і змушувати вас відповідати на нього, тому що тоді ви з самого початку будете просто наздоганяти їхні дії. Це не принесе успіху. Проактивна позиція є альтернативою як агресії, так і пасивній реакції та являє собою найкращу відповідь інформаційній агресії та операціям впливу. Причому важливо розбудовувати власний наратив, що базується на цінностях із реальним смисловим наповненням, а не штучно створених через протиставлення зовнішньому ворогу. Так само важливо коректно поширити такий наратив. Можливо, для Європейського Союзу було б доречно створити медійну альтернативу російським телеканалам, яка дозволила б запропонувати російськомовній аудиторії іншу точку зору, відмінну від дезінформації та пропаганди. Поява альтернативи російським ЗМІ, які фактично утилізують інформаційний вакуум, в якому наразі перебуває ця аудиторія, може суттєво поліпшити стійкість європейських суспільств до операцій впливу.

Як один з можливих способів боротьби з інформаційними атаками, Я. Каленський назвав *ініціативу маркувати ті медіа-ресурси, які були помічені у розповсюдженні фейків та дезінформації відповідною міткою, яка би дозволила потенційним глядачам одразу ідентифікувати можливу загрозу*. Він провів паралель із попередженнями, розміщеними на пачках тютюнових виробів, – такий принцип дозволить уникнути цензури та допомогти глядачу зробити поінформований вибір.

Втім, необхідно розуміти, що такий крок може бути ефективним лише як один з елементів цілого комплексу заходів. Крім того, його результативність може знизитися, зважаючи на те, що людям характерно вірити тим повідомленням, які співпадають з їхньою уже сформованою точкою зору, підкріплюють їхні переконання; тому подібне маркування не буде ефективним відносно людей, які довгий час споживають російський медіа-контент і мають високий рівень довіри до нього.

Для Європейського Союзу було б доречно створити медійну альтернативу російським телеканалам, яка дозволила б запропонувати російськомовній аудиторії іншу точку зору, відмінну від дезінформації та пропаганди

Іншою частиною комплексу заходів протидії дезінформації має бути оновлення законодавчої та регуляторної бази. Зокрема, йдеться про необхідність зменшити кількість вищезгаданих «білих плям» у національному законодавстві і чітко визначити, коли відповідь на інформаційні атаки та виклики у кіберпросторі може належати до компетенції військових та/або силових структур.

Суперечливим питанням міжнародного дискурсу залишається ідея визнання за соціальними платформами

статусу медіа, або накладання на них відповідальності за публікацію неправдивої інформації, підбурювання до протестів, антидержавних закликів, маніпуляцію громадською свідомістю, поширення реклами в соцмережах з метою дезінформації. Принцип свободи слова протиставитися принципу відповідальності. Якщо традиційні ЗМІ обмежені відповідним законодавством, наприклад, законами про дифамацію, то соціальні мережі довгий час залишалися поза межами правового поля, при цьому маючи більший вплив на громадську думку.

1 березня 2018 року Європейська комісія опублікувала Рекомендації щодо ефективної боротьби з нелегальним контентом в Інтернеті. Основний посил – посилення відповідальності постачальників інтернет-послуг (включно з хостинг-провайдерами) за управління контентом, в першу чергу, визначення й видалення контенту із мовою ворожнечі та насильством. Німеччина у жовтні 2017 року ухвалила закон (The Network Enforcement Act або NetzDG), який передбачає ширше регулювання «неоднозначного» контенту, окрім явної мови ненависті. Цей закон вимагає від соціальних медіаплатформ вилучення контенту з мовою ворожнечі протягом 24 годин після отримання скарги (і за сім днів у випадках спірного контенту). У іншому випадку на них може бути накладено штраф у розмірі до 50 мільйонів євро. Президент Франції Е. Макрон також анонсував підготовку закону задля обмеження поширення дезінформації під час виборів.[57]

Важливим елементом залишається і фінансування операцій впливу. За словами В. Черниша, *система фінансування інформаційних операцій схожа на лінійне фінансування тероризму.* Тому об'єднання різних служб та відомств у процесі виявлення та протидії таким операціям є вкрай важливим.

Поруч із доопрацюванням законодавства, одним з найбільш важливих напрямів є координація зусиль, причому як на національному, так і на міжнародному рівні. Спікери неодноразово відзначали, що *в Україні існує значна кількість ініціатив, які займаються дослідженнями та боротьбою з дезінформацією, але при цьому, частково через конкуренцію, їх зусилля рідко узгоджені*. Окрім такого узгодження, надзвичайно важливим є залучення державних органів, що дозволяє сформувати потужну відповідь проти масштабних цілеспрямованих інформаційних атак, фінансованих російською державою. За словами, В. Черниша, *інформаційна війна – це багатовимірна проблема, яка потребує узгодженої діяльності не тільки між фахівцями, що безпосередньо займаються інформаційними операціями та операціями впливу, військовими. Необхідно об'єднати експертизу фахівців з різних сфер для напрацювання спільних підходів.*

57 «Демократичний захист від дезінформації»: рекомендації Atlantic Council. *Detector media*. 27.03.2018. https://ms.detector.media/trends/1411978127/demokratichniy_zakhist_vid_dezinformatsii_rekomendatsii_atlantic_council/

На міжнародному рівні координація має значення, насамперед, для обміну досвідом. Експерти з роботи медіа та протидії дезінформації з Балтійських країн та України, що мають великий відповідний досвід, можуть вести плідний діалог не тільки між собою, але й зі своїми колегами з країн, у яких операції впливу потрапили у поле зору спеціалістів не так давно.

Нарешті, принциповою рекомендацією, на якій зробили наголос практично всі спікери, є підвищення обізнаності населення. Ніхто не може захистити споживачів контенту краще, ніж вони самі, але для цього необхідно виконати великий пласт освітньої роботи. Як зазначила М. О'Хейген, *необхідно постійно робити наголос на трьох основних тезах – самому факті інформаційної атаки, на тому, як вона відбувається, та на тому, з якою метою вона здійснюється.* Надзвичайно важливим є факт роз'яснення: саме лише твердження про існування російської дезінформації є малоефективним. Натомість, навчити аудиторію бачити механізми, за якими агенти впливу через медіа-простір маніпулюють громадською думкою, дати їй інструментарій для протидії таким маніпуляціям означає допомогти у створенні свого роду стабільного внутрішнього орієнтиру, який є найбільш ефективним способом протидіяти дезорієнтації.

Такий системний підхід може бути більш ефективним, ніж точкові зусилля, такі як перевірка фактів. Зокрема, Д. Золотухін відзначив, що *не є прихильником подібного підходу через систематичний характер російської дезінформації та пропаганди. Враховуючи обсяг продукованих повідомлень, на розвінчування кожного фальшивого інфоприводу витрачається значна кількість ресурсів.*

> Координація зусиль країн-членів Альянсу та партнерів має особливе значення, зважаючи на те, що вироблений у Кремлі медіа-дискурс робить НАТО однією з основних мішеней атак

Принциповим напрямом роботи є поглиблення і розширення співпраці України з НАТО. Очевидно, що проблема дезінформації та пропаганди має не тільки військовий вимір, але й відноситься до ширшої сфери безпеки. Координація зусиль країн-членів Альянсу та партнерів має особливе значення, зважаючи на те, що вироблений у Кремлі медіа-дискурс робить НАТО однією з основних мішеней атак, просуваючи тезу, відповідно до якої Альянс представляє собою ворога, від якого необхідно активно оборонятись.[58]

Окрім того, співробітник Державного департаменту США в період президенства Обами Джеффрі Стейсі відзначив

58 "Image of European countries on Russian TV". *Estonian Center of Eastern Partnership and Ukraine Crisis Media Center Report.* May 2018: http://ucmc.org.ua/wp-content/uploads/2018/02/TV-3.pdf

існування так званої «спільної пастки безпеки» – кризової ситуації, вихід з якої можливий лише завдяки кооперації всіх, хто у неї потрапили. Такою пасткою є процеси формування та розповсюдження дезінформації, і потрапила у неї не тільки Україна, але й інші європейські країни та Сполучені Штати Америки. А тому саме координація зусиль в рамках НАТО та підтримуваних Альянсом ініціатив може бути шляхом, який дозволить пережити кризу інформаційного суспільства з найменшими втратами.

Теоретично можна вести мову про створення спільної платформи в рамках НАТО та ЄС, що дозволило б організовано та системно протидіяти інформаційним атакам як явищу. Україна як держава, що має краще розуміння специфіки сучасної російської дезінформації, отримала б можливість не тільки поділитись відповідним досвідом і вивчити уроки інших країн, але й взяла б практичний курс на зближення з Альянсом в одній з найбільш актуальних сфер його компетенції. Таке зближення дозволило б збільшити ціну відповідних операцій впливу для агресора, про необхідність чого неодноразово згадували учасники конференції.

ЩО ТРЕБА ЗНАТИ ТА РОБИТИ ДЛЯ УСПІШНОГО РУХУ ВПЕРЕД?

Наведені нижче висновки та рекомендації є результатом дискусій під час Конференції та аналізу, проведеного авторами цієї доповіді. Вони покривають різні аспекти застосування гібридних методів ведення війни та дестабілізації суспільства – політичну, військову, інформаційну сфери, питання кібербезпеки та розбудови стійкості, у першу чергу, українського суспільства.

Окремі висновки стосуються підвищення рівня взаємодії з союзниками та партнерами, як на двосторонньому, так і багатосторонньому рівні, зокрема з НАТО. Часто зазначається, що боротьба з гібридними загрозами – це, в першу чергу, завдання національного рівня. Така думка має право на існування, але міжнародне співробітництво, як на двосторонньому рівні, так і європейському або навіть трансатлантичному, дає додаткові інструменти, можливості та поштовх у боротьбі та попередженні гібридних загроз.

Загальні висновки та рекомендації:

1. Необхідні зміни на законодавчому рівні, що дозволять краще боротися з поширенням неправдивої інформації, з пропагандистськими ЗМІ, а також з маніпуляціями у соціальних мережах. Водночас, такі зміни повинні пройти суспільне та експертне обговорення з метою мінімізації можливого порушення права на свободу слова, забезпечення розуміння та підтримки суспільства для впровадження таких змін, зменшення можливостей політичного маніпулювання на цій темі.

2. Питання агресивної дезінформації та ворожої пропаганди повинні залишатися на безпековому та зовнішньополітичному порядку денному держав та міжнародних організацій. Це, зокрема, включає і питання покращення якості стратегічних комунікацій України та її дипломатичних представництв за кордоном щодо ключових питань зовнішньої та внутрішньої політики України, належне співробітництво з іноземними експертами та медіа-спільнотою.

3. Публічно оспорювати дії прихильників кремлівської дезінформації, особливо серед політиків та публічних діячів. Розкривати суть дезінформаційних кампаній та механізми їх розповсюдження. Водночас, саме лише твердження про існування російської дезінформації є малоефективним. Необхідно навчати аудиторію бачити механізми, за допомогою яких агенти впливу через медіа та інтернет-простір маніпулюють громадською думкою.

4. Тісна співпраця з громадянським сектором та медіа. Дії державних органів обмежені та недостатньо

швидкі, а тому мають бути підсилені неурядовими організаціями та медіа. У першу чергу, це стосується експертизи щодо можливих загроз, аналізу медіа та інформаційного контенту, виявлення потенційних конфліктних тем, які можуть бути використанні у ворожій пропаганді, та освіті, підвищення обізнаності суспільства щодо фактів застосування гібридних методів.

5. З метою покращення діяльності розвідувальних служб, необхідно розробити нові принципи їхньої взаємодії з неурядовими організаціями та експертним співтовариством в питаннях прогнозування та аналізу «гібридних» загроз, активно використовувати їхній потенціал для протидії означеним загрозам, розробивши механізм залучення та мотивації експертів.

6. Необхідно продовжувати зусилля щодо поглиблення взаємодії всередині розвідувального співтовариства. Необхідно вдосконалювати способи оцінки та корегування роботи розвідувальних органів, зокрема через механізми парламентського контролю.

7. Координація зусиль, як на національному, так і на міжнародному рівні залишається серед пріоритетних завдань. Дублювання функцій, ресурсів, відсутність співпраці та обміну інформацією з партнерами та іншими відомствами веде до небажаної конкуренції замість узгодженості дій та мультиплікації зусиль.

8. Експертне вивчення та аналіз розважального контенту, як-то фільмів та телесеріалів. Необхідно більш детально дослідити, як саме медіа-продукція такого формату може використовуватись для інформаційних атак та маніпуляцій громадською думкою.

9. Вкрай важливим є приділення особливої уваги науковим дослідженням політичних, економічних, соціальних, демографічних, етноконфесійних проблем Російської Федерації, розвитку поточної політичної ситуації. У більшості західних країн, як і в Україні, все ще бракує ґрунтовних досліджень, які б давали чітке та комплексне розуміння поточних політичних та економічних процесів в Росії. Крім того, переважають фахівці в сфері «радянських» досліджень, що не дає адекватного розуміння ситуації та логіки прийняття рішень, яка змінилась за останні роки порівняно з часами СРСР, незважаючи на певну спадкоємність.

10. Вирішальним є довготривалий процес розбудови стійкості держави та суспільства щодо гібридних загроз, їхня моральна та технічна готовність, а також внутрішні реформи та перетворення в країні, які будуть сприяти мінімізації можливостей використання слабких місць суспільства та політичної системи. Подолання внутрішніх розколів та протиріч, з метою недопущення їх використання в інформаційних атаках є важливим елементом стійкості суспільства.

11. Забезпечення умов для обміну досвідом між Україною та країнами-партнерами у сфері боротьби з російською пропагандою та інформаційними впливами також залишається пріоритетним. Україна як держава, що має краще розуміння специфіки сучасної російської дезінформації, таким чином може отримати можливість практичного зближення з Альянсом в одній з найбільш актуальних для нього сфер.

12. Північноатлантичний Альянс, як і Україна, залишається серед пріоритетних мішеней російських інформаційних операцій. Серед іншого формується образ ворога в сусідніх з НАТО країнах, тому необхідно спільно організувати протидію подібним операціям, а також просувати позитивний імідж та підвищення обізнаності широкої громадськості щодо діяльності НАТО, принципів та цінностей його функціонування.

У військово-політичній сфері:

1. Створити та забезпечити функціонування міжнародної експертної мережі (потенційно на базі платформи Україна-НАТО), покликаної виробити комплексну стратегію протидії гібридній агресії.

2. Запровадити моніторинг безпекової ситуації в окремих регіонах країн Європи в рамках формування специфічних індексів безпеки та, на їхній основі, – розробити систему раннього попередження та знешкодження певних дестабілізуючих тенденцій в регіонах, які можуть стати джерелом для розвитку російської гібридної агресії.

3. Забезпечити стійкий моніторинг ситуації з безпекою на Чорному та Азовському морях, зокрема йдеться про запобігання військовим інцидентам і напруженості, а також створити спеціалізований форум для військово-морського флоту (використовуючи досвід і модель Венеціанського форуму) для обговорення подій і ризиків в регіоні.

4. Розробити комплексну та всебічну прогностичну модель, базовану на прикладі конфлікту на сході України, яка допомогла б визначити методику запобігання гібридним актам агресії на різних етапах для формування безпекової політики держав щодо «заморожених» або потенційних конфліктних ситуацій.

5. Включити елементи гібридної агресії у всі сценарії військових навчань, як національного, так і міжнародного рівня та для всіх видів і родів військ, а також інших служб та відомств, які відповідають за надзвичайні ситуації.

6. Україні важливо відновити діяльність Комітету у справах розвідки, який має стати основним органом, що здійснює координацію діяльності розвідувальних служб, планування розвідувальних операцій, надання рекомендацій РНБОУ відносно реагування на «гібридні» загрози.

7. У сфері діяльності органів розвідки покращити принципи роботи з агентурою, як всередині країни, так і назовні, зробивши ставку на матеріально та морально мотивованого агента.

8. Вдосконалити критерії оцінки ефективності роботи співробітників розвідувальних служб та агентів.

9. Ініціювати створення євроатлантичної групи експертів високого рівня з питань розвідки, чиєю сферою дослідження будуть елементи гібридної війни, й залучити до неї також представників недержавних установ, колишніх співробітників спецслужб, які мають відповідні знання та досвід.

10. За умови успішного проведення реформ для набуття членства в Альянсі, та за наявності відповідного консенсусу в НАТО, Україна може стати потужним союзником, що має значний військовий потенціал і неоціненний практичний досвід, зокрема, і в сфері боротьби з гібридними загрозами.

У сфері кібербезпеки:

1. Стабільність глобального кіберпростору повинна базуватися на трьох стовпах:

   a. застосування вже наявних норм міжнародного права, включаючи Статут ООН, та чітке визнання кіберпростору рівноправним театром військових дій;

   b. вироблення норм відповідальної поведінки держав в інформаційній та кіберсфері;

   c. розробка заходів зміцнення довіри (confidence-building measures) в кіберпросторі.

2. Партнерство з бізнесом, зокрема, IT-компаніями. У держави не завжди вистачає ресурсів, щоб самостійно протидіяти кібератакам, ефективно розвивати системи захисту інформаційної та критичної інфраструктури. Крім того, повинні бути створені умови для підвищення власної відповідальності за безпеку з боку приватних компаній, навчання співробітників та співробітництво в цій сфері з органами державної влади.

3. Налагодження співпраці з інтернет-гігантами (Twitter, Facebook, Google тощо) для виявлення та блокування поширення дезінформації, дій, спрямованих на розпалювання ворожнечі та ненависті у суспільстві.

4. Важливим елементом є розробка механізму запровадження санкцій за використання кібератак. Необхідна чітка позиція міжнародної спільноти, аби покінчити з відчуттям безкарності в кіберсфері, саме тому повинні бути запроваджені механізми відплати за зловмисну кіберповедінку.

5. Публічне оприлюднення даних про виконавців та замовників кібератак є дієвим інструментом впливу на поведінку агресора, який сприятиме зменшенню загроз; в короткостроковій перспективі агресор може припинити кібероперацію, а у довгостроковій – взагалі відмовитись

від подальшого застосування кібероперацій.

6. Посилення спроможностей держави, зокрема сектору безпеки та оборони, у кіберпросторі. Серед можливих варіантів: створення волонтерських груп для відповіді на надзвичайні ситуації та масовані кібератаки, створення платформ партнерського обміну інформацією між приватними та державними структурами у сфері кібербезпеки, постійне підвищення кваліфікації фахівців з кібербезпеки у складі державних структур.

Автори:

Валерій Борис, Патронатна служба Апарату Верховної Ради України

Сергій Герасимчук, Рада зовнішньої політики «Українська призма»

Валерій Кравченко, к.істор.н., Національний інститут стратегічних досліджень

Артем Филипенко, Національний інститут стратегічних досліджень

Олександра Цехановська, Група з аналізу гібридних загроз Українського кризового медіа-центру

Ганна Шелест, к.політ.н., Рада зовнішньої політики «Українська призма»

За редакцією Ганни Шелест, к.політ.н., Рада зовнішньої політики «Українська призма», UA: Ukraine Analytica

Рецензенти:

Єгор Аушев, к.фіз-мат.н., Hacken, Cyber School

Любов Цибульська, Група з аналізу гібридних загроз Українського кризового медіа-центру

Оксана Осадча, к.політ.н., консультант

Сергій Данилов, Центр близькосхідних досліджень

ЕВРОПА
УКРАЇНА
ЄВРОПА

ОФІС ВІЦЕ–ПРЕМ'ЄР МІНІСТРА З ПИТАНЬ ЄВРОПЕЙСЬКОЇ ТА ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ УКРАЇНИ

ЕВРОПА
НАТО
УКРАЇНА

УРЯДОВИЙ ОФІС КООРДИНАЦІЇ ЄВРОПЕЙСЬКОЇ ТА ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ