ВПЛИВИ У ЦИФРОВОМУ ПРОСТОРІ:

ЯК ЄВРОПА ШУКАЄ СВІЙ ШЛЯХ ПРОТИДІЇ ТА ЩО МОЖЕ ЗАПОЗИЧИТИ УКРАЇНА?

ПРЯМУЄМО РАЗОМ
МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ
УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

УДК 32.019.51+327.8:004

Електрона версія: ufss.com.ua

Безверха А.О., Дубов Д.В., Каздобіна Ю.К., Шулімов С.Ф.
Аналітичний звіт «Впливи у цифровому просторі: як Європа шукає свій шлях протидії та що може запозичити Україна?»
Висловлюємо подяку Баровській А.В., Дубовій С.В., Мельник І.В., Петрову В.В. та Петровій І.В. за підтримку та консультування.
ISBN 978-617-7315-48-2

Присвячено проблемі протистояння зловмисному іноземному впливу на вибори та громадську думку. Проаналізовано відповідь на виклики сучасних гібридних конфліктів ЄС, НАТО та цифрових платформ. Показано, що ситуація в ЄС та Україні схожі як у відносинах з Інтернет платформами, так і щодо багаторівневого протистояння США та Китаю у сфері технологій та пов'язаних з ними процесів. Так само, як і для значної кількості країн Європи, Росія є найбільшою загрозою національній безпеці України. Розраховано на державних службовців, аналітиків та широкий загал.

Матеріал підготовлено за підтримки Європейського Союзу та Міжнародного Фонду «Відродження» в межах грантового компоненту проєкту EU4USociety. Матеріал відображає позицію авторів і не обов'язково відображає позицію Міжнародного фонду «Відродження» та Європейського Союзу».

Європейський Союз складається з 27 держав-членів та їхніх народів. Це унікальне політичне та економічне партнерство, засноване на цінностях поваги до людської гідності, свободи, рівності, верховенства права і прав людини. Понад п'ятдесят років знадобилось для створення зони миру, демократії, стабільності і процвітання на нашому континенті. Водночас нам вдалось зберегти культурне розмаїття, толерантність і свободу особистості. ЄС налаштований поділитись своїми цінностями та досягненнями з країнами-сусідами ЄС, їхніми народами, та з народами з-поза їхніх меж.

Міжнародний фонд «Відродження» – одна з найбільших благодійних фундацій в Україні, що з 1990-го року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проектів, до реалізації яких долучилися понад 60 тисяч активістів та організацій України на суму понад 200 мільйонів доларів США. Сайт: www.irf.ua

ISBN 978-617-7315-48-2 **УДК 32.019.51+327.8:004**

Аналітичний звіт

ВПЛИВИ У ЦИФРОВОМУ ПРОСТОРІ: ЯК ЄВРОПА ШУКАЄ СВІЙ ШЛЯХ ПРОТИДІЇ ТА ЩО МОЖЕ ЗАПОЗИЧИТИ УКРАЇНА?

Друкується в авторській редакції

Формат - А5

Верстка: ТОВ «Інтерконтиненталь-Україна»

ЗМІСТ

ВСТУП

Інтеграція України до Єдиного цифрового ринку Європейського Союзу є одним із головних пріоритетів секторальної інтеграції з ЄС. Вона передбачає широке застосування та доступ до інформаційно-комунікаційних технологій для якомога ширшого кола громадян. Як свідчить досвід демократичних країн, рух у цьому напрямку має, як позитивні, так і негативні наслідки. З одного боку – він створює можливості для комунікації, торгівлі та економічного розвитку, а з іншого – цифрове середовище є полем багаторівневого міждержавного протистояння, яке впливає на баланс сил на міжнародній арені, стирає межі між війною та миром, а також трансформує сферу медіа та масової комунікації.

Публічний обмін думками та інформацією є одним з ключових елементів демократичного устрою. Саме під час такого обміну громадяни демократичних країн формують свою думку, а потім приймають рішення на виборах та референдумах. Обрані ж особи керують країною відповідно до волі громадян та згідно з процедурами та повноваженнями, визначеними у законі. Явище, відоме під різними назвами, як то «політична війна», «інформаційна війна», «активні заходи», «гібридна агресія» та інше, яке полягає у втручанні зловмисних зовнішніх гравців у внутрішньополітичні процеси інших країн з метою отримання бажаного результату через вплив на громадську думку набуває все більшої ваги завдяки поширенню та розвитку інформаційно-комунікаційних технологій.

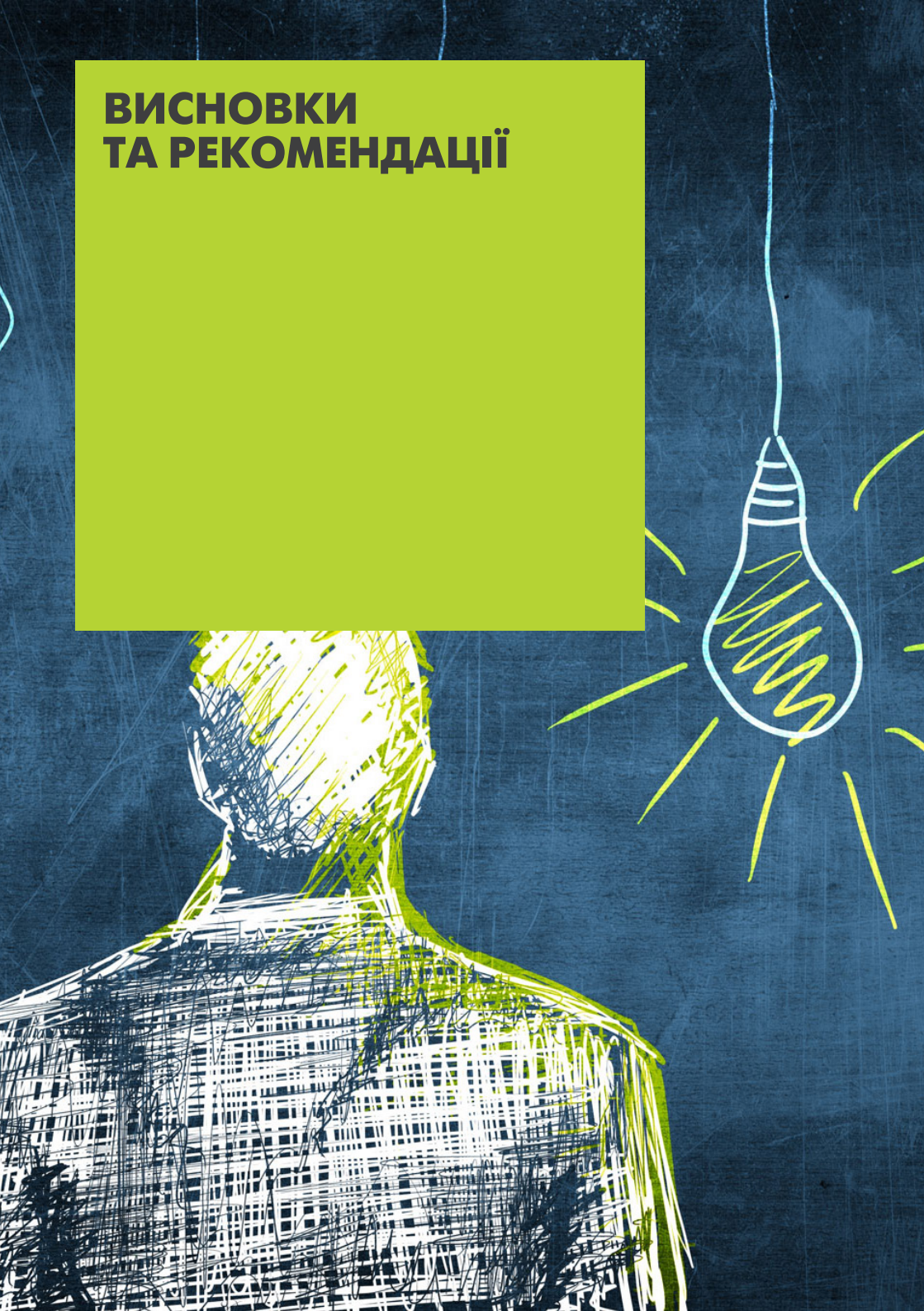
Серед іншого, складність реагування на такі зловмисні дії полягає у тому, що сфера масової комунікації, в якій часто здійснюється таке втручання, знаходиться між сферами відповідальності безпекових відомств, на які розділено урядування в Західних країнах, а деякі гравці, такі як платформи, фізично знаходяться поза їх юрисдикцією. Публічний інформаційний простір демократичних країн є майже вільним від силового втручання державної влади, як сфера, в якій має відбуватися вільний обмін думками громадян. В той же час, публічний інформаційний простір фактично став одним з доменів, в якому здійснюється протистояння та просування власних інтересів держав, що останнім часом описується нейтральним терміном «стратегічні комунікації», не останню роль в яких відіграють непублічні дії

та контрдії спеціальних служб, відомі, як спеціальні інформаційні операції, активні заходи, психологічні та інформаційно-психологічні операції, операції сприяння, спеціальні заходи впливу тощо.

Більше того, загроза постійно еволюціонує. В той час як наміри та підходи гравців, які намагаються чинити вплив вивчені та досліджені, але медійне та інформаційне середовище, інструменти та засоби впливу постійно змінюються. Розширюється також і коло тих, хто бере інструментарій впливу на озброєння. Намагання протистояти зовнішньому впливу вже охрестили грою «піймай крота» (whack-a-mole), тобто у відповідь на захисні дії відбуваються певні процеси або дії противника, які призводять до нових, часто непередбачуваних викликів.

Мета цього звіту – вивчити та проаналізувати європейський досвід протидії та його реагування на втручання у внутрішні процеси демократичних країн та запропонувати рекомендації до Стратегії інформаційної безпеки, над якою сьогодні працює Уряд України.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ



ВИСНОВКИ

Значна кількість світових тенденцій останнього часу стали наслідком стрімкого розвитку цифрових інформаційно-комунікаційних технологій. Серед них трансформація поняття «війна» та перехід від чіткого розділу на мирний та воєнний час до безперервного та неунормованого протистояння із застосуванням переважно невійськових засобів. Саме у цьому контексті ЄС та інші демократичні країни все більше розглядають необхідність протистояти зловмисному іноземному впливу на вибори та громадську думку. І хоча сьогодні в Європі ще не вироблено остаточне розуміння механізму протидії, «захист демократії» визначено основним завданням, а повага до прав і свобод громадян – основним принципом.

Європейський досвід є актуальним для України не тільки тому, що Україна має на меті інтеграцію до ЄС, а й тому, що західний підхід базується на емпіричному вивченні проблеми та аналізі ефективності запроваджуваних заходів. Ситуація ЄС та України також схожі як у відносинах з інтернет платформами, так і у ситуації багаторівневого протистояння США та Китаю в сфері технологій та пов'язаних з ними процесів. Можливість України впливати на політику платформ одноосібно є значно обмеженою, а її місце на світовій мапі технологій не дозволяє їй бути впливовим самостійним гравцем, отже вона також змушена буде зробити вибір між двома конкуруючими системами. Так само, як і для значної кількості країн Європи, Росія є найбільшої загрозою національній безпеці України.

Відкритість публічної сфери західних суспільств, у поєднанні з економічною глобалізацією, вільним пересуванням через кордони та можливістю прямого доступу до громадян за допомогою транскордонних інформаційно-комунікаційних технологій, зробила їх вразливими до зовнішнього втручання. Інтернет-платформи, які до подій виборів у США 2016 на Заході сприймались переважно, як інструмент звільнення від авторитарного правління, стали знаряддям дестабілізації демократичних країн з боку Російської Федерації. Інформаційно-психологічна складова російських операцій стала несподіванкою для західних фахівців з інформаційної безпеки, адже їх підхід на той момент вбачав загрозу лише у шахрайстві та втручанні у технічну складову.

ЄС, НАТО та цифрові платформи, чия відповідь на виклики сучасних гібридних конфліктів стала предметом цього дослідження, є різними за своїми функціями, мотиваціями та інструментарієм. Відповідно, їх погляд на проблему та можливості реагу-

вання відрізняються. В той час, як НАТО є військово-політичним союзом, чиї фахівці найкраще обізнані у темі переходу до гібридних методів ведення війни, він не має законодавчих та правозастосовних функцій, необхідних для адаптації до відповідних змін. ЄС такі функції має, але еволюція його розуміння проблеми та підходу до її вирішення відбувається доволі повільно та виходить з принципу якомога меншого державного втручання в інформаційну сферу. Можливості такого втручання також є обмеженими. Платформи, які стали потужними транскордонними гравцями, формулюють проблему саме, як протидію операціям впливу та мають найбільше можливості регулювати процеси, але часто не мають мотивації, а легітимність їх рішень та універсальність правил під значним питанням.

Транскордонна природа гібридних загроз означає, що відповідь не може бути дана лише на рівні окремих держав і потребує міжнародної координації та співпраці. Разом з тим, той факт, що агресори таргетують також і вразливості окремих держав, зумовлює необхідність розвивати власний інструментарій захисту. Велика кількість інструментів, застосовуваних при операціях впливу, а також, можливість застосовувати їх одночасно для підсилення їх ефективності, означає, що заходи необхідно вживати не лише в інформаційній сфері.

На сьогодні дії ЄС та європейських країн мають переважно захисний характер. Не існує ані усталеного підходу до протидії новітнім загрозам, ані чітко визначеної термінології. Поступово з ужитку виходить поняття «фейк ньюз», є чітке розуміння необхідності розрізняти ненавмисне та цілеспрямоване розповсюдження недостовірної інформації, є розуміння, що сьогоднішня діяльність РФ є продовженням радянської практики «активних заходів», адаптованих до нових умов, все більше акцентується координація дій зловмисних акторів в інформаційному просторі, як ознака операцій впливу. Розрізняють також незаконний контент та «законний, але шкідливий». Акцентується складність реагування через перетворення мирних засобів на зброю та викривлене розуміння поняття «м'яка сила» з боку РФ та її колег по авторитарному табору.

Серед засобів протидії, які вживають в ЄС – розвиток стратегічних комунікацій, розвиток інструментів публічної дипломатії, посилення спроможності у виявленні, аналізі та викритті недостовірної інформації, співпраця з приватним сектором, покращення комунікації з громадським сектором, розвиток соціальної стійкості, розвиток мережі фактчекерів та сприяння якісній

журналістиці, академічний аналіз дезінформаційних кампаній, навчання та поширення знань про дезінформацію. Європейський підхід також пов'язаний зі зміцненням кібербезпеки. План дій щодо демократії також визначив поняття операцій впливу та зовнішнього втручання в інформаційний простір та поставив завдання розробити більш рішучу відповідь на них, включаючи заходи стримування, які мають на меті змусити учасників операцій впливу та зовнішнього втручання заплатити достатньо високу ціну за свої дії.

І хоча відповідь ЄС має багато вимірів, Інтернет є одним з ключових елементів, якому приділяється увага. На відміну від США, ЄС все далі відходить від бачення Інтернету, як простору, вільного від державного втручання. Ще в 2017 році було прийнято рішення, що контент, який є нелегальним оффлайн, має також бути нелегальним онлайн. ЄС також вважає, що соціальні мережі, які надали нової якості явищу дезінформації, мають нести більшу відповідальність. Запровадження добровільного Кодексу практик щодо дезінформації було визнано недостатньо ефективним заходом і сьогодні ЄС працює над Законом про цифрові послуги, який має задати рамку більшої прозорості та підзвітності платформ.

НАТО розглядає проблему в контексті протидії «гібридній війні», під якою розуміють тактику, яка складається із пропаганди та дезінформації, методів економічного тиску, а також таємного використання сил спеціального призначення. Протягом відносно короткого проміжку часу Альянс спромігся оцінити нову загрозу та відпрацювати, принаймні на політичному рівні шляхи протидії їй. Йдеться, зокрема, про можливість прийняття Північноатлантичною радою НАТО рішення про приведення у дію статті 5 Вашингтонського договору для протидії гібридній війні у рамках колективної оборони.

У протидії гібридним загрозам НАТО визначило основним своїм партнером структури Європейського Союзу, тобто НАТО, як військово-політична організація продовжуватиме й надалі протидіяти, насамперед, жорстким викликам безпеки, ЄС же відповідатиме за протидію «м'якій силі». В НАТО працюють над концепцією стійкості, яка поступово інтегрується у безпековий дискурс європейських та інших демократичних країн. Стійкість країн ЄС та НАТО великою мірою залежить від безпеки важливих інформаційних систем, сталого функціонування критично-важливих послуг (публічні послуги, енергопостачання, банківські послуги тощо) та суспільно-політичної стабільності. НАТО також приділяє

значну увагу розвитку стратегічних комунікацій, розвідувальній діяльності, обміну розвідувальною інформацією, детальному вивченню загрози, просвіті відповідальних за розробку та впровадження політики, розробленню набору індикаторів раннього попередження для опрацювання різних варіантів реагування на кризові ситуації.

Соціальні мережі та їх суспільне сприйняття пройшли значну еволюцію від інструментів звільнення, від автократії та надання можливості висловитися упослідженим спільнотам до цензорів, та інструментів іноземного впливу. Урядові та неурядові організації стверджують, що на сьогодні техгіганти мають надто велику владу над політичною дискусією в демократичних країнах, що без належного мандату, процедури та підзвітності громадян становить ризик для демократичного розвитку. Намагання зменшити їх владу та врегулювати їх діяльність залишатиметься викликом для демократичних країн.

Не менший ризик становить використання соціальних мереж з метою впливу та маніпуляцій громадською думкою. Саме протидії операціям впливу на платформах було присвячено багато уваги соцмереж після виборів Президента США 2016 року. На додачу до фактчекінгу, та збільшення прозорості реклами, Facebook одразу звернув увагу на те, що під час операцій впливу розповсюджують не лише недостовірну інформацію, а й інші види висловлювань та обрав координацію дій та намагання ввести користувачів в оману щодо особи розповсюджувача, як критерія обмеження такої діяльності. З тією самою метою блокувалися і фейкові аккаунти.

Контраверсійною була і залишається політика платформ щодо модерування контенту, яка є переважно непрозорою, автоматизованою, її правила постійно змінюються, а користувач часто не має можливості оскаржити рішення компаній. Також під питанням залишається здатність платформ запроваджувати власну політику, як через неефективність вживаних ними заходів, так і через винахідливість агентів впливу, які знаходять шляхи обходу заборон та обмежень.

Пандемія COVID та події виборчої кампанії в США 2020 року, кульмінацією яких став напад на Капітолій 6 січня змусили технічні компанії переглянути свою політику в бік більш жорстких заборон. З платформ було прибрано акаунти Президента Трампа та декількох його прибічників, які продовжували розповсюджувати недостовірну інформацію, незважаючи на результати фактчекінку та правила платформ. Такі рішення залишаються кон-

троверсійними та переважно неприйнятними для Європейських країн, адже ці компанії знаходяться поза їх юрисдикцією, і правила ухвалення ними подібних рішень щодо громадян та політиків європейських країн та України лишаються не встановленими, що несе ризики для суспільно-політичних процесів всередині наших країн. Процес осмислення подій 2020 року продовжується. Серед інших документів, цікавим для вивчення є звіт Election Integrity Partnership, які відслідковували процеси розповсюдження інформації та вивчали реакції платформ у реальному часі.

Більш детальне дослідження політик соціальних мереж у відповідь на операції впливу та розповсюдження недостовірної інформації може стати підґрунтям для дискусії щодо законодавчого врегулювання протидії операціям впливу, адже вони формулювали проблему саме, як операції впливу (не дезінформація), а також, мали можливість запроваджувати політики та правила, і тестувати їх ефективність у реальному часі, швидко вносячи необхідні, на їх думку, зміни. Вони виступали у ролі квазідержав, які мають весь необхідний інструментарій.

Українські підходи, запропоновані в Стратегії інформаційної безпеки, багато в чому співпадають з європейськими. Зокрема, в частині необхідності розвитку стратегічних та кризових комунікацій, регулювання ринку масової комунікації, саморегулювання журналістської спільноти, захисту журналістів та розвитку незалежної журналістики, підвищення рівня медіакультури та медіаграмотності суспільства.

Разом з тим, Стратегія приділяє недостатньо уваги транскордонній природі загрози, акцентує розповсюдження дезінформації та необхідність протидіяти розповсюдженню інформації, яка заборонена законом, а не скоординовану діяльність, мета якої ввести громадянина в оману, на яких акцентують європейські полісімейкери та соціальні мережі. Разом з тим, їх підхід видається більш продуктивним з точки зору виявлення зловмисного впливу та менш загрозливим для індивідуальної свободи слова.

РЕКОМЕНДАЦІЇ

Виходячи із зазначеного вище, пропонуємо внести такі зміни до проекту Стратегії інформаційної безпеки України, яку сьогодні розглядає український уряд:

1) Врахувати підхід Європейського Союзу щодо необхідності захисту демократії від зловмисного впливу та викласти мету Стратегії інформаційної безпеки України у такій редакції

«Метою Стратегії є зміцнення національної безпеки України шляхом стримування та протидії загрозам в інформаційній сфері, спрямованим проти реалізації життєво важливих інтересів громадянина, суспільства та держави, на підрив державного суверенітету і територіальної цілісності України, втручання та зловмисний вплив на демократичні процеси, порушення права громадян на демократію».

2) Доповнити розділ «Загальні положення» термінами «спеціальна інформаційна операція» та «іноземне втручання в інформаційний простір», аналогічними за змістом термінам з Європейського плану дій щодо демократії. Визначити їх наступним чином: Спеціальна інформаційна операція – це скоординовані зусилля вітчизняних або іноземних суб'єктів впливу на цільову аудиторію з використанням оманливих засобів, включаючи придушення незалежних джерел інформації у поєднанні з дезінформацією; Іноземне втручання в інформаційний простір – це дії, які спрямовано здійснюються іноземною державою або її агентами, які протирічать визначеним національним інтересам України та мають на меті порушити процес вільного формування та вираження її громадянами своєї політичної волі шляхом залякування або введення їх в оману.

3) Визначення терміну «стратегічний наратив» викласти у такій редакції: стратегічний наратив – це сукупність офіційно закріплених пріоритетів національних інтересів України, основних напрямів державної політики у сфері національної безпеки та завдань суспільного розвитку, визначених Стратегією національної безпеки України.

4) Рекомендувати врахувати досвід соціальних мереж, а саме в частині протидії скоординованій діяльності та порушення правил платформ при розробці національного законодавства з протидії дезінформації та операціям впливу.

5) Визначити забезпечення суспільного нагляду та контролю за діями силових структур в інформаційній сфері, як один з напрямків удосконалення нормативно-правової бази в інформаційній сфері.

6) Унормувати проведення періодичної оцінки ефективності запроваджених заходів протидії операціям інформаційного впливу та діяльності Центру протидії дезінформації при РНБО.

7) Акцентувати стійкість суспільства та держави до деструктивних інформаційних впливів, як необхідну умову для забезпечення інформаційної безпеки, визначити формування такої стійкості стратегічною ціллю Стратегії.

8) Визначити, що стійкість розвивається, серед іншого, і шляхом підвищення рівня довіри громадян до державних інституцій та правоохоронних органів, та акцентувати необхідність розвитку інструментів «зрозумілої мови» в державному управлінні з метою забезпечення належного сприйняття державних рішень, процесів вироблення політик та налагодження ефективного діалогу з громадськістю.

9) Визначити координацію дій України з міжнародними партнерами у сфері протидії зловмисним впливам та управління інтернетом, як одну зі стратегічних цілей Стратегії.

10) Запровадити системний підхід до розбудови комунікативних спроможностей держави, що охарактеризувати у відповідному розділі Стратегії.

11) Підрозділи, присвячені інформаційній реінтеграції мешканців окупованих територій та утвердження позитивного іміджу України виключити як такі, що розкриті у відповідних тематичних стратегіях, а саме Стратегії реінтеграції тимчасово окупованих територій та Стратегії публічної дипломатії відповідно.

ГЛОБАЛЬНИЙ ЦИФРОВИЙ КОНТЕКСТ СУЧАСНИХ ОПЕРАЦІЙ ВПЛИВУ:

НОВІ ГРАВЦІ, НОВІ ВІДНОСИНИ, СТАРІ ПРОБЛЕМИ

РОЗДІЛ 1

1. ГЛОБАЛЬНИЙ ЦИФРОВИЙ КОНТЕКСТ СУЧАСНИХ ОПЕРАЦІЙ ВПЛИВУ: НОВІ ГРАВЦІ, НОВІ ВІДНОСИНИ, СТАРІ ПРОБЛЕМИ

Цифрова інформаційна сфера сьогодні являє собою поле боротьби та конкуренції на багатьох рівнях, від міжнародного до внутрішньополітичного. Її характеризує, як загострення старих протистоянь, так і поява нових викликів, зумовлена зміною економічного та безпекового балансу, а також, поява нових потужних гравців.

Протиборство США та КНР формує ключовий наратив сучасних міжнародних відносин. Різні моделі суспільно-політичного устрою, діаметрально протилежні бачення моделі управління глобальною мережею Інтернет та відмінні підходи до використання новітніх технологій у різних сферах політичного та суспільного життя – все це створює простір напруженості та суперництва між цими геополітичними гравцями, маючи істотний вплив на інші світові держави всіх рівнів. Китай не лише складає конкуренцію США у багатьох сферах, він ставить собі завдання домінувати та залучати на свій бік країни, які на сьогодні є партнерами США.

Протистояння сьогодні відбувається на тлі розчарування функціонуванням демократичних інституцій[1] та зростання популярності китайської економічної моделі. Протягом останніх 50 років Китай продемонстрував небачені темпи економічного розвитку. Як результат, він поступово піднімається в індексі м'якої сили, в той час, як США втрачає свої позиції. Розрив між ними все ще складає 25 пунктів, але останніми роками він скорочується.[2]

Швидкі темпи економічного розвитку дозволяють КНР виступати з глобальними економічними ініціативами. Наймасштабніша серед них – «Один пояс, один шлях», що має за мету побудувати морський та сухопутний торгівельний шляхи між Азією та Європою. Ініціатива має і цифрову складову, яка полягає у побудові мережі транскордонних магістральних кабелів та просуванні власних технологій до країн регіону, які проходять через цифрову трансформацію. Робота у цьому напряму дозволяє КНР, яка переважно покладається на державні або контрольовані державою приватні компанії, створювати цифрову залежність від себе та своїх технологій через побудову власних мереж.

1. https://www.pewresearch.org/fact-tank/2020/02/27/how-people-around-the-world-see-democracy-in-8-charts/
2. https://softpower30.com/

Просування власних технологій має не лише економічну складову. Як зазначають дослідники цієї тематики, технології та технічні стандарти також мають юридичний, політичний та дискурсивний компоненти.[3] Цікавим з точки зору конкуренції США та Китаю є саме дискурсивний елемент.

Дизайн технологій дуже часто відображає етичний або ціннісний підхід їх розробників. Як приклад, в конкуренції технологій бездротової локальної мережі переміг Wi-Fi, який став міжнародним стандартом. Його конкурент WAPI програвав йому за приватністю, але вигравав за ефективністю. Отже, вибір однієї технології перед іншою мав ціннісну та етичну складову. Подібний вибір стояв перед міжнародними організаціями зі стандартизації, коли в травні 2020 китайська компанія Huawei запропонувала прийняти нові стандарти Інтернет протоколу. У разі прийняття китайського стандарту, було б значно розширено технічні можливості держави в Інтернеті, і держава мала б набагато більшу роль у розробці технічних стандартів.[4]

Просування власних стандартів має стосунок і до конкуренції моделей управління інтернетом, яка триває на міжнародній арені. З одного боку лежить модель мультистейкхолдеризму та відкритого інтернету без кордонів, яка існує на сьогодні, з іншого – суверенітет держави над своїм інформаційним простором з правом регулювати доступ до нього із зовні та фільтрувати всередині. Тут, на одному боці виступає США, які відстоюють модель мультистейхолдеризму, а на іншому – Китай та РФ. На підтримку своєї позиції Китай мобілізує країни Африки та інші країни, де він присутній завдяки ініціативі «Пояс і шлях».

Конкуренція між цими моделями та підходами у цифровій інформаційній сфері становить значний виклик для європейських країн, адже мережеві ефекти часто не дають можливості перебувати в обох системах одночасно. Європа постала перед значним викликом в технологічній сфері і європейські експерти зазначають, що на сьогодні вона швидше поле бою, аніж самостійний гравець. Тільки одна з 20 найбільших технологічних компаній світу є європейською (Німеччина). На ринку домінують американські та китайські фірми.[5]

Наполягання США, що у конкуренції технологій Європа має обирати між США та Китаєм на користь США створює напруженість у стосунках. А ініціатива «Чиста мережа» щодо розвитку мереж 5G, яку в останній рік президентства Дональда Трампа

3. https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/2021/ui-brief-no.-1-2021.pdf
4. https://jamestown.org/program/huaweis-global-advancement-of-alternative-internet-protocols/
5. https://www.forbes.com/top-digital-companies/list/#tab:rank

оголосив Держсекретар Помпео, не має одностайної підтримки в Європі. Якщо Британія приєдналася до цієї ініціативи США, то Франція та Німеччина продовжують внутрішні дебати і лише обіцяють приєднатися. Деякі країни західних Балкан не зробили жодного кроку в цьому напрямку.[6]

Між Європою та США також існує непорозуміння у сфері оподаткування тих гігантів, які отримують прибутки на місцевих ринках, а податки платять у США. У багатьох країнах вони присутні лише у віртуальному просторі, але займають велику частку рекламного ринку, чим підривають доходи традиційних ЗМІ. За адміністрації Трампа багатосторонні переговори зайшли у глухий кут, і США з них вийшли. Європейські країни почали запроваджувати податок в односторонньому порядку. В квітні 2021 адміністрація Байдена виступила з ініціативою, яка має збалансувати різні підходи, і досягнення домовленостей виглядає більш реальним.[7]

Значним гравцем, переважно деструктивного характеру, залишається Росія, чиє бачення суспільних відносин та управління інформаційною сферою є ближчим до китайських практик, але яка не має співмірної з Китаєм глобальної ваги. Внутрішню політику РФ та Китаю в інформаційній сфері на Заході часто характеризують, як «повзучий авторитаризм», коли технології використовуються державою для того, щоб контролювати громадян. У боротьбі за зміну глобальної системи управління Інтернетом зі свого боку РФ також залучає власні позиції впливу у Латинській Америці, Африці, та частково в Європі, для підтримки вказаного підходу. Водночас спроби РФ вирішити завдання «суверенізації» є лише обмежено вдалими.[8] Разом з тим, Росія має значні потужності у кіберсфері, які регулярно застосовує проти США та країн Європи.[9] І хоча кібератаки не стали «цифровим Перл Харбором», як колись попереджав Міністр оборони США Леон Панетта, РФ активно використовує свій кіберарсенал в операціях політичного впливу, щодо яких у неї існує розвинена доктрина з глибоким історичним корінням.

Росія та Китай також працюють, щоб підірвати демократію в Європейських країнах. І хоча не йдеться про навмисну координацію зусиль, кожна з них використовує власні інстру-

6. https://www.rferl.org/a/which-european-countries-support-the-5g-clean-network-initiative-/30928122.html
7. https://www.bbc.com/news/business-56675225
8. https://www.washingtonpost.com/opinions/2021/02/01/russia-internet-rules-united-nations/
9. https://www.reuters.com/article/global-cyber-russia/explainer-russias-potent-cyber-and-information-warfare-capabilities-idUSKBN28T0ML

менти, що потім дає синергетичний ефект, в якому зусилля однієї країни підсилюють зусилля іншої. Як приклад, можна навести ситуацію в Сербії, де Росія втручається у вибори та політичні процеси звичними для неї засобами маніпуляції інформацією, а Китай надає кредити без додаткових умов, що сприяє корупції та іще більше підриває демократію. Подібні дії можна спостерігати і в країнах Європейського Союзу.[10]

Значну роль на міжнародній арені відіграють Інтернет платформи, які часто називають квазідержавами, через їх не підконтрольність переважній більшості урядів та здатність встановлювати та запроваджувати власні правила. Вони отримали значну владу через побудову широкої мережі користувачів, контроль над тим, яку інформацію вони споживають, позбавили традиційні ЗМІ важливого джерела доходів – реклами, і виступають у ролі модераторів обміну думками та інформацією, які майже не несуть відповідальності. Вони є непідконтрольними користувачам, а переважна більшість урядів не мають інструментів для притягнення їх до відповідальності. Також, вони змінюють динаміку суспільних відносин, надаючи громадянам не лише рупор та легкий доступ по широкої аудиторії, а й механізми легкої організації та мобілізації.

Як зазначає професор політології та філософії Стенфордського університету Роб Райх, соціальні мережі є інструментом, який дозволяє отримати доступ до публічного простору тим суспільним групам, які не мають його через традиційні ЗМІ. І якщо в авторитарних країнах такою групою переважно є політична опозиція, то в демократичних суспільствах це, як правило, різні маргінальні ідеології, теорії змови та інше. Ця особливість соціальних мереж спрощує завдання агентам зловмисного впливу, адже їм потрібно лише підсилювати тенденції, які вже існують.

Одночасно відбувається переосмислення поняття «війна», яке раніше переважно стосувалося збройного протистояння. «Всюдисущість інформації та темпи технологічних змін трансформують характер війни. Старі відмінності між «миром» та «війною», між «державним» та «приватним», між «іноземним» та «внутрішнім», а також між «державним» та «недержавним» все більше застарівають», - йдеться в Інтегрованій опе-

10. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS-Report-Russia-China-Alignment-final-v2.pdf

раційній концепції Британського Уряду 2025 року.[11] Російські теоретики наголошують на тому, що війна триває постійно, не починаючись і не закінчуючись: «На відміну від класичних дій в минулих війнах з дипломатичною нотою на початку війни і мирним договором в її кінці, сучасні війни ніколи не оголошуються і ніколи не закінчуються.»[12]

Нові методи ведення війни в кіберпросторі включають в себе як втручання в діяльність інформаційних систем, так і операції впливу на громадян демократичних країн та їх вибір. Питання застосування міжнародного гуманітарного права, або права війни до операцій у кіберсфері залишається неврегульованим. Можливості нових технологій та неповага до міжнародного права змінюють норми щодо ведення війни. Як приклад, міжнародне гуманітарне право забороняє атакувати цивільних, а операції впливу та кібератаки часто спрямовані саме проти цивільних. Розмивається поняття агресії, як через появу концепції активного захисту, так і через можливість діяти на території іншої країни в мирний час на допороговому рівні. Активну участь у конфліктах беруть недержавні гравці, що разом з технічними моментами ускладнює можливість визначити, хто саме здійснив атаку, і чи причетна до неї якась держава. Це, в свою чергу, ускладнює можливість стримування та притягнення до відповідальності, а допороговий характер таких дій стримує Західні країни, які з часів появи ядерної зброї діють в логіці уникання ескалації, від збройної відповіді на таку поведінку.

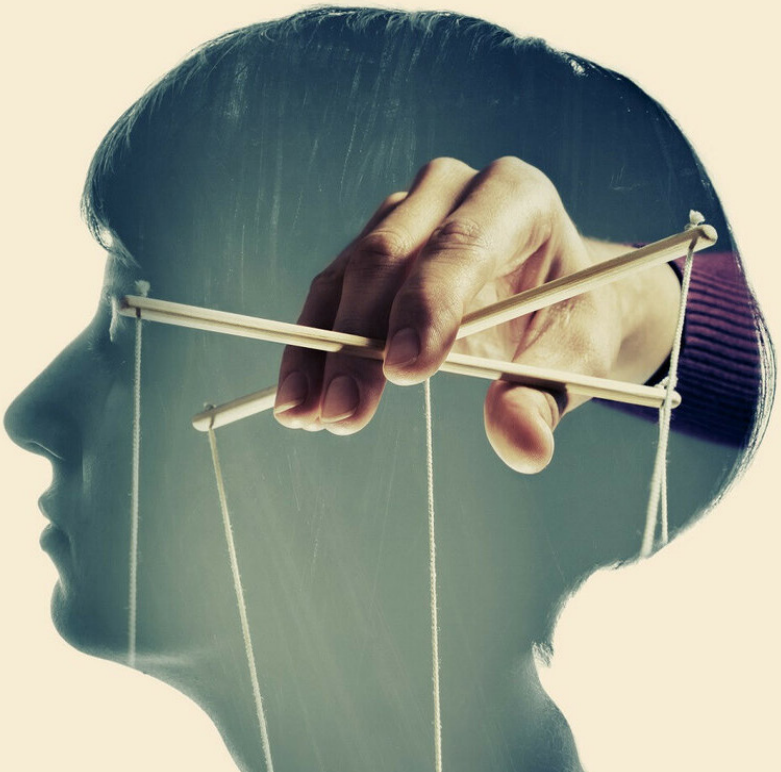
Цифровізація є довгостроковою тенденцією, вочевидь такі інновації, як 5G та штучний інтелект зроблять завтрашні ІТ-мережі ще більш уразливими, ніж сучасні. Оскільки авторитарні держави стають все більш справними в технологіях і дедалі більше стимулюють технологічні інновації, демократіям, серед яких сьогодні також Україна, необхідно критично оцінити вплив цих змін на різні аспекти суспільно-політичного життя. Європейським державам та інституціям доведеться мати справу не лише з фінансовими та регуляторними проблемами, які постануть з цією трансформацією, але й з потенціалом їх зловживання.[13]

11. https://www.gov.uk/government/publications/the-integrated-operating-concept-2025/the-integrated-operating-concept-2025-accessible-version#:~:text=The%20Integrated%20Operating%20Concept%202025%20sets%20out%20a%20new%20approach,military%20thought%20in%20several%20generations
12. https://vm.ric.mil.ru/Stati/item/222832/
13. https://www.gmfus.org/publications/european-policy-blueprint-countering-authoritarian-interference-democracies

ВПЛИВ НА ГРОМАДСЬКУ ДУМКУ ТА ЙОГО ІНСТРУМЕНТИ:

ТРАНСФОРМАЦІЇ КЛАСИЧНИХ ІНСТРУМЕНТІВ

РОЗДІЛ 2



2. ВПЛИВ НА ГРОМАДСЬКУ ДУМКУ ТА ЙОГО ІНСТРУМЕНТИ: ТРАНСФОРМАЦІЇ КЛАСИЧНИХ ІНСТРУМЕНТІВ

Сьогодні загальна загроза безпеці для Європи змінилася: супротивники рідше використовують звичайну військову силу для ведення геополітичних битв і частіше використовують асиметричні засоби для компенсації традиційних військових слабкостей. Ця діяльність є доволі різноманітною і, як правило, прихованою, що ускладнює вжиття контрзаходів. З одного боку, подальше вивчення інструментів впливу на громадську думку, їх каталогізація, поширення відповідних знань сприяють легшому виявленню деструктивної діяльності. З іншого боку, посиленню ефективності протидій зовнішньому впливу допомагатиме введення відповідних понять у правове поле, що дозволить фіксувати та попереджувати у майбутньому такі випадки.

2.1. Нормативно-правове визначення понять, як засіб протидії зовнішнім впливам

«Як урядам розмежовувати традиційно визнану військову та розвідувальну діяльність від втручання з використанням асиметричних інструментів, якщо немає визначення?» – порушують слушне питання експерти[1]. Без визначення політики можуть розглядати цю діяльність, як допустиму, навіть, якщо вона є небажаною, і відчувати себе обмеженими у вжитті заходів для захисту від неї. Натомість чітке визначення може окреслити межі допустимого та надати урядам інструменти для встановлення норм у цьому просторі.

Ситуацію ускладнює несформований політичний та науковий консенсус щодо того, що саме таке «втручання» і чим термін «втручання» схожий або відрізняється від інших суміжних понять таких, як «вплив». Відсутність загальної рамки «втручання» може не лише затримати або ускладнити ініціативи законодавців, а й негативно вплинути на зусилля громадянського суспільства щодо підвищення обізнаності та згуртування опозиції проти вторгнень у демократичні процеси. Водночас у порівнянні понять «втручання» та «інтервенція» є більше чіткості. Неоднозначний і некінетичний характер втручання ставить його твердо за рамки жорсткої сили. З тієї ж причини

1. https://securingdemocracy.gmfus.org/wp-content/uploads/2020/03/Conceptualizing-Foreign-Interference-in-Europe.pdf

«втручання» відрізняють від «інтервенції», оскільки значна частина літератури про інтервенцію описує той чи інший ступень військових дій[2].

У препринті, опублікованому Фінським інститутом міжнародних відносин (*Finnish Institute of International Affairs*, FIIA) у вересні 2019 року, Мікаель Вігелл (*Mikael Wigell*) використовує поняття «гібридне втручання» на позначення «невійськової практики для переважно прихованих маніпуляцій стратегічними інтересами інших держав». М. Вігелл чітко розмежовує його від гібридної війни, яка на думку автора є «військовим підходом до ведення «непрямої війни» за особливих обставин» [3].

Загалом термінологічний пошук розгортається за декількома напрямами:

- аналіз близьких за змістом понять, у т.ч. зовнішнє втручання, гібридне втручання, гібридні загрози, підривні дії, активні заходи, операції впливу, інформаційні операції, операції у кіберпросторі;
- аналіз відповідних родових понять: втручання, вплив, інтервенція;
- порівняння вживаних означень: «зловмисний» (англ. *malign*) чи «шкідливий» (англ. *malicious*); «іноземний» (англ. *external*), «зовнішній» (англ. *foreign*) та «третіх країн» (англ. *third country*) тощо.

Автори дослідження «Іноземне втручання в демократії: розуміння загрози та еволюція відповідей» переконані, що те, як ЄС визначить у правовій площині іноземне втручання, може мати значний вплив у майбутньому, оскільки глобальні демократії будуть розглядати європейське визначення, як стандарт[4].

Два питання, на які інші країни намагалися відповісти у своїх визначеннях втручання і, які могли б служити керівництвом для дискусій в ЄС, є такими:

- «як ми можемо ідентифікувати діяльність з втручання», що відкриває двері для розмови про намір або наслідки, і
- «чим втручання відрізняється від прийнятної поведінки»?[5]

2. https://securingdemocracy.gmfus.org/wp-content/uploads/2020/03/Conceptualizing-Foreign-Interference-in-Europe.pdf
3. https://www.fiia.fi/wp-content/uploads/2019/09/wp110_democratic-deterrence.pdf
4. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652082/EPRS_BRI(2020)652082_EN.pdf
5. https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf

Фахівці пропонують спиратися на два основні критерії, які допоможуть визначити, чи не є певна діяльність втручанням: (1) намір (включаючи чинники часу, координації поведінки та масштаб наслідків) та (2) прозорість. Акт діяльності не повинен відповідати обом критеріям, щоб бути класифікованим, як втручання, але вони, безумовно, взаємно підкріплюють один одного[6].

Важливо, що ці критерії можна застосувати до широкого спектру тактик втручання, зокрема кібератак, інформаційних операцій, зловмисних фінансових впливів, підривної діяльності політичних і громадських організацій, стратегічного економічного примусу. Ці критерії також слугують основою для визначення, яке може охоплювати нові тактики у міру розвитку технологій.

У дослідженні «Дезінформація та пропаганда – вплив на функціонування верховенства права в ЄС та його країн-членів», йдеться про «агресивні інформаційні практики», які визначаються, насамперед, не за змістом розповсюджуваного контенту, а за методами, як, наприклад, маніпулятивні прийоми, автоматизовані методи розповсюдження, зловживання персональними даними та порушення правил фінансування політичних партій.

Такі практики повинні відповідати щонайменше таким критеріям відносно тих, хто розповсюджує інформацію або дає доручення на таку діяльність:

- інформація є хибною, сфальсифікованою або оманливою, або підводить до певної думки;
- розповсюджується з наміром ввести в оману, поляризувати або дестабілізувати суспільство або значну його частину;
- розповсюджується з прямою або опосередкованою метою отримання політичної чи геополітичної влади або фінансової вигоди;
- походить із прихованих джерел або осіб, або використовує мікротаргетування або штучний інтелект для більш широкого поширення такого контенту;
- потенційно негативно може вплинути на соціальну згуртованість, громадський порядок чи мир[7].

6. https://securingdemocracy.gmfus.org/wp-content/uploads/2020/03/Conceptualizing-Foreign-Interference-in-Europe.pdf
7. https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf

Більшість існуючих підходів до визначення того, чи є діяльність іншої держави неприйнятною, залежить від питання про наміри: чого прагнув досягти іноземний актор? Наприклад, замість використання терміну «дезінформація», як це робить ЄС, французький уряд надає перевагу терміну «маніпулювання інформацією», щоб «підкреслити політичний намір, що лежить в основі інформаційних маніпуляційних кампаній, як визначальний критерій цього явища»[8]. Декілька додаткових чинників можуть сприяти визначенню наміру: час, координація дій та масштаб наслідків. Час проведення інформаційної операції або кібератаки є важливим.

Витік даних зі зламаних електронних листів під час президентської виборчої кампанії у Франції у 2017 році стався безпосередньо напередодні дня виборів, з метою впливу на рішення електорату у момент голосування[9]. Обраний час для зливу допомагає визначити намір зірвати виборчий процес. Проте, чинник часу сам по собі не є єдиним визначальником втручання. Втручання проводяться постійно, не лише навколо виборчих кампаній. Агентство Інтернет-досліджень – Російська Ботоферма, що фінансується державою, розпочала таргетування американських громадян у 2014 році, задовго до того, як в центрі уваги стали президентські вибори в США 2016 року, і продовжувала таргетувати їх ще довгий час після перемоги Дональда Трампа[10].

Координація поведінки також є суттєвим чинником при визначенні наміру інформаційних операцій. Політика *Facebook* щодо видалення облікових записів передбачає вжиття заходів за «... використання декількох акаунтів *Facebook* або *Instagram*, для спільної діяльності, яку можна класифікувати, як просування дезінформації (англ. *Inauthentic Behavior*) ... і за якої використання фейкових акаунтів є основним [інструментом] для проведення операції»[11]. Координація між цими обліковими записами встановлює намір операції.

Ще одним корисним маркером наміру може бути масштаб ефекту (наслідків) атаки чи операції. Дункан Холліс (*Duncan Hollis*)[12] і Джеймс Паммент (*James Pamment*)[13] обговорюють масштаби наслідків або дестабілізації у своїх критеріях неприйнятного впливу. Тут є цінність – масштаб наслідків може дати уяв-

8. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf
9. https://www.theatlantic.com/international/archive/2017/05/france-macron-leak-hack/525738/
10. https://www.justice.gov/file/1035477/download
11. https://about.fb.com/news/2019/10/inauthentic-behavior-policy-update/
12. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3155273
13. https://www.msb.se/RibData/Filer/pdf/28697.pdf

лення про те, наскільки добре забезпечена конкретна операція ресурсами та наскільки серйозними є іноземні суб'єкти у своїх зусиллях втрутитися в демократію. Але дійсно вимірювати наслідки складно, як і вимірювати масштаби. Недорога і, здавалося б, невелика онлайн-операція насправді може мати вплив, що перевищує її сприйняту цінність. Для політиків важливо відзначити, що великий ефект можна отримати за невеликі кошти.

Масштаб впливу може сприяти встановленню наміру, але сам по собі він недостатній, як критерій втручання. Хакери російського військового розвідувального управління (ГРУ), які викрали електронні листи DNC у 2016 році, вперше прагнули поділитися ними через *Facebook*, але їм не вдалося привернути значну увагу. Їхнім постом поділилися лише 17 разів. Тільки коли *WikiLeaks* опублікував інформацію, її стали широко поширювати і вона справила значний ефект.[14] Зосередження уваги на масштабі наслідків, або масштабі дестабілізації, при визначенні того, чи є щось втручанням, може припустити, що невдалий злом і витік ГРУ в Facebook не є вартим уваги. ППроте, намір в обох випадках був однаковим – зірвати політичний процес у США, вплинути на кампанії кандидатів і сформувати суспільне сприйняття кандидатів.

Загальною особливістю втручання є його прихований або непрозорий характер. Іноземні уряди намагаються використовувати непрозорі засоби, щоб приховати свої зусилля з дестабілізації демократії. Російське агентство Інтернет-досліджень видавало себе американцями і створило 129 подій у *Facebook* в період з 2015 по 2017 рік, в деяких випадках навіть створюючи події, які могли призвести до справжніх сутичок між громадянськими групами, зокрема, шляхом планування акції протесту «Зупинити ісламізацію Техасу» через вулицю від заходу «Збережи ісламські знання» у Х'юстоні[15].

Аналогічно прозорість є важливою для фінансової сфери: джерела політичного фінансування, справжні бенефіціари інвестицій тощо. Підходи до визначення втручання повинні спиратися саме на концепт «прозорості», а не «обману» (англ. *deception*). Акцент на важливості прозорості може мати суттєве нормативне значення. Часто заходи з протидії втручанню являють собою негативну реакцію на негативні дії: неприйнятний контент – заборонений; корупційна політична поведінка – ка-

14. https://www.washingtonpost.com/business/technology/russian-hackers-who-stole-dnc-emails-failed-at-social-media-wikileaks-helped/2019/11/12/751690ae-0580-11ea-a5e2-fccc16fa3576_story.html
15. https://money.cnn.com/2018/01/26/media/russia-trolls-facebook-events/index.html

рається. Проте, формування цієї дискусії навколо прозорості змінює наратив від заборони – і відтак потенційної можливості порушення прав, особливо в інформаційному просторі, – до відкритості та свободи волі. Підкреслення важливості прозорості онлайн-платформ, реєстрів бенефіціарів власності та фінансування політичних партій надає громадянам більше повноважень щодо участі у демократичних процесах.

Міжнародний досвід пропонує низку термінологічних рішень. Наприклад, Альянс за збереження демократії звертається до досвіду Австралії, яка використовує такий поділ: якщо діяльність здійснюється відкрито і прозоро, – це іноземний вплив. Ці дії позитивно сприяють публічним дискусіям і є бажаною (прийнятною) частиною міжнародної взаємодії.

Важлива економічна форма впливу – це підкуп еліти, «elite capture»: і росіяни, і китайці в такий спосіб формують своїх агентів впливу.

Давід Стулік

Іноземне втручання, навпаки, – це діяльність, яка:

- здійснюється іноземним актором або від його імені;
- є примусовою, прихованою, оманливою, підпільною;
- проводиться всупереч суверенітету, цінностям та національним інтересам держави. Втручання іноземних держав виходить за рамки рутинного дипломатичного впливу, яке здійснюється урядами. Втручання може відбуватися самостійно або одночасно із шпигунською діяльністю[16].

Інші дослідники аналізують досвід США[17], де Департамент внутрішньої безпеки (*Department of Homeland Security*, DHS) запропонував визначення «іноземне втручання»: «Зловмисні дії іноземних урядів або суб'єктів, покликані посіяти розбрат, маніпулювати публічним дискурсом, дискредитувати виборчу систему, упереджувати розвиток політики або порушувати ринки з метою підриву інтересів Сполучених Штатів та їхніх союзників»[18]. Крім того, DHS представив таксономію іноземного втручання, яка охоплює такі дії: інформаційна діяльність (включаючи зловживання новими ЗМІ, зловживання традиційними ЗМІ та кіберзлочинність), торгові / стратегічні інвестиції, примус / корупція, експлуатація міграції та маніпулювання з боку

16. https://securingdemocracy.gmfus.org/wp-content/uploads/2020/03/Conceptualizing-Foreign-Interference-in-Europe.pdf
17. https://www.cisa.gov/publication/foreign-interference
18. Cybersecurity and Infrastructure Security Agency, Foreign Interference, U.S. Department of Homeland Security https://www.cisa.gov/publication/foreign-interference

міжнародних організацій. Тому сьогодні європейські законодавці вже мають на що спиратися у своїй роботі.

У «Плані дій щодо Європейської демократії» запропоновані такі визначення:

- *операція інформаційного впливу* стосується скоординованих зусиль, як вітчизняних, так і іноземних суб'єктів впливу на цільову аудиторію з використанням цілого ряду дезорієнтуючих (англ. *deceptive*) засобів, включаючи придушення незалежних джерел інформації у поєднанні з дезінформацією;
- *іноземне втручання в інформаційний простір*, найчастіше здійснюване в рамках більш широкої гібридної операції, можемо розуміти, як примус та дезорієнтуючі зусилля, які спрямовані на порушення вільного формування та вираження політичної волі людей іноземною державою або її агентами[19]. Проте експерти застерігають, що визначення втручання пов'язане з ризиком.

Політики можуть запропонувати визначення, яке є або:

- занадто широким, і відтак може створювати перешкоди свободі слова або створювати надмірні ускладнення для політичної участі;
- навпаки – занадто вузьким, щоб охопити певні форми зловмисної поведінки у сферах, що наразі швидко розвиваються, і відтак це заважатиме демократіям захищати себе, тому що атака не «вкладається» у наявне визначення.

Вибір визначення, яке просто каталогізує загальновживані тактики (наприклад: кібератаки, дезінформацію, економічний примус та зловмисне фінансування), також виявиться недостатнім, – оскільки будь-яке визначення втручання має бути досить гнучким, щоб охопити нові технології та підходи. Понад те, перелік тактик не може пояснити основні чинники, що зумовлюють втручання[20].

2.2. Інструменти впливу: підходи до структурування, сутність, особливості застосування

Ідея Дж. Ная-мол. (Joseph S. Nye, Jr.), що результат конфліктів залежить не тільки від того, чия армія переможе, а й від того, чий переможе наратив – є актуальною, як ніколи. Адже успіх ге-

19. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A790%3AFIN&qid=1607079662423#PP2Contents
20. https://securingdemocracy.gmfus.org/wp-content/uploads/2020/03/Conceptualizing-Foreign-Interference-in-Europe.pdf

ополітичного протистояння так само залежить від просування свого наративу. І, як часто це доводиться спостерігати у діях недемократичних акторів, просування наративу відбувається всіма можливими засобами: легальними та нелегальними.

Просування наративу відбувається як за допомогою суто інформаційних інструментів, так і через інші види діяльності. До інструментів зовнішнього впливу Трекер авторитарних втручань (*Authoritarian Interference Tracker*), що його запровадив Альянс за збереження демократії (*Alliance for Securing Democracy*[21]) відносить:

- маніпуляції з інформацією;
- кібероперації;
- зловживання фінансами;
- підрив громадянського суспільства;
- економічний примус.

Ці інструменти становлять ядро підривної діяльності. Проте, залежно від конкретних цілей та завдань акторів, можуть по-різному використовуватися, з одного боку. З іншого боку, їх по-різному структурують дослідники. Останніми роками є чимало робіт присвячених російському впливу.

У книзі Джеймса Шерра (*James Sherr*) «*Жорстка дипломатія та м'який примус – вплив Росії за кордоном*»[22] виділено цілий ряд використовуваних інструментів, включаючи військову, державну та публічну дипломатію, бізнес, енергетику, ЗМІ, соціальні і культурні впливи, а також низку тактик, таких, як експлуатація відмінностей та вразливостей, проникнення, кооптація, фіктивні компанії та тіньові структури, агенти впливу, лінгвістичні маніпуляції та пропаганда.

За оцінками П. Померанцева та М. Вайса «*Кремлівський інструментарій*»[23] включає дезінформацію, медіа, соціальні мережі, широкий спектр альянсів, експлуатацію розбіжностей, використання Православної Церкви та неурядових організацій, кооптацію і корупцію, PR, приховану військову силу, гроші, комерцію та енергетику.

21. The Alliance for Securing Democracy (ASD), a nonpartisan initiative housed at the German Marshall Fund of the United States, develops comprehensive strategies to deter, defend against, and raise the costs on autocratic efforts to undermine and interfere in democratic institutions.
22. James Sherr. Hard Diplomacy and Soft Coercion. Chatham House. 2013 // https://books.google.com.ua/books?id=FYPRDAAAQBAJ&printsec=frontcover#v=onepage&q&f=false
23. Pomerantsev P., Weiss M (2014) The menace of unreality: How kremlin weaponizes information, culture and money. Institute of Modern Russia, New York, NY // https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf

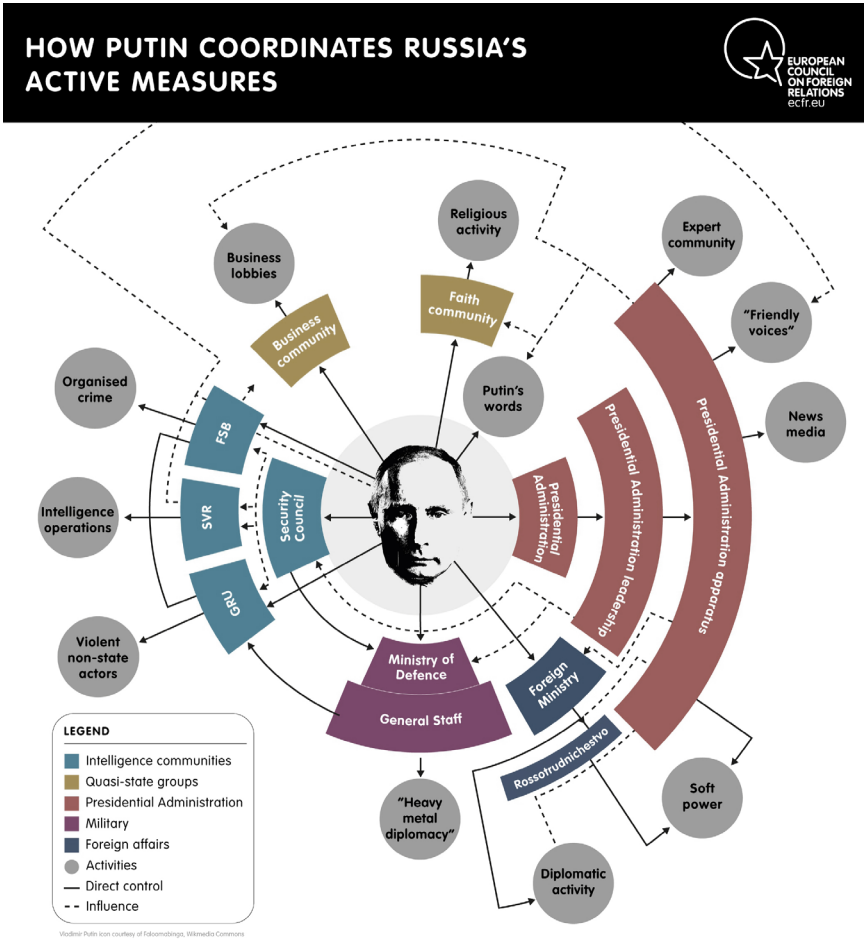
Автори своє дослідження розпочинають з ретроспективи – появи у радянській Росії ідеології «активних заходів», частиною яких була дезінформація. За визначенням експерта ЦРУ Лотара Метцеля (*Lothar Metzel*) дезінформація – це «операції, спрямовані на те, щоб отруїти процес формування думок на Заході». Під час таких операцій у міжнародні ЗМІ та інші джерела вкидаються помилкові, сфабриковані дані, щоб зганьбити супротивника і «у кінцевому підсумку ... змусити його прийняти рішення [в інтересах Радянського Союзу]».

Сучасна російська пропаганда об'єднала кращі радянські прийоми – критику в дусі «сам дурень» (або «критика у відповідь на критику») і чекістські «активні заходи» з постмодерністським підходом, розумним, глузливим, який натякає, що все навколо фікція. Якщо Радянська влада була змушена засвоїти і видозмінити такі концепції, як «демократія», «права людини» і «суверенітет», щоб приховати свої протилежні наміри, прихильники Путіна використовують ці концепції граючи, запевняючи навколишній світ, що навіть Захід більше не вірить в них. Гуантанамо, війна в Іраку, протести у Фергюсоні, «Йоббік», Шредер – усе це використовується, щоб показати, що лібералізм дорівнює ханжеству і будь-кого можна купити.

У «*Визначенні сучасного російського конфлікту*»[24] член парламенту Великобританії Б. Сілі (*Bob Seely*) наводить близько 50 інструментів державної влади і, що їх об'єднано у сім груп: політичний конфлікт, культура та управління, економіка та енергетика, військова сила, дипломатія та публічна дипломатія, а також інформаційна та наративна боротьба, які пов'язані між собою через командування та контроль. У роботі автор здійснює безпосереднє порівняння «активних заходів» КДБ часів Холодної війни з агресією путінської Росії. Він підкреслює, що Кремль вважає невійськові інструменти потенційно потужнішими, ніж військові, при цьому такі інструменти, як інформаційна війна, маніпуляції у сфері культури та хактивізм у соціальних мережах використовуються для досягнення цілей зовнішньої політики без використання прямої сили. У цьому новому виді конфлікту хакери, тролі, вбивці, політично пов'язані з керівники бізнесу, спін-докторінг, оплачувані протестувальники та вуличні бандити часто є більш корисними та більш придатними, ніж звичайні засоби ведення війни, такі, як літаки, танки та артилерія. Проте усі вони займають своє місце в цьому повному спектрі бойових дій.

24. Seely B. (2018) A definition of contemporary Russian conflict: how does the Kremlin wage war? Henry Jackson Society, London // http://henryjacksonsociety.org/wp-content/uploads/2018/06/A-Definition-of-Contemporary-Russian-Conflict-new-branding.pdf

Запрошений стипендіат Європейської ради з міжнародних відносин (*The European Council on Foreign Relations*, ECFR) Марк Галеотті (*Mark Galeotti*) у дослідженні «*Контроль над хаосом: як Росія управляє своєю політичною війною в Європі*»[25] охоплює увесь спектр інструментів, включаючи розвідку, злочинність, бізнес, релігію, аналітичні центри, медіа, м'яку силу, дипломатію, військові та фронт організації. М. Галеотті також спирається на концепт «активних заходів» та показує, як уся діяльність координується з Кремля.



25. Galeotti M. (2017b) Controlling Chaos: How Russia manages its political war in Europe. European Council on Foreign Relations Policy Brief, London // https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/

Директор нідерландського аналітичного центру «Фундація Цицерона» Марсель ван Герпен (*Marcel H. Van Herpen*) у книзі *«Пропагандистська машина Путіна»*[26] згадує використання роботи під прикриттям, культурну дипломатію, вплив на громадську думку, PR та лобізм, ЗМІ, соціальні мережі, фінансування політиків, шпигунів, Російську православну церкву, підрив західних альянсів, побудову нових політичних альянсів, економічну взаємозалежність і використання громадянського суспільства. Також він аналізує трансформацію концепції «м'якої сили», яку Джозеф Най-молодший (*Joseph S. Nye Jr.*) визначає, як «силу привабливості» у офіційному політичному дискурсі Росії. Аналітики Кремля, оцінюючи потенціал російської м'якої сили Росії, як «близький до нуля», здійснили переосмислення концепції м'якої сили, перетворивши її на «жорстку силу в оксамитовій рукавичці». У цій перевизначеній концепції «м'якої сили» Марсель ван Герпен розрізняє три складові: «мімікрія», «відкидання» та «винахід». «Мімікрія» складається із спроб копіювати західну публічну дипломатію, «відкидання» – це стратегія нападу на ініціативи західної публічної дипломатії, а «винахід» включає нові методи інформаційної війни. Одним з таких винаходів є найм західних PR-фірм для поліпшення іміджу Кремля на Заході.

Ще одним нововведенням є організація міжнародних семінарів дискусійного клубу Валдай у Росії та фінансування Кремлем аналітичних центрів за кордоном. Ці ініціативи не тільки служать меті створення репутаційного капіталу, але й використовуються Кремлем, як випробувальний полігон для російських дипломатичних ініціатив. І хоча в західних концепціях «м'якої сили» немає місця шпигунству, у розумінні «жорсткої», «м'якої сили» Кремля це по-іншому. Зусилля з інфільтрації «агентів впливу» до іноземних урядів й міжнародних організацій спираються на усталену традицію радянської епохи.

У виданні Королівського інституту міжнародних відносин (*Chatham House*) «*Російський виклик*»[27] проаналізовано широкий спектр інструментів, включаючи енергетику, торгівлю, національні меншини, кібер, кооптування ділових та політичних еліт, прикордонні суперечки, військову силу, інформаційну війну та пропаганду. Автори зазначають, що сучасна російська

26. Herpen M.V. (2015) Putin's propaganda machine: Soft power and Russian foreign policy. Rowman and Littlefield Publishers, Lanham, MD // https://books.google.com.ua/books?id=CTiCCgAAQBAJ&printsec=frontcover&hl=uk#v=onepage&q&f=false
27. Giles K, Hanson P, Lyne R, Nixey J, Sherr J, Wood A (2015) The Russian Challenge. Chatham House, London // https://www.chathamhouse.org/sites/default/files/field/field_document/20150605RussianChallengeGilesHansonLyneNixeySherrWoodUpdate.pdf

практика інформаційної війни поєднує низку випробуваних часом інструментів впливу разом з новими сучасними технологіями та можливостями, насамперед інтернетом. Деякі основні цілі та керівні принципи визнаються, як відновлені аспекти підривних кампаній часів Холодної війни та раніше. Але Росія інвестувала величезні кошти в адаптацію принципів підривної діяльності до епохи Інтернету.

Ці нові інвестиції охоплюють три основні сфери:

- медіа орієнтовані, як на внутрішню, так і на зовнішню аудиторію, що мають значну присутність в інтернеті. Найбільш відомим з них є RT (раніше *Russia Today*);
- використання соціальних мереж, онлайн дискусійних майданчиків та можливостей коментарів, як мультиплікатора для забезпечення широкого охоплення та проникнення російських наративів;
- мовні спроможності, щоб взаємодіяти з цільовою аудиторією на міжнародному фронті їхньою мовою.

Результатом цього є домінуюча онлайн-присутність, відома наразі, як кремлівська армія тролів, яка діє у координації з державними ЗМІ.

Отже, до інструментів інформаційного впливу належать:

- традиційні та цифрові медіа;
- соціальні мережі;
- інформаційні агентства;
- публіцистична та науково-публіцистична література;
- агітаційні матеріали, що використовуються під час вуличних заходів або поширюються у поштові скриньки чи роздаються на вулицях;
- рекламна продукція (постери, біг борди).

Показово, що незважаючи на стрімке зростання кількості та якості цифрових медіа в житті суспільств, в багатьох випадках для поширення дезінформації використовуються абсолютно традиційні для розвідувальних органів інструменти – зокрема, мережі агентів впливу. Це надзвичайно широка категорія, до якої можуть бути включені, як свідомо використовуючи свою діяльність особи, так і ті, хто здійснює свою діяльність виходячи з інших мотивів.

Такі мережі включають:

- **псевдо громадські організації**, які складаються з 1 чи двох осіб, але, які можуть створювати інформаційні приводи;
- **політики з європейських проросійських партій**, які самою своєю присутністю можуть легітимізувати злочинну діяльність Росії;

- **експертні мережі**, які підтримують активні контакти із російськими колегами і заходи, які використовуються для ведення агітації;
- **блогери** (справжні та вигадані), що долучаються до поширення ворожих наративів та інші.

Питання інструментів впливу доцільно розглядати у сув'язі з питанням суб'єкта впливу.

У 2011 році тодішній держсекретар Гілларі Клінтон (*Hillary Clinton*) заявила, що Сполученим Штатам необхідно робити більше, щоб донести свої цінності та поширити їх вплив на решту світу через медіа, підтримувані урядом. «Ми беремо участь у інформаційній війні і ми програємо цю війну»[28], – попередила вона, зазначивши, що Китай і Росія запустили багатомовні телевізійні мережі саме тоді, коли США скорочували свою діяльність у цій сфері. Гілларі Клінтон дійшла висновку, що «Ми платимо велику ціну» за демонтаж міжнародних мереж комунікації після закінчення Холодної війни[29].

У грудні 2014 року Пітер Хоррокс (*Peter Horrocks*) – колишній директор Всесвітньої служби Бі-Бі-Сі, аналогічно стверджував, що Великобританія та США програють глобальну інформаційну війну. «Нас випереджають Росія та Китай», – сказав він одночасно підкресливши, що «Роль, яку ми повинні відігравати, має бути рівноцінною. Ми не повинні бути прихильниками тієї або іншої сторони, ми повинні забезпечити те, чому люди можуть довіряти»[30]. Росія – не єдина країна, де очевидний підвищений інтерес до інформаційно-комунікативних стратегій. Китай теж активно готується до майбутніх інформаційних воєн.

За словами Стефана Гальпера (*Stefan Halper*), керівника Інформаційного бюро Державної Ради Китаю Лі Чанг-Чун (*Li Jiang Jianguo*), позиція уряду, що «глобальний інформаційний простір належить до числа найважливіших полів для битви за владу у XXI столітті». За словами китайського чиновника: «Здатність комунікувати визначає ступінь впливу... У якої країни комунікативні спроможності є найсильнішими – це та нація, чия культура та основні цінності поширюються далеко й широко, ... це та нація, що може з найбільшою силою впливати на світ»[31].

28. Colby Hall, «Hillary Clinton: 'America Is Losing' an Information War That 'A1 Jazeera Is Winning, « *Mediate.com* (March 2. 2011), http://www.mediaite.com/tv/hillary-clinton-claims-al-jazeera-is-winning-an-information-war-that-america-is-losing/.
29. Ibid.
30. Josh Ilalliday, «BBC World Service Fears Losing Information War as Russia Today Ramps Up Pressure,» The Guardian (December 21. 2014).
31. Stefan Halper, The Beijing Consensus: Legitimizing Authoritarianism in Our Time (New York: Basic Books, 2012), 10.

80% зусиль усього зовнішнього впливу на Європейський Союз справляє Росія. Решта 20% – це вплив інших держав (переважно Китаю та Ірану) та недержавних суб'єктів (груп джихадистів, зокрема ІДІЛ). Ця статистика міститься у французькій доповіді «Маніпулювання інформацією: виклик нашим демократіям»[32].

«Росію називають іноземною державою, яка найбільше намагається впливати на європейську політику та її процеси прийняття рішень. Основна увага Китаю спрямована на процеси прийняття політичних рішень, протидію еміграції, технічне та промислове шпигунство», – підтверджує наведену статистику норвезьке дослідження[33], здійснене на матеріалах щорічних звітів[34] служб розвідки країн ЄС[35] та США. У цілому Росія продовжує реалізовувати відому з часів Холодної війни доктрину активних заходів, адаптувавши її до реалій цифрового світу.

Марк Галеотті запропонував таку категоризацію підходів Кремля до здійснюваного інформаційного впливу[36]:

Цілі Кремля	Дії Кремля
Переривання комунікації	Придбання західних медіа
	Влаштування DDoS-атаки
	Паралізування роботи медіа, звинувативши журналіста у наклепі

32. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf
33. https://www.nature.com/articles/s41599-019-0227-8
34. Відповідно до цих звітів, Кремль має три основні стратегічні цілі. По-перше, забезпечити безпеку режиму та зберегти власну владу. По-друге, забезпечити домінування у країнах ближнього зарубіжжя, під якими зазвичай розуміється колишній Радянський Союз мінус країни Балтії. Нарешті, забезпечити Росії статус світової держави із відповідним впливом та повагою на міжнародному рівні.
Головною та довгостроковою метою є послаблення двох основних західних альянсів – НАТО та ЄС. У короткотерміновій перспективі Росія прагне зняття санкцій, введених з 2014 року.
Діяльність російського впливу охоплює широкий спектр сфер, включаючи політичну, безпекову, військову, економічну, енергетичну та технологічну. У країнах з російськими меншинами також охоплюються етнічні, соціальні та історичні питання.
35. Чеська Республіка, Данія, Естонія, Фінляндія, Німеччина, Латвія, Литва, Нідерланди, Норвегія, Швеція
36. https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf

Деморалізація ворога	Заплутання Заходу за допомогою суперечливих повідомлень
	Залучення експертів на свою сторону, запрошуючи їх на форуми високого рівня
Придушити систему управління	Кампанії з дезінформації
	Розділення Заходу за допомогою підходу «розділяй і володарюй»
	Здобути якомога більше політичного впливу

У Європі, зараз ми говоримо про іноземний вплив, передусім, двох країн – це Росія і Китай. Коронавірусна криза багато процесів пришвидшила і трішки розкрила карти Китаю, оскільки раніше ніхто не звертав багато уваги на китайський вплив: він не такий агресивний, він не такий нахабний, я би сказав, на відміну від російського, яким ми почали тут, в Європі, займатися після початку агресії Росії проти України.
Також тут іноді відчувається вплив інших держав, наприклад, Ірану, частково – Турції.

Давід Стулік

Діяльність впливу, спрямована на населення Європи, має на меті створення недовіри і підрив наявного укладу суспільства, стверджують звіти з розвідки. Підхід «розділяй і володарюй» полягає у експлуатації якомога більшої кількості «ліній розламу» на якомога більш кількісному рівні. Росії, як великій державі, тоді буде легше мати справу з мульті фрагментованою Європою. Вбачаються такі три рівні застосування підходу «розділяй і володарюй». Перший – європейський рівень, на якому атакуються альянси, НАТО та ЄС. Другий – міждержавний рівень, на якому створюється розкол і недовіра між народами. Нарешті, третій – внутрішньодержавний рівень, на якому створюється внутрішній поділ між різними соціальними групами в окремих країнах. Межі між цими рівнями розмиті, будь-яка діяльність, що розпалює невдоволення ЄС, безумовно, може також створити поділ між країнами і всередині країни з дружнім до ЄС урядом[37]. Для створення недовіри і підриву наявного укладу суспільства використовується низка методів, у тому числі дезінформація, інформаційний шум, релятивізація правди, твердження, що «всі брешуть», підтримка популістів та екстремістів, поширення чуток та використання страху перед війною з Росією.

37. https://www.nature.com/articles/s41599-019-0227-8

Основними засобами для охоплення населення є ЗМІ та соціальні мережі. Також Росія використовує соціальні меншини та біженців, бізнеси та фронт-організації. Російська пропаганда та дезінформація є широкомасштабними, а великі ЗМІ, що є добре забезпечені ресурсами – лояльні до російського уряду. Телебачення знаходиться під повним контролем, і Адміністрація Президента щотижня надає головним редакторам інструкції, деталізуючи теми та ключові фрази, які слід висвітлити. Найбільш помітними ЗМІ у міжнародному просторі є RT та Sputnik, які працюють на багатьох мовах. Росія спілкується через телебачення, радіо, Інтернет та публічні заходи, а також наймає платних журналістів у західних медіа. Незважаючи на значні ресурси, ефективність діяльності цих ЗМІ ставиться під сумнів. Зміст російськомовних засобів масової інформації не обов'язково стосується російських меншин таких, як країни Балтії, і рейтинги вказують на те, що RT і Sputnik не є особливо ефективними. За власними оцінками ЄС, Росія витрачає понад 1 мільярд доларів на рік на свої пропагандистські видання[38].

Значення соціальних медіа зростає. Їх можна використовувати у т.ч. через приховані ідентичності, поширюючи прокремлівську інформацію, дезінформацію та коментарі, а також мобілізуючи та організовуючи акції протесту, особливо з таких важливих для Росії питань, як збиття рейсу MH17 над Україною. Іноді потік коментарів розміщується для маніпулювання громадською думкою або зриву дискусій у соціальних мережах. Росія також використовує так званих ботів, автоматизовані акаунти, що просувають контент у соціальних мережах. Вони можуть підтримувати інших користувачів або поширювати певні повідомлення, заглушувати реальний контент та порушувати справжню дискусію. Картування соціальних та професійних відносин робиться для посилення поширення дезінформації та пропаганди. Також було вжито заходів для зменшення впливу протилежних голосів.

Загальна мета російського впливу, що досягається використанням сукупності інструментів впливу, – це послаблення довіри громадян до держави, до демократичних процедур, до демократичних цінностей. Це також часткова спроба ослабити політичні традиції еліти і політичні механізми. У підсумку відбувається поляризація європейського суспільства щодо соціальних та політичних питань та руйнування інституційного карка-

38. Samuel Stolton, «EU Commission Takes Aim at Disinformation, Admits Funding Deficit,» Euractiv, December 6, 2018, last updated January 3, 2019

су Європи – ЄС та НАТО[39]. Відтак, російський вплив спрямований на її послаблення.

Китай – навпаки, хоче посилювати свій економічний вплив та нарощення високотехнологічних послуг, і тому в Пекіні зацікавлені у тому, щоб Європейський Союз і далі існував та розвивався. Можливості виходу на ринок ЄС є визначальним чинником китайського впливу. Для росіян економічний вплив інвестиції у Європу немає економічного значення, для них це в першу чергу – геополітика[40]. Отже, і вплив має різні форми, проте інструменти часто ті самі.

Комуністична партія Китаю для зовнішнього впливу використовує: кооптування представників етнічних меншин, релігійних рухів, а також ділових, наукових і політичних груп, виступи від імені цих груп і використання їх для підвищення своєї власної легітимності. З метою надання адекватної протидії, дослідники пропонують розглядати мережу партійних і державних установ, відповідальних за вплив, на групи поза партією, особливо ті, які стверджують, що представляють громадянське суспільство, як систему «єдиного фронту» КПК[41]. Пекін також намагається змінити європейський дискурс про зростання Китаю шляхом обміну журналістами та наукової співпраці, з метою зменшення рівня критичності щодо його зовнішньої політики (наприклад, у Греції та Чеській Республіці)[42]. Загалом, китайська доктрина інформаційної війни включає декілька компонентів, а саме психологічну війну, маніпуляції громадською думкою або медіа війна, та маніпулювання юридичними аргументами, відома, як юридична або правовійна (*Lawfare*).[43]

Необхідно пам'ятати, що чим більше авторитарних акторів застосовуватимуть асиметричні інструменти та тактики, тим частіше Європа буде стикатися зі зростаючою кількістю загроз з різних сторін. Авторитарні актори активно експлуатують «наріжні камені ліберальної демократії: обмеженість державної влади, плюралізм, вільні медіа та відкриту економіку»[44].

39. https://www.gmfus.org/publications/european-policy-blueprint-countering-authoritarian-interference-democracies
40. Дискусія зі старшим аналітиком чеського аналітичного центру «Європейські цінності» Давідом Стуліком про європейський підхід до протидії зловмисним впливам // https://fb.watch/5vWDsw5QGw/
41. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652082/EPRS_BRI(2020)652082_EN.pdf
42. https://www.gmfus.org/publications/european-policy-blueprint-countering-authoritarian-interference-democracies
43. https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/Expeditions-with-MCUP-digital-journal/To-Win-without-Fighting/
44. https://www.fiia.fi/wp-content/uploads/2019/09/wp110_democratic-deterrence.pdf

З точки зору досягнення результату можна виділити чотири лінії захисту.
1. Документування загрози.
2. Підвищення обізнаності щодо загрози.
3. Виправлення слабкостей, які експлуатує агресор.
4. Покарання та стримування агресора.

Якуб Каленський

Водночас існує значний розрив між накопиченими знаннями щодо наслідків зовнішнього впливу та ефективністю різних контрзаходів[45]. Подолання цього розриву є без перебільшення чинником стабільності існування демократичних режимів.

45. https://carnegieeurope.eu/strategiceurope/83758

ЄВРОПЕЙСЬКИЙ ШЛЯХ ПРОТИДІЇ:

ЯК НЕОБХІДНІСТЬ ЗАХИСТИТИ ДЕМОКРАТІЮ ЗМІНЮЄ ПОЛІТИКУ ЄС?

РОЗДІЛ 3

3. ЄВРОПЕЙСЬКИЙ ШЛЯХ ПРОТИДІЇ: ЯК НЕОБХІДНІСТЬ ЗАХИСТИТИ ДЕМОКРАТІЮ ЗМІНЮЄ ПОЛІТИКУ ЄС?

Проблема захисту Європейського Союзу від підривної іноземної діяльності співпадає із самим заснуванням Європейського товариства вугілля та сталі. Саме тоді, у перші повоєнні роки, загострилось протиборство між Радянським Союзом та США за вплив на європейські країни та їх політику. В подальшому Радянський Союз вибудував цілу мережу впливу на європейських політиків та громадськість, яка мала істотний вплив на саму логіку побудови ЄС.

Першими функціонерами європейських інституцій ставали і члени комуністичних та соціалістичних партій європейських держав, в т.ч., як ці партії не просто перебували у дружніх відносинах із Комуністичною партією Радянського Союзу, але подекуди контролювались СРСР (на рівні фінансової, організаційної, технічної допомоги). Розгалужена мережа різноманітних організацій «дружби» та «братерства», потужні симпатії до лівих ідеологій з боку творчої інтелігенції ЄС (що часто продовжується і зараз), розташування на території Європи штаб-квартир відомих організацій прикриття КДБ – все це забезпечувало радянським спецслужбам потужні позиції впливу майже у всіх країнах ЄС.

Література 70-80х років ХХ століття каже і про спроби втручання Радянського Союзу у виборчі процеси в Британії та Німеччині, а грецькі партії та преса завжди були прихильні до Радянської влади. Безумовно, цей вплив намагались обмежувати, але в багатьох випадках спеціальні служби СРСР (як і зараз) користувались «сірим простором» права, а їх діяльність лише зрідка виходила поза межі суто морального осуду і ставала предметом кримінального переслідування. І тоді і зараз багато хто знав та розумів, що деструктивний вплив на політичні процеси в Європі здійснюється, однак це не мало істотного впливу на реальність боротьби з цим явищем.

Дезінформація так само відігравала важливу роль, хоча і була пов'язана з іншими темами – ядерне роззброєння, наслідки розміщення збройних сил США в Європі, винахід нейтронної бомби, тиск на політичне керівництво. Для поширення дезінформації з цих питань СРСР використовувало весь традиційний арсенал медіапоширення – газети, журнали, телебачення (інтерв'ю, фільми), фестивалі, підкуп посадовців, використання агентів впливу у різних сферах. Часткова пауза в цьому проти-

борстві, яка була характерна для 90-х років XX століття, поступово почала змінюватись із приходом до влади В. Путіна. Слід відмітити, що зростання впливу РФ у ЄС відбувалось значно швидше, ніж в США.

Цьому сприяло декілька обставин:

- **наявні сильні позиції**. Зникнення СРСР не означало зникнення з європейської політичної арени всіх тих людей, які сформувались за підтримки радянського режиму. Усталені зв'язки, які зберігались і в найбільш неспокійні моменти сучасної європейської історії (наприклад, війна в Югославії) дозволили РФ не просто зберегти ці контакти, але й розширити їх мережу;
- **відновлення старих мереж впливу**. Створені ще за радянських часів товариства «дружби» (які майже зникли у 90-і роки) знов почали відновлювати свою роботу, «РПЦ за кордоном» розпочала свою активну діяльність, будуючи нові храми та виступаючи донором різноманітних навколорелігійних проектів, особи, які навчались у Росії залучаються до співпраці вже після їх повернення до батьківщини (саме такі особи пізніше сформували нову мережу псевдо-громадських організацій, які просували тези про «громадянську війну в Україні»);
- **посилення економічного впливу та корупція**. Різноманітні російські економічні проекти із сумнівними економічними вигодами, але вираженими геополітичними інтересами, вибірковий доступ іноземних інвесторів на російський ринок енергоносіїв, активізація лобістської діяльності – все це дозволило створити РФ в Європі міцний фундамент, на якому базується і частина операцій впливу. Корупція є іншим фронтом цієї діяльності – Росія знає та вміє використовувати цей важіль у політичній діяльності. Сьогодні цей метод застосовує і Китай, скориставшись ситуацією із пандемією. Так у Чехії виникла низка скандалів навколо Міністра охорони здоров'я та його зв'язків із КНР в питаннях надання допомоги, що в подальшому виявилась питанням звичайного експорту, а не безкоштовної допомоги.

> *Європа не любить заборон, Європа не любить жорстких дій, Європа дуже обережно впроваджує санкції... Тому європейський підхід дуже м'який.*
>
> ***Давід Стулік***

Все це поєднувалось із більш загальними поглядами та підходами ЄС, як щодо власної зовнішньої політики, так і можливостей впливати на внутрішні дискусії.

Незважаючи на це, російська агресія проти України в 2014 році стала для ЄС важливим тестом на дієвість таких підходів і наочно продемонструвала, якими можуть бути можливі наслідки стрімкого поширення дезінформації.

Посилення уваги європейських інституцій до дезінформації, як загрози європейській демократії поставило питання і про інші джерела впливів, з якими ЄС змушений рахуватись. Серйозної ваги набуває КНР, що маючи один з найпотужніших економічних потенціалів у світі поступово вчиться конвертувати його у політичний, культурний та інформаційний вплив. Методи, які при цьому застосовує КНР є, як повністю новими, так і схожими із російськими. Пан Стулік в цьому контексті звертає увагу на відмінності у стратегічних цілях операцій впливу, що здійснює РФ та КНР в Європі: «На що спрямований російський вплив? Він спрямований на послаблення демократичних інституцій, послаблення довіри громадян до держави, до демократичних процедур, до демократичних цінностей. Це також часткова спроба, скажімо, еліти послабити політичні традиції і політичні механізми. Китай, навпаки хоче посилювати свій економічний вплив і тому вони, наприклад, зацікавлені в тому, щоб такий Європейський Союз і далі існував. Можливо, слід вийти на ринок ЄС, як на економічний простір. Для росіян економічний вплив інвестиції у Європу немає економічного значення. У них це все, в першу чергу – геополітика. Китаю потрібні ринки збуту, ринки, з якими він співпрацює, торгує і тому вони тут дивляться на Європейський Союз з іншої позиції».

Хоча посилення російської дезінформації в 2014-2015 році і сприяло появі перших реакцій ЄС на цю проблему, однак можна констатувати, що і сьогодні Союз знаходиться у процесі не стільки застосування механізмів захисту, скільки артикулювання проблеми та дискусії щодо прийнятності тих, чи інших методів захисту. Важлива частина цих дискусій – зміщення фокусу уваги від боротьби з «пропагандою третіх сторін» (як це визначалось у 2015-2016 роках) до «захисту демократії», як основного завдання. Російське втручання у вибори США, спроби втручання у Brexit (ситуація з передачею даних Cambridge Analytica), у референдум в Нідерландах, небезпека виборчого процесу в декількох європейських країнах – все це змусило ЄС досить швидко змінити ставлення до проблеми. Дезінформаційні атаки більше не сприймались, як епізодичні недоліки недійного процесу, а, як спрямована атака на самі основи демократичних процедур, а відтак на демократію, як таку. Відтак, починаючи з 2016 року ЄС

намагається вибудовувати свою стратегію стримування дезінформації. В 2016 році було створено левову частку інструментів та вжито заходів, які в подальшому здебільшого розширювались та ускладнювались.

3.1. Виклики регулювання деструктивного впливу щодо європейської демократії

Європа залишається надзвичайно різною як за моделями управління національних держав, так і щодо їх відношення до проблеми дезінформації (в т.ч., але не тільки - російської). В той час, як ціла низка європейських країн із травматичним радянським досвідом у історії свого державотворення (як то країни Балтії чи Польща) вживають достатньо радикальних (за європейськими мірками) заходів із протидії, деякі інші самі включаються у підтримку російських наративів (Угорщина, Греція, Італія).

Водночас ступінь жорсткості вживаних заходів є досить дискусійним та неоднозначним. Хоча Великобританію вважають одним із лідерів протидії деструктивним впливам, але реально вжиті заходи є сумнівними в частині реального впливу на ситуацію. Зокрема, основним інструментом боротьби з можливою підривною інформаційною діяльністю є регулятор Ofcom, який видає приписи і може впливати на саме функціонування медіа в державі. Однак, фактичний вплив його на ситуацію досить обмежений, а штрафи та різноманітні приписи для потенційних порушників є слабким обмежувальним інструментом (досвід позбавлення ліцензії китайського мовника є одним з небагатьох прикладів, коли діяльність регулятора дала результати).

Діяльність більшості суб'єктів, задіяних в операціях впливу, не підпадає під будь-які обмежувальні заходи і вони можуть її здійснювати посилаючись на норми законодавства, які захищають свободу слова. Але навіть інші заходи (скажімо, робота з меншинами) також часто охороняється міжнародним правом, яке захищає права національних меншин і робить будь-яку спробу обмеження впливу із використанням такого каналу вкрай дискусійною та некомфортною для демократичних держав. Європа не є виключенням – робота російських посольств із російськими меншинами (які часто погано інтегруються у суспільства) у Чехії, Німеччині

Напевно, варто говорити про месиджі, про наративи. Якщо вони дуже схожі з тим, що загрожує основам естонської держави, естонському суспільству, якщо це протирічить нашій конституції, всім тим цінностям, які в ній закріплені. Якщо ці наративи такі, то ми маємо справу з загрозою безпеці.

Дмитро Теперик

або інших європейських країнах є активною і дозволяє посилено впливати на ці цільові групи. Для цього використовуються не лише російські медіа (наприклад, в Німеччині багато з мігрантів споживає виключно російські телеканали), але і російськомовні газети, які видаються, як за допомогою Російської держави, так і подекуди за державними коштами самих країн (як частина заходів підтримки національних меншин).

Російські дипломатичні працівники також продовжують свою діяльність, активізуючи доступні їм мережі та встановлюючи нові контакти між європейськими та російськими організаціями. Будапешт, Відень та Прага знову стають столицями їх шпигунської активності в Європі.

Водночас Європа, як і більшість демократичних країн, намагається сформулювати чим взагалі є «операції впливу» і, як їх відрізнити від цілком легальної і нормальної політичної боротьби. Наприклад, концепція «політичних дебатів», яка є однією з основ демократичних режимів, так само, як і інші цілком нормальні демократичні практики атакуються сторонніми країнами у своїх інтересах. Межа між «жорсткою політичною дискусією» (яка може зачіпати вкрай складні теми) та спробою штучно це зробити досить неоднозначна та не піддається чіткій сепарації.

3.2. Боротьба з операціями впливу: панєвропейські та національні підходи

Припинення діяльності класичних розвідників чи їх прямих агентів в ЄС є більш відпрацьованим. Про це свідчить викриття в Європі[1] мереж російських розвідників чи попередження атак на об'єкти критичної інфраструктури[2]. Арешти агентів

1. https://www.lemonde.fr/international/article/2019/12/04/la-haute-savoie-camp-de-base-d-espions-russes_6021648_3210.html
2. https://english.defensie.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw

російських спецслужб у Польщі[3], Балтійських країнах[4], Чорногорії[5] та інших країнах вказує на те, що ця контррозвідувальна компонента залишається на традиційно високому рівні. Водночас, як тільки ця діяльність починає стосуватись інформаційних заходів впливу (в т.ч. – дезінформації) ефективність істотно знижується.

Навіть ті моделі, до яких вдаються європейські держави, що визнають проблему мають брак практичних інструментів, що дозволили б побудувати систему протидії більш ефективно. Наприклад, у Чехії, яка докладає багато зусиль для зменшення деструктивного впливу РФ, відсутні чіткі та зрозумілі координаційні міжвідомчі механізми, які б дозволили держорганам консолідувати свої зусилля. Як вказує пан Стулік: «Минулого року ми програли боротьбу з Росією за історичну правду, бо Росія дуже агресивно розповсюджувала інформацію, що в Чехії починаються фашистські тенденції: зносять радянські пам'ятники, пам'ятник Конєву, Жукову і так далі, знищують поховання радянських вояків, що взагалі не відповідало правді. Але, наприклад, в МЗС Чехії не було жодної людини, яка би могла займатися таким страткомом: роз'яснювати чесну позицію». Інша ситуація у Польщі, де така група в складі МЗС існує і активно спростовує фейкову інформацію з найбільш критичних тем».

Естонія намагається будувати свою систему захисту від операцій впливу базуючись на, так званому, «широкому підході», в основі якого – концепція **стійкості**. Свою модель захисту вона почала будувати після подій 2007 року, коли стало зрозуміло, що можливості російського впливу на суспільну та політичну ситуацію в цій країні є значними. Після цього було сформовано нову міжсекторальну та інтердисциплінарну модель, яка робить суб'єктами захисту не лише і не стільки державу, скільки інших стейхолдерів: експертів, громадянське суспільство та приватний сектор (особливо в частині кібербезпеки критичної інфраструктури). Однак, як слушно зауважує пан Теперік: «На словах це, звичайно, звучить досить красиво… І навіть принципи цього закріплено в нормативних документах. Але на практиці це потребує великого залучення та постійної практики. Адже у всіх організаціях, по-перше, різний погляд на загрози та їх джерела, а по-друге – різний погляд на культуру безпеки. Тому пошук

3. https://www.rbc.ru/politics/29/04/2015/5540fc4f9a79478e0208f2cc
4. https://www.ukrinform.ru/rubric-world/2210518-v-estonii-vpervye-zaderzali-agenta-rossijskogo-gru.html
5. https://www.radiosvoboda.org/a/news-chornohoria-sproba-perevorotu-vyrok/29930317.html

спільної мови щодо того, як аналізувати загрози, як їх сприймати, як на них відповідати – все це потребує постійної практики та важкої праці. По суті ми кажемо, що у людей, які відповідають за ці питання, має сформуватись спільний словник, єдиний словниковий запас для того, щоб вони могли разом розуміти, про які загрози йде мова і, як на них спільно реагувати. І це дійсно суттєвий виклик. І це потребує постійних спільних навчань».

Ще одним інструментом захисту, який використовує Естонія для попередження ворожої активності – **є масштабні програми підвищення стратегічної та ситуативної обізнаності про загрози**. Для цього розвідувальні та контр розвідувальні служби щорічно публікують відкриті звіти про основні загрози, де пояснюють суть цих загроз, аргументують їх важливість та показують можливий вплив на естонське суспільство. З іншого боку, проводяться різнопланові курси з питань національної безпеки для найрізноманітніших верств населення: від політиків і державних службовців, закінчуючи священнослужителями та вчителями шкіл.

Великою складовою естонської відповіді на загрози (в т.ч. цифрової) є створення нормативних рамок для діяльності добровольців – спочатку це стосувалось суто військових питань, але зараз сфера розширилась і на інші компоненти (в т.ч. рятувальні служби, поліцію та кібербезпеку).

3.3. Формування загальноєвропейської стратегії стримування деструктивного впливу

ЄС поступово змінює свої підходи до протидії ворожим впливам, вибудовуючи багатошарову модель захисту. Водночас в цьому питанні спостерігається певний дисбаланс уваги на користь боротьби з дезінформацією (як елементом впливів) та зменшеною увагою до інших складових цього явища.

Хоча, вже у 2016 році Дослідницька служба Європарламенту впевнено оперувала поняттями «вороже втручання у демократію», «іноземні операції впливу проти ЄС», «активні заходи Кремля»[6]. В їх матеріалах такі операції розглядаються у всій їх повноті, включно з «не інформаційними» складовими (такими, як вбивства, кібератаки, вепонізація міграції, вплив через економічну сферу, використання псевдо НУО тощо). Однак, як

6. https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf

вже зазначалось, в центрі підвищеного інтересу протидії впливам є саме протидія дезінформації. При цьому ЄС виходить з того, що ключова проблема дезінформації у атаці на демократію полягає не стільки у самому факті поширення неправди, скільки в тому, що спеціально підготовлені неправдиві повідомлення зменшують критичність сприйняття (споживачі сприймають все емоційно, а не раціонально), загострюють суспільні протиріччя. Відтак це впливає на ключові демократичні механізми, такі, як вибори, суспільні дискусії чи референдуми – рішення приймаються не на основі об'єктивної інформації та фактів, а виходячи з емоційного стану, який може бути штучно загострений. Ворожі ЄС треті країни намагаються використовувати ці особливості сприйняття, дестабілізуючи ситуацію, поширюючи відчуття страху чи гніву, зіштовхуючи різні групи, атакуючи саму демократію.

Загальноєвропейський підхід в питанні протидії дезінформації є продовженням загального погляду ЄС на вирішення складних проблем, що передбачає не так домінуючу центральну волю центральної влади (Європейської комісії чи її структур), як багатосторонній підхід, в який залучені уряди, загальноєвропейські інституції, новинні медіа, онлайн платформи, вчителі в школах, фактчекери і кожен громадянин. Ключову роль в цьому питанні відводилась Службі зовнішніх зв'язків Європейського Союзу (EEAS), яка спираючись на діяльність оперативних робочих груп, мала:

- оптимізувати роботу лінгвістів, які вільно володіють мовами, що не є офіційними в ЄС;
- оптимізувати роботу фахівців із соціальних медіа, які можуть проводити моніторинг інформації не з ЄС;
- забезпечити цілеспрямовану комунікацію для реагування на дезінформацію.

У формуванні європейської політики стримування впливу (та побудови заходів з протидії, передусім – дезінформації) можна виокремити низку рішень Європарламенту та Єврокомісії. Так, 23 листопада 2016 р. Європейським Парламентом прийнято резолюцію[7] «Стратегічні комунікації ЄС, як протидія пропаганді третіх сторін», в якій європейським інституціям було надано низку рекомендацій, яких вони мають вжити для зменшення впливу російської дезінформації.

В 2018 році Єврокомісія представила «План дій проти дезінформації»[8], який з одного боку став наслідком дезінфор-

7. https://goo.gl/9jddH6
8. https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf

маційної кампанії навколо подій в Солсбері, а з іншого – наслідком широких дискусій у Європейському парламенті, Раді Європи та самій Єврокомісії з цього питання. Хоча документ вказує, що число суб'єктів, які вдаються до дезінформації по відношенню до ЄС зростає (і вони є, як державними, так і недержавними), однак ключовою загрозою залишається РФ, що «має належні ресурси, якісну координацію та таргетованість, а також націленість на стратегічні цілі».

> *Представлені нижче дії, спрямовані на запобігання маніпулятивному поширенню шкідливого вмісту, шляхом збільшення прозорості, обмеження маніпулятивних методів та зменшення економічних стимулів для розповсюдження дезінформації, а також на запровадження стримування шляхом збільшення ціни, яку платять суб'єкти, що беруть участь в операціях впливу та іноземному втручанні.*
>
> ***European democracy action plan***

План дій встановлює 4 базових пріоритети (стовпи), на яких базується побудова відповіді ЄС на загрози дезінформації:

- поліпшення спроможностей ЄС у виявлені, аналізі та викритті дезінформації;
- посилення скоординованості та спільних відповідей на дезінформацію;
- мобілізація приватного сектору на зменшення дезінформації;
- підвищення обізнаності та поліпшення соціальної стійкості.

Хоча у преамбулі документу підкреслюється, що соціальні мережі є особливо важливим специфічним простором поширення дезінформації, але жоден із вказаних стовпів немає специфічних заходів, спрямованих на протидію дезінформації саме в соціальних мережах та цифрових медіа.

В 2020 році Європейська комісія прийняла комплексний документ, що має сприяти ліпшому захисту Європи від стороннього впливу – «План дій для європейської демократії» (*European democracy action plan*)[9]. Преамбула документу підкреслює, що «Демократія – це не те, що треба сприймати, як належне» і вона потребує підтримки та захисту, в т.ч. від атак на неї, що посилились останнім часом. Особливо це стосується атаки на виборчий процес, поширення дезінформації, погіршення медіа середовища. Особливий акцент документа – цифрове середовище, яке «дозволило політичним акторам взаємодіяти з

9. https://ec.europa.eu/info/sites/info/files/edap_communication.pdf

кожним виборцем… однак, стрімке зростання онлайн компаній та онлайн платформ також відкрило нові уразливості та зробило більш складним підтримання цілісності виборів, ускладнило переконаності в тому, що медіа вільні та плюралістичні, а демократичний процес захищений від дезінформації та маніпуляцій». Документ окреслює і можливі заходи ЄС в частині протидії ворожим впливам. Крім традиційного викриття самих операцій впливу та методів, які в них застосовуються («з метою зробити їх оперативно не придатними»), пропонується розглянути можливість накладання санкцій за таку діяльність, для того щоб зробити їх проведення менш вигідним для ініціаторів.

Цей документ на сьогодні – найбільш цілісна політична позиція ЄС з питань протидії деструктивним впливам на демократичний процес, а також генеральний план захисту демократії. Він показує і певну еволюцію поглядів ЄС, яка від теми суто протидії дезінформації, як елементу операцій впливу, перейшла до створення комплексних планів захисту демократії від впливу, як такого.

Поряд з цією лінією вироблення політики ЄС розвивав і практичні інструменти стримування та протидії. Першим з таких практичних інструментів загальноєвропейського рівня з протидії дезінформації став *East StratCom Task Force* – орган публічної дипломатії при Європейській службі зовнішньої діяльності. Діяльність цього органу (зокрема, його ефективність) довгий час викликала (а подекуди – і викликає) сумніви.

Його діяльність розпочалась вже у вересні 2015 року[10] і була спрямована на:

- роз'яснення ключових аспектів політики Європейського Союзу, створення його позитивного іміджу та протидія дезінформації;
- забезпечення ефективної комунікації та просування політики ЄС щодо Східного партнерства;
- загальний розвиток медійного простору в країнах Східного партнерства та країнах-членах ЄС, що передбачає сприяння свободі ЗМІ;
- вдосконалення механізмів, що уможливлюють передбачення, оцінку та реагування ЄС на дезінформацію, яка поширюється зовнішніми акторами;
- надання інформаційної підтримки делегаціям ЄС в Азербайджані, Вірменії, Білорусі, Грузії, Молдові, Україні;

Одним з важливих (і, як виявилось у стратегічній перспек-

10. https://euvsdisinfo.eu.

тиві – ефективних) інструментів, який створив East StratCom Task Force став проект «EUvsDisinfo». EUvsDisinfo виявляє та розкриває випадки дезінформації, створені про кремлівськими ЗМІ, які розповсюджуються в країнах ЄС та Східного партнерства. Станом на 2019 рік проект зібрав близько 6500 прикладів кремлівської дезінформації[11]. Створення цієї служби стало і прикладом практичної адаптації українського досвіду протидії дезінформації Європейським Союзом. За словами Якуба Каленського, саме українська організація StopFake стала прототипом EU vs. Disinfo, яка наслідувала системний підхід StopFake. Її завданням було збирати фейки різними мовами в різних країнах, щоб можна було простежити їхній шлях від появи до поширення[12].

В 2018 році EEAS визначив основні пріоритети ЄС у сфері протидії гібридним загрозам наступним чином[13]:

- активні стратегічні заходи в сфері оптимізації протидії фейковим новинам;
- зміцнення кібербезпеки в Європі із вжиттям великої кількості конкретних заходів та удосконаленням механізмів реагування;
- вжиття заходів із протидії дезінформації в мережі Інтернет задля безпеки користувачів, організація більш ефективного інформування зацікавлених осіб про ЄС та його політику, а також задля недопущення втручання у вибори;
- посилення контррозвідувальних заходів на рівні ЄС, зокрема, координація такої діяльності з НАТО та країнами-членами;
- розширення спроможностей із виявлення гібридних загроз та вжиття відповідних заходів проти компаній з дезінформації. При цьому спроби протидії та реагування на гібридні загрози мають базуватись на спроможності виявлення шкідливих дій та їх джерел, як всередині ЄС, так і за його межами, на ранній стадії, а також на розумінні зв'язків між подіями, які на перший погляд здаються зовсім різними.

ЄС вже вдається до таких заходів протидії[14]. Зокрема надається системна підтримка **європейській мережі факт-чекерів** через софінансування[15] платформи «InVID project», яка

11. https://euvsdisinfo.eu/ru/%d0%be-%d0%bd%d0%b0%d1%81/
12. https://detector.media/infospace/article/186363/2021-03-26-chotyry-linii-borotby-z-dezinformatsiieyu/
13. https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46536/node/46536_ru
14. https://www.youtube.com/watch?v=-KH1uj1ZB3A
15. https://multimedia.europarl.europa.eu/en/this-is-what-europe-does-for-fact-checkers_EPB100_EN-A_a

дозволяє виявити, перевірити на надійність та точність відео (і фото) контент, що поширюється через соціальні медіа[16]. Також одним з елементів протидії є **сприяння якісній журналістиці**.

Хоча фактчекінг продовжує залишатись основою реактивної діяльності європейських структур (як на загальноєвропейському, так і національному рівні) на дезінформацію, однак сумніви щодо реальної ефективності такої діяльності лише посилюється. Майже загально визнаним є розуміння обмежених можливостей донести інформацію про розвінчування фейку до аудиторії, яка раніше вже побачила фейк, вплинути на її початково сформоване відчуття. Крім того, залишається обґрунтований сумнів, чи не виступає розвінчування фейків ще одним каналом їх фактичного поширення, адже дозволяє дізнатись про них навіть тим споживачам, які до того могли і не знати про його існування.

Було зроблено чимало корисних чи зайвих дій, проектів та програм, коли ресурси були спрямовані лише на те, щоб постійно розвінчувати ті чи інші вигадки, фейки. Це все має реактивний характер, що відволікає увагу та ресурси. Небезпека цього – у помилковому враженні щодо ефективності діяльності. Цього недостатньо і цього непотрібно робити в таких обсягах, як це почалось у 2014 році.

Дмитро Теперик

Ще один інструмент протидії – Європейська обсерваторія цифрових медіа (European Digital Media Observatory). Це створений коштами Європейської комісії консорціум (керівництво яким здійснює European University Institute у Флоренції), який включає також Datalab у Aarhus University, Athens Technology Center (обидва – надають технологічну підтримку), а також координують Соціальну обсерваторію щодо дезінформації та аналізу соціальних медіа (Social Observatory for Disinformation and Social Media Analysis (SOMA).

Цей проект забезпечує функціонування безпечної онлайн платформи для академічного аналізу дезінформаційних кампаній, проводить навчання та поширення знань про дезінформацію, підтримує та фасилітує діяльність фактчекерів у Європі, підтримує та модерує наукові дослідження щодо дезінформації у Європі, надає підтримку державним органам у моніторингу заходів, які вживаються онлайн платформами для обмеження розповсюдження та впливу дезінформації.

16. ©https://sdelano.media/invid/

3.4. Протидія впливам у цифровому просторі: відносини з платформами

ЄС звертає особливу увагу на небезпеку поширення дезінформації, яка походить з соціальних мереж, що стають джерелом стрімкого поширення чуток, напівправди та відвертої брехні (того, що ЄС і вважає дезінформацією). Занепокоєння полягає в тому, що соціальні медіа надають традиційному і давньому явищу дезінформації нової якості – швидкості поширення, ускладнення аналізу та спростування. Особлива небезпека – діяльність бот-мереж і тролів, що дозволяють забезпечувати ширше охоплення ворожими наративами та неправдивими повідомленнями. Кількісне збільшення дезінформації призводить до того, що люди частіше її поширюють. Питання відносин із соціальними медіа залишається складним та неоднозначним. Базова ідея визначення ролі та місця соцмедіа у цих процесах полягає в тому, що не ЄС має вдаватись до жорстких заходів регулювання, але більшу відповідальність мають прийняти на себе самі соціальні медіа.

Певною проблемою для обох сторін (європейських представників та власників платформ) є те, що відсутні чіткі та неспростовні дані чи дійсно операції впливу, які здійснюються за допомогою платформ ефективні. Парадоксальним чином це дає аргументи кожній із сторін, адже дозволяє трактувати сумніви на свою користь. Цьому сприяє і сформована за ці роки суспільна думка, що такі операції, які проводяться через покупку таргетованої реклами чи окремих повідомлень, дають їх авторам можливість додаткового впливу. Спроби пов'язати кількість переглядів повідомлень із ефектом впливу здебільшого невдалі, а ініціативи більшого розкриття інформації платформами будуть наштовхуватись на природні обмеження в частині комерційної таємниці.

Розуміючи, що самі соціальні мережі не будуть змінювати свою поведінку, ЄС вдається до заходів, що мають спонукати адміністрації соціальних платформ переглянути свою діяльність, зробивши їх більш прозорими та відповідальними. Одним з таких інструментів є виконання Кодексу практик (*Code of practice*) щодо протидії фейковому контенту та фейковим акаунтам.

Слід відмітити, що ідея «більшого регулювання» та «контролю» кореспондується з іншими ініціативами ЄС, які вже набули свого втілення. Прикладом цього стало прийняття законодавства щодо GDPR, яке встановило жорсткі правила щодо

персональних даних європейських громадян. Схожа тенденція спостерігається і щодо кібербезпеки – NIS Directive та більш нових законодавчих ініціатив, все більш впевнено впроваджують механізми сертифікації для ІТ-систем (що є предметом тривалих дискусій з США).

Посилення жорсткості підходу ЄС щодо діяльності соціальних мереж можна пояснити і напруженими відносинами, що склались між європейськими функціонерами (в т.ч. євро парламентарями) та керівниками великих соціальних мереж. Так, у позиційному матеріалі[17] Дослідницької служби Європарламенту (*European Parliamentary Research Service*) щодо заходів, які вживає Європа для протидії дезінформації підкреслюється, що Марк Цукерберг у травні 2018 року уникав питань євро парламентарів щодо захисту даних, фейкових новин та безпеки виборів. При цьому оприлюднені у грудні того ж року конфіденційні листи Цукерберга свідчать, що FB таємно надавав певним компаніям доступ до даних друзів користувачів і ще це питання викликає питання до етики FB загалом.

Європейська комісія спробувала знайти проміжне рішення щодо взаємодії з онлайн платформами шляхом укладання в 2018 році Кодексу практик щодо дезінформації (*Code of Practice on Disinformation*)[18] – першої погодженої всесвітньої угоди представників онлайн індустрій, яка базується на відповідальній поведінці та стандартах саморегуляції для боротьби з дезінформацією. Цю угоду підписали Facebook, Google, Twitter та інші онлайн компанії. В 2019 році було опубліковано перший річний звіт про виконання, за яким Єврокомісія зробила висновок про прогрес в цьому питанні.

Зокрема звіт вказує, що платформи посилюють горизонтальне співробітництво один з одним. Водночас слабко вираженою залишається співпраця платформ із незалежними дослідниками – платформи неохоче йдуть на надання їм даних та відповідних інструментів для пошуку маніпуляцій у повідомленнях. Таке співробітництво, якщо і виникає, є епізодичним, не охоплює всі європейські мови. Найбільші здобутки спостерігаються у діях платформ, які спрямовані на зменшення можливостей ініціаторів дезінформації поширювати її через рекламний контент, поліпшення прозорості політичної реклами та посилення боротьби з ботами, підробними обліковими записами і загалом не аутентичною поведінкою. Але для всіх цих здобутків

17. https://epthinktank.eu/2018/04/24/online-disinformation-and-the-eus-response/
18. https://ec.europa.eu/digital-single-market/en/code-practice-disinformation

Єврокомісія констатує, що зусилля не виглядають цілісними і різні підписанти Кодексу рухаються із різною швидкістю на цьому шляху.

Хоча існували і існують очікування, що події січня у 2021 року в США призведуть до більш жорсткої позиції і Єврокомісії і Європарламентарів щодо механізмів забезпечення відповідальності соцмереж за контент і загалом щодо підвищення прозорості їх діяльності, однак реальність може бути іншою. Хоча 6 січня 2021 року Twitter і Facebook (а також декілька інших соціальних мереж) спочатку обмежили, а потім і заблокували його акаунти в своїх мережах, однак Європа сприйняла цю ситуацію у притаманних для неї підходах.

Готовність соціальних мереж (а також платформ, від яких багато в чому залежить сьогоднішнє міжнародне спілкування, на кшталт Google Play Market та Apple Store) приймати такі рішення самостійно, волюнтаристські, без жодних пояснень та оминаючи власні правила викликає занепокоєння у європейських очільників. Це може призвести до спроб ЄС зробити Code of Practice on Disinformation більш обов'язковим для всіх онлайн учасників та посилити відповідальність платформ аж до заходів, аналогічних GDPR. Водночас це не характеризує негативно поточний рівень ефективності заходів, вже вжитих платформами для більшого контролю за підозрілою активністю.

> *Хоча це [події 6 січня] був шок і для Європи, однак багато хто не сприйняв рішення соцмереж Twitter чи Facebook заблокувати президента Трампа назавжди. Це сприймалося тут більшістю людей, як обмеження свободи слова, свободи висловлювання.*
>
> ***Девід Стулік***

Кодекс практики та підготовлені на його основі звіти вже почали призводити до формування більш системного діалогу між європейськими інституціями та платформами. Вже загаданий вище документ 2020 року «План дій для європейської демократії» також звертається до проблеми відносин з платформами, прямо вказуючи, що розроблені у п. 4.2. пропозиції («Більше зобов'язань та відповідальності для онлайн-платформ») стали наслідком саме оцінки функціонування Кодексу практики. Основний висновок і стратегію, яку формулює на його основі Європейська Комісія – платформи мають бути більш прозорими та підзвітними, а система цієї підзвітності має бути більш стабільною, ніж добровільні звіти платформ.

Рамку такої підзвітності має задати Закон про цифрові послуги (The Digital Services Act, DSA[19]). План дій так описує сутність цього закону: «Він запропоновує правила для забезпечення більшої підзвітності щодо того, як платформи модерують вміст, рекламу та алгоритмічні процеси. Дуже великі платформи будуть зобов'язані оцінювати ризики, які їх системи становлять, не лише щодо нелегального вмісту та продуктів, але й системних ризиків для захисту суспільних інтересів, фундаментальних прав, громадського здоров'я та безпеки. У цьому контексті дуже великим платформам також потрібно буде розробити відповідні інструменти управління ризиками та вжити заходів для захисту цілісності своїх послуг від використання в них маніпулятивних методів. DSA надасть користувачам значні можливості оскаржити рішення платформ щодо видалення або позначення вмісту».

На даному етапі основний об'єкт цього закону – вказані «великі платформи», які завдяки своєму положенню на ринку мають найбільший потенціал впливу на суспільну ситуацію та економіку ЄС. Але і для менших платформ також встановлюються правила, які мають зобов'язати їх боротись із незаконною діяльністю своїх користувачів, забезпечити свою прозорість (в т.ч. – для ліпшої комунікації між власниками цих платформ та державними структурами чи іншими зацікавленими особами). Також закон встановлює додаткові правила щодо розміщення реклами (передусім – політичної). Для ліпшої взаємодії з цих питань, а також для нагляду за дотриманням відповідного законодавства, пропонується створити (або визначити з існуючих установ) Координатора цифрових послуг (Digital Services Coordinator) у кожній державі-члені.

19. https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN

НАТО ПРОТИ ОПЕРАЦІЙ ВПЛИВУ:

СПІЛЬНА З ЄВРОПОЮ ВІДПОВІДЬ НА ГІБРИДНІ ЗАГРОЗИ

РОЗДІЛ 4

4. НАТО ПРОТИ ОПЕРАЦІЙ ВПЛИВУ: СПІЛЬНА З ЄВРОПОЮ ВІДПОВІДЬ НА ГІБРИДНІ ЗАГРОЗИ

Особливістю НАТО є те, що Альянс – це, насамперед, військово-політичний союз, з самого початку створений для протидії жорстким викликам безпеки та забезпечення колективної оборони країн-членів.

Найбільш дієвий та радикальний механізм закладений в ст. 5 Вашингтонського договору, який ототожнює напад на одну країну із нападом на всі країни – учасниці Альянсу. Водночас зазначений інструмент був використаний єдиний раз – під час терактів 11 вересня 2001 року в США[1]. Однією з основних причин того, що традиційний інструментарій зовнішньої та безпекової політики є більше недієвим, полягає в видозміненні форм міжнародних конфліктів, яке відбувається на тлі «революції у військовій справі».

Цілі та задачі, які раніше вирішувались здебільшого військовим шляхом, можуть досягатись задіянням комплексу взаємопов'язаних заходів в інших сферах. Не в останню чергу цьому сприяють глобалізація економіки та промисловості, інтернаціоналізація медіа, більша відкритість суспільств, побудованих на ліберальних цінностях, уразливість демократичних систем для зовнішнього впливу та маніпулятивних технологій.

Розвиток сучасних інформаційно-комунікаційних технологій, у тому числі технологій транскордонної передачі даних, їх збереження та пошук, зумовили появу глобального інформаційного середовища, в якому функціонують різноманітні потужні цифрові платформи для комунікації чи надання сервісів, ведення бізнесу, отримання освіти чи довідкової інформації, розраховані на багатомільйонні аудиторії. До того ж розвитку набули технології маніпулювання індивідуальною та груповою свідомістю, які беруть свої витоки, з одного боку, з традиційної реклами та маркетингу, з іншого боку, від спеціальної пропаганди та інформаційних воєн, які з 80-х років є невід'ємною частиною воєнної стратегії. Піонером в цьому є США, яка першими офіційно включили інформаційні війни та інформаційні операції до військових доктрин та настанов. Водночас, все ж таки інформаційне супроводження розглядалось на той час, як допоміжний елемент воєнної кампанії, здатний суттєво вплинути на її перебіг, але все ж таки похідний від її замислу.

Зазначені вище зміни призвели до того, що «нав'язати

1. https://www.nato.int/nato-welcome/index.html

противнику свою волю», як мету війни за класичним визначенням Клаузевіца [2] стало можливим досягнути не воєнним (або не тільки і не стільки воєнним) шляхом.

Хоча тренд на «гібридизацію» конфліктів окреслився після ІІ Світової війни, формальне оголошення війни СРСР Японії було чи не останнім юридично оформленим початком війни в історії людства, остаточно доктрина гібридних війн була сформульована начальником Генерального Штабу ЗС РФ В. Герасимовим у широко відомому виступі перед Академією воєнних наук із доповіддю про гібридну війну в лютому 2013 року. Основні тези цієї доповіді були згодом надруковані в статті «Ценность науки в предвидении» у виданні «Военно-промышленный курьер»[3]. Серед її важливих положень слід відзначити задеклароване співвідношення невоєнних та воєнних заходів, як 4 до 1. У вказаній доповіді також наголошується на важливості ведення інформаційного протиборства, підтриманні опозиційних рухів та, зрештою, заміни уряду противника на більш лояльний. До цього ж слід додати відпрацьовані в Росії теоретичні та ймовірно практичні засади рефлексивного управління, тобто вплив на цикл прийняття рішень противником.

Практичну реалізацію Доктрини Герасимова можна було спостерігати в українсько-російському конфлікті з початку 2014 року, яка фактично змусила замислитись Альянс про стратегію протидії гібридній агресії, адже з точки зору міжнародного гуманітарного права її важко класифікувати, як звичайну збройну агресію, а отже це унеможливлює надання адекватної і - що найголовніше – своєчасної відповіді.

На сьогоднішній день під «гібридною війною» в НАТО розуміють тактику, яка складається із пропаганди та дезінформації, методів економічного тиску, а також таємного використання сил спеціального призначення. Захід неодноразово звинувачував Росію у веденні «гібридної війни» проти України, відзначаючи, зокрема, масивну пропаганду в державних ЗМІ, а також використання під час анексії Криму і конфлікту на Донбасі військовослужбовців в уніформі без розпізнавальних знаків.

Наприкінці 2015 року Генеральний секретар НАТО Єнс Столтенберг, виступаючи на зустрічі Міністрів закордонних справ країн НАТО в Брюсселі, заявив, що дії Росії в Україні спонукали НАТО продумати механізми протидії агресії, яка не вигля-

2. Клаузевиц К. О войне. — М.: Госвоениздат, 1934. / Clausewitz K. Vom Krieg. 1832/34.
3. Герасимов В. В. Ценность науки в предвидении // Военно-промышленный курьер. 2013. № 8(476). 27 февр.

дає, як прямі військові дії. Альянс прийняв нову стратегію з боротьби з загрозою так званої «гібридної війни». Оскільки мова йде про суміш «військової та цивільної загрози», Альянс має намір погоджувати свої дії з Європейським Союзом.

Генсек НАТО не став детально викладати суть нової стратегії. За словами Столтенберга вона базується на «трьох китах: підготовці, стримуванні і обороні». Серед механізмів протидії гібридним загрозам, крім покращення в роботі розвідувальних служб і обміні розвідданими, є і можливість застосування спеціальних сил швидкого реагування. Генсек також зазначив, що ведення гібридної війни проти будь-якої країни Альянсу, повинно приводити в дію п'яту статтю статуту НАТО про колективну оборону в разі агресії[4].

Основні положення Стратегії реагування на гібридні загрози передбачають:

- удосконалення обміну розвідувальними даними;
- забезпечення раннього попередження для прогнозування і фіксування гібридної воєнної діяльності (передусім з боку РФ);
- використання державними та недержавними суб'єктами у протистоянні гібридним загрозам широкомасштабних і тісно поєднаних між собою традиційних та нетрадиційних засобів, відкритої та прихованої військової сили, воєнізованих формувань та заходів цивільного характеру;
- розроблення набору індикаторів раннього попередження для опрацювання різних варіантів реагування на кризові ситуації;
- можливість прийняття Північноатлантичною радою НАТО рішення про приведення у дію статті 5 Вашингтонського договору для протидії гібридній війні у рамках колективної оборони;
- продовження ефективної співпраці та координації зі своїми партнерами та відповідними міжнародними організаціями (зокрема, ЄС), відповідно до домовленостей, спрямованих на протидію гібридній війні.

Таким чином, можна констатувати, що протягом відносно короткого проміжку часу Альянс спромігся оцінити нову загрозу та відпрацювати, принаймні на політичному рівні шляхи протидії їй.

Практично одночасно, на початку квітня 2016 Єврокомісія ухвалила «Спільні принципи протидії гібридним за-

4. https://p.dw.com/p/1HFcl

грозам — відповідь Європейського Союзу» (Joint Framework on countering hybrid threats a European Union response[5]). У Спільних принципах наголошується на необхідності вироблення державами-членами узгоджених механізмів реалізації стратегічних комунікацій для протидії дезінформації та публічного викриття гібридних загроз. Документ визначає, що діяльність у сфері стратегічних комунікацій передбачає тісну взаємодію з НАТО. Зазначається, що співпраця ЄС та НАТО дозволить обом організаціям більш ефективно реагувати на гібридні загрози.

Також у документі стверджується, що провокатори можуть систематично поширювати дезінформацію, у тому числі в межах цілеспрямованих кампаній у соціальних мережах, прагнучи радикалізації окремих індивідів та дестабілізації суспільства. Стратегічні комунікації мають сповна використовувати соціальні медіа, а також традиційні візуальні, аудіо та інтернет ЗМІ. Фактично, саме ЄС є основним партнером НАТО у протидії гібридним загрозам НАТО. Тобто НАТО, як військово-політична організація, продовжуватиме й надалі протидіяти насамперед жорстким викликам безпеки, ЄС же відповідатиме за протидію «м'якій силі».

Спільна декларація з цього питання між ЄС та НАТО була підписана Генеральним секретарем НАТО Єнсом Столтенбергом і президентами Європейської комісії і Ради Жан-Клодом Юнкером і Дональдом Туском в липні 2016 року у Варшаві. В ній міститься «спільний набір пропозицій» із 74 конкретних дій, багато з яких зосереджені на гібридних загрозах, розвитку стійкості в аспекті кібербезпеки і стратегічних комунікаціях. Друга Спільна декларація, узгоджена в Брюсселі в липні 2018 року, привернула додаткову увагу до військової мобільності, протидії тероризму і стійкості до ризиків застосування хімічних, біологічних, радіологічних і ядерних агентів. НАТО також швидко прийняла стратегію протидії гібридним загрозам на основі горизонтального «всенатовського» підходу.

За узгодженими поглядами експертів НАТО та ЄС гібридні загрози поєднують традиційні та нетрадиційні, воєнні та невоєнні дії, які координуються державними або недержавними суб'єктами, що ставлять перед собою певні політичні цілі. Гібридні кампанії є багатовимірними, поєднують в собі, як примусові, так і провокативні заходи, використовують традиційні і нетрадиційні інструменти й тактики. Вони реалізуються таким чином, щоб їхнє джерело було важко ідентифікувати. Загрози

5. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

такої природи впливають та критично важливі слабкі місця. Їх завданням є заплутати противника та ускладнити ухвалення швидких та ефективних рішень.

Гібридні загрози можуть варіюватись від кібератак на важливі інформаційні системи, порушення функціонування критично важливих послуг (публічні послуги, енергопостачання, банківські послуги тощо) до підриву довіри суспільства до урядових установ чи, то поглиблення соціальних протирічь. Також наразі до гібридних загроз відносять загрози пов'язані з використанням хімічних, біологічних, радіаційних чи ядерних речовин, доставлених нетрадиційним способом. Отже, головною особливістю гібридних загроз є їхня динамічність та, відповідно, неможливість надати чітку дефініцію.

Подібно Європейському союзу, НАТО створила засоби моніторингу і аналізу гібридних загроз на основі роботи розвідувальних служб і у співпраці з іншими установами НАТО. Більше того, НАТО створила групи підтримки протидії гібридним загрозам, які можуть залучатись на підтримку відповідних органів ураженої країни.

На додаток до забезпечення співробітництва між НАТО і ЄС довгоочікуваною платформою спільних інтересів, протидія гібридним загрозам привела до низки подій в Європейському союзі. Європейська комісія і Європейська служба зовнішніх справ (EEAS) створили міжвідомчу групу з протидії гібридним загрозам, яка проводить регулярні засідання на різних рівнях. Ця група покликана забезпечувати спільну обізнаність з подіями і процесами за допомогою європейських інституцій, що стосуються протидії гібридним загрозам і є першим перспективним кроком до комплексної моделі викликів у галузі безпеки. В ідеалі, вона може сприяти появі більш потужної платформи цивільної і економічної готовності, кібербезпеки та інших питань, які по суті стосуються багатьох секторів.

Одним з найбільш конкретних результатів спільної роботи ЄС та НАТО з протидії гібридним загрозам став Центр передового досвіду з гібридних загроз в Гельсінкі. Ще у 2016 році Європейська комісія і EEAS розробили Об'єднану структуру протидії гібридним загрозам, що складається із 22 заходів для країн-учасниць і інституцій, які визначають підходи до виявлення гібридних загроз, покращують інформованість про них і здійснюють кроки з розвитку стійкості.[6] Хоча ці заходи в жодному

6. https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozam/index.html

разі не є вичерпними, структура продемонструвала чітке бажання зробити протидію гібридним загрозам пріоритетом для ЄС. Найбільш відчутними результатами діяльності структури стало створення в рамках Розвідувального і ситуаційного центру ЄС групи зі збирання даних про гібридні загрози і Європейського центру передового досвіду з протидії гібридним загрозам в Гельсінкі.

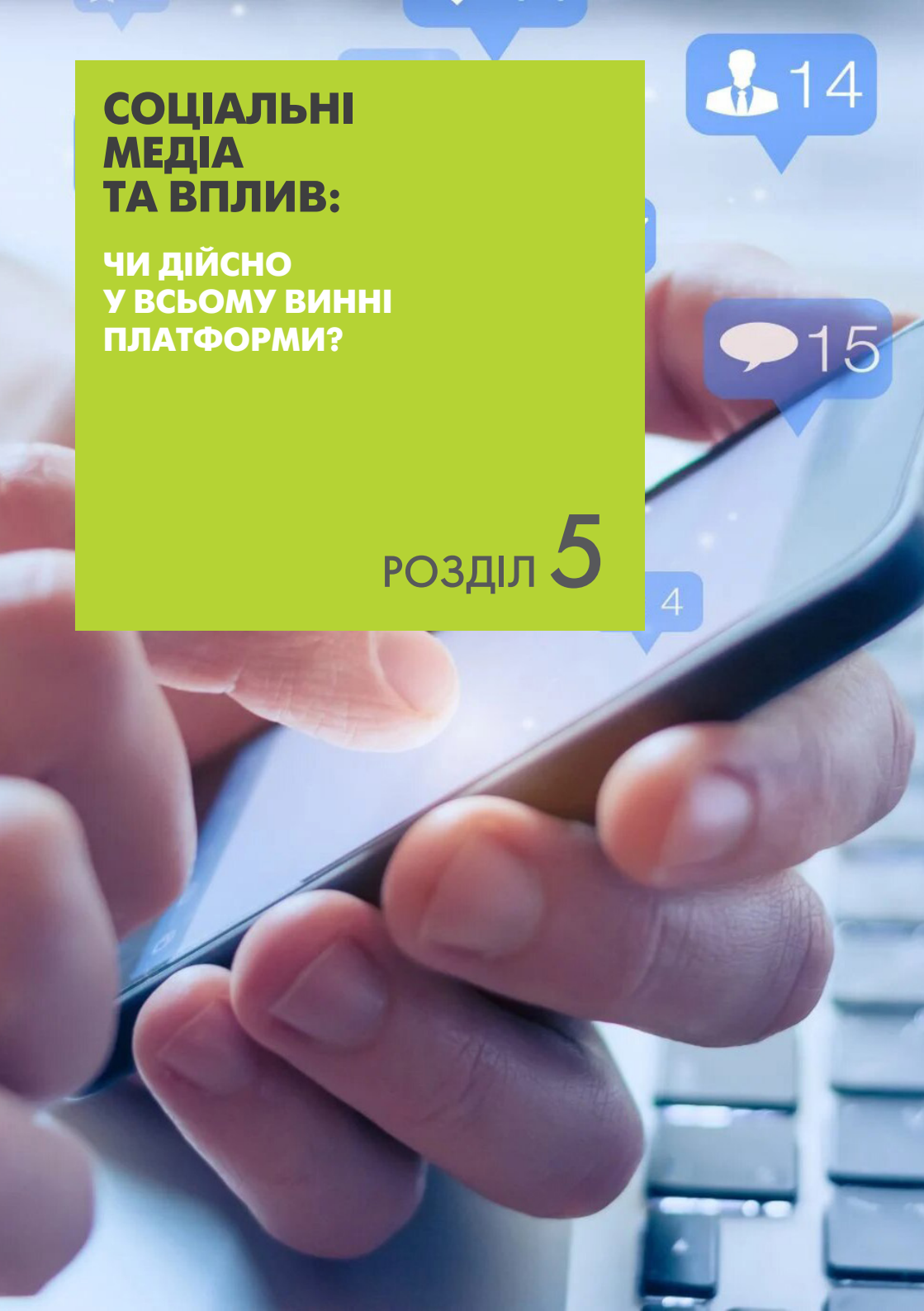
Рішення про створення фінського Центру було ухвалене в квітні 2017 представниками країн НАТО та ЄС, але оперативної спроможності він набув у вересні 2017 року. Засновниками центру стали 12 країн: Фінляндія, Швеція, Норвегія, США, Франція, ФРН, Великобританія, Іспанія, Польща, Естонія, Латвія і Литва. Початковий річний бюджет Центру становить близько 1,5 млн Євро.

Метою Центру є протидія «новим загрозам, спрямованим на дестабілізацію ситуації в європейських країнах». Діяльність Центру спрямовано на:

- проведення досліджень, аналіз гібридних загроз та методів боротьби з ними;
- організацію спільного навчання для країн-учасниць;
- проведення консультацій на стратегічному рівні між учасниками ЄС та НАТО,
- залучення до діалогу урядових та неурядових експертів.

Ще однією інституцією, яка також обіймає важливе місце в системі протидії гібридним загрозам є Центр передового досвіду з питань стратегічних комунікацій (The NATO Strategic Communications Centre of Excellence)[7], який знаходиться в м. Рига, Латвія. Вказаний центр був утворений в червні 2014 року за участі Латвії, Естонії, Італії, Литви, Польщі, Великобританії та Німеччини. Метою його діяльності є розвиток спроможностей НАТО у сфері стратегічних комунікацій. Центр є воєнною структурою НАТО та має статус міжнародної воєнної організації. Зазначена установа здійснює науково-аналітичну, навчально-методичну та інформаційно-комунікативну діяльність. Ним розроблено низку спеціальних навчальних курсів зі стратегічних комунікацій; видається журнал «Стратегічні комунікації у сфері оборони» (Defence Strategic Communications); здійснюються теоретичні та прикладні дослідження; проводяться конференції та семінари на теми: роль пропаганди в сучасному світі, російська інформаційна війна проти України, маніпулятивні техніки, перетворення соціальних медіа на зброю, практика НАТО щодо стратегічних комунікацій тощо.

7. https://www.stratcomcoe.org/



СОЦІАЛЬНІ МЕДІА ТА ВПЛИВ:

ЧИ ДІЙСНО У ВСЬОМУ ВИННІ ПЛАТФОРМИ?

РОЗДІЛ 5

5. СОЦІАЛЬНІ МЕДІА ТА ВПЛИВ: ЧИ ДІЙСНО У ВСЬОМУ ВИННІ ПЛАТФОРМИ?

5.1. Інтернет платформи та їх роль у врегулюванні питання впливу

Платформи стали інноваційним явищем у медіа просторі, чий вплив на суспільні процеси ще до кінця не вивчено. Вони зазнали значного розвитку та розповсюдження наприкінці першої декади XXI сторіччя. В їх основі лежить ідея з'єднати між собою знайомих осіб для підтримки зв'язку та дружнього спілкування.

В 2009 році Twitter несподівано голосно заявив про себе, як фактор міжнародного політичного життя, і вперше з'явилося поняття «Twitter революція». Непідконтрольна уряду глобальна соціальна мережа стала основним джерелом інформації про протести проти фальсифікації результатів виборів Президента Ірану, завдяки фото та відео, якими на платформі Twitter ділилися учасники подій. З'явилося поняття громадських журналістів.

Ще більш значну роль Twitter та Facebook зіграли під час подій 2010-2012 років, відомих, як Арабська весна. Хвиля масових протестів, яка почалась в Тунісі 17 грудня 2010 року призвела до падіння декількох авторитарних режимів на Близькому Сході та у Північній Африці. Під час цих подій Facebook та Twitter не лише слугували платформою для розміщення інформації та вільного висловлення думки, а й допомагали мережі активістів організовувати протестну діяльність та скоординовано інформувати про неї світ. Подібну роль вони відіграли і під час протестів проти результатів виборів у Молдові.[1] Соцмережі отримали ауру інструменту звільнення від авторитаризму та побудови демократії, яка вкладалась у домінуючий на Заході дискурс третьої хвилі демократизації.

Як наслідок, втручання Російської Федерації у вибори Президента США 2016 року застали Захід зненацька. Широко обговорювані сьогодні операції впливу з використанням можливостей соціальних мереж навіть не фігурували серед потенційних загроз. В листопаді 2016 засновник і власник Facebook Марк Цукерберг назвав думку, що його платформа могла ста-

1. https://digital.report/twitter-revolyutsiya-v-moldove-otsenka-vosem-let-spustya/

ти інструментом впливу на виборців «доволі божевільною»,[2] а звіт розвідувального співтовариства США від 6 січня 2017 року[3] згадував російських тролів лише побіжно. Серед медіа, основну увагу його автори приділили російському телебаченню, орієнтованому на закордонні аудиторії (Russia Today (RT) та Spunik).

Як стало відомо пізніше, російська кампанія впливу на вибори США складалась з оффлайн та онлайн компонентів. В оффлайн брали участь державні телеканали іномовлення РФ (Супутник та Russia Today), які також агресивно просували свій контент онлайн, здійснювалися особисті контакти з виборчою кампанією Трампа. Онлайн Росія отримала доступ до машин для голосування у багатьох штатах, було проведено операцію ГРУ (hack and leak), під час якої в Інтернеті було розповсюджено викрадену електронну переписку представників передвиборчого штабу Гілларі Клінтон, а також кампанію прихованого впливу від приватної компанії «Агенція з досліджень інтернету». Кампанія в інтернеті була спрямована переважно на збільшення конфліктності в американському суспільстві.

Інший приклад таких кампаній (на яких відпрацьовувались і подальші втручання російськи тролі) – історія із «вибухом на Columbian Chemical»[4].

Близько 8:30 ранку 11 вересня 2013 року в окрузі Сент-Мері штату Луїзіана почалось лавиноподібне поширення інформації про те, що на місцевому заводі Columbian Chemicals стався вибух і є ризик потрапляння в повітря шкідливих речовин. Спочатку в Twitter, а потім і в ЗМІ почали поширювати картинку, на якій начебто зображено, як горить завод компанії і у небо підіймається стовп чорного диму.

З самого ранку місцеві мешканці почали отримувати СМС наступного змісту: «До 13:30 в даній місцевості зберігається небезпека небезпечних випаровувань – спробуйте знайти укриття. За додатковою інформацією звертайтесь до місцевих ЗМІ або на сайт columbiachemical.com». Пізніше громадяни почали активно дзвонити до урядових структур та місцевих ЗМІ, намагаючись з'ясувати наскільки небезпечна ситуація.

2. https://apnews.com/article/1fc42b60a63e49568f0b3707a36c6b23
3. «Background to «Assessing Russian Activities and Intentions in Recent US Elections»: The Analytic Process and Cyber Incident Attribution» https://www.dni.gov/files/documents/ICA_2017_01.pdf
4. https://www.nytimes.com/2015/06/07/magazine/the-agency-russian.html?

Одночасно з цим інформація про вибух активно почала розганятись через Twitter. Деякі користувачі (наприклад, @AnnRussel) активно поширювали вказане фото вибуху, а інші розповідали, що чули потужний вибух, який було чутно за багато миль. Ще один користувач виклав відео з бензоколонки, на якому видно спалах, як при вибуху. Інший користувач запостив картинку з сайту CNN, де видно, що новина вже потрапила у загальнонаціональні новини. Оперативно з'явилось відео, на якому в центрі кадру було видно телевізор із записом відео, де люди у масках представлялись бійцями ІДІЛ і щось казали арабською, а коментатор (який начебто зробив цей запис) каже, що вони беруть на себе відповідальність за вибух. З багатьох Twitter-акаунтів із начебто американськими іменами та прізвищами почали поширюватись твіти на адресу відомих осіб з вимогами зробити хоч щось або взагалі почати когось бомбити, якщо за вибухом стоїть ІДІЛ.

Фальшивкою було все – фотографія вибуху, скріншот CNN, відео ІДІЛ та сотні Twitter-акаунтів, які розганяли цю новину. Зловмисники підготувались досить добре. Вони не просто намалювали картинку «під CNN» - вони створили цілу низку клонів місцевих ЗМІ. У Вікіпедії було оперативно створено сторінку про вибух на заводі, в якій активно посилались на фальшиві «докази». І все це активно просувалось через мережу фальшивих ботів. Як пізніше було переконливо доведено, за операцією стояло «Агентство інтернет досліджень» Пригожина. Ця акція допомогла Агентству ліпше зрозуміти, як ведуть себе американські споживачі інформації, як можна викликати паніку, чи доречно використовувати підробки та багато іншого.

Facebook визнав факт використання платформи для впливу на вибори, випустивши 27 квітня 2017 року звіт «Операції впливу на Фейсбуці».[5] Звіт розрізняє поняття «фейкові новини», за якими може стояти і фінансова мотивація, та політично мотивовані «операції впливу», які здійснюються шляхом координованої групової активності, спрямованої на просування та підсилення певної історії або меседжу. Звіт також наголошує, що більша частина такої активності не була автоматизованою, а виконувалась людьми, які використовували неавтентичні акаунти. Високий рівень мовних навичок та глибоке розуміння політичної ситуації в цільовій країні вказували на високий рівень координації та попередньої підготовки учасників цих операцій.

«Якщо коротко, нам довелося розширити коло наших завдань в галузі безпеки додавши до традиційних злочинних

5. https://about.fb.com/wp-content/uploads/2017/04/facebook-and-information-operations-v1.pdf

дій, таких, як злом облікових записів, зловмисне програмне забезпечення, спам та фінансове шахрайство, більш витончені та підступні форми зловживання, включаючи спроби маніпулювати громадянським дискурсом та обманювати людей», - йдеться у звіті. Автори визнають, що проблема є складною, і, що реакція FB на такі дії буде постійно еволюціонувати.

5.2. Соціальні мережі та радикалізація

Хоча соціальні мережі відносять до медіа, а в США вони потрапляють під дію статі 230 Акту щодо пристойності комунікацій, яка звільняє нейтральних посередників від відповідальності за контент, створений третіми сторонами, вони не є ані традиційними ЗМІ, ані нейтральними платформами для розміщення контенту. З одного боку, у них дійсно нема редакційної політики та премодерації: користувачі розміщують контент без попереднього контролю з боку мережі. З іншого – вони базовані на алгоритмах, які визначають, з чого складається стрічка користувача.

Бізнес модель мережі Facebook побудовано на монетизації уваги та даних про її користувачів. Компанія відстежує та систематизує діяльність користувачів на платформі та за її межами, а також обробляє їх особисті дані. Доступ до цієї інформації продається рекламодавцям з метою кращого таргетування повідомлень. Вона також використовується для формування індивідуалізованої стрічки користувача за допомогою алгоритму.

Алгоритми соціальних мереж є комерційною таємницею. Їх спрямовано на те, щоб збільшувати залученість користувачів, демонструючи їм повідомлення, які утримуватимуть їх увагу та змусять залишатися на платформі якомога довше. Зазвичай, користувачам демонструють те, що їм подобається або цікавить, виходячи з інформації про попередню діяльність на платформі та про веб сайти, які користувач відвідує.

Алгоритм Фейсбуку сприяє тому, що користувач бачить переважно дописи своїх однодумців та не бачить альтернативної точки зору. Такий спосіб споживання інформації призводить до підтвердження попередніх переконань. Користувачі також можуть створювати групи однодумців. Ненавмисним наслідком такого підходу стало розділення суспільства на віртуальні групи, які майже не перетинаються та поступово поляризуються. Цей феномен компанія дослідила ще в 2016 році, але було прий-

нято рішення не вживати жодних заходів, адже це могло вплинути на залученість користувачів.[6]

Штучне сприяння цим процесам відбувається завдяки мережам ботів – автоматизованих програм, які створюють групи фейкових акаунтів. За словами дослідниці соціальних мереж з Університету Карнегі Мелон Кетлін Карлі: «Боти не лише маніпулятивно втручаються в розмови між користувачами, вони створюють групи та об'єднують їх».

Можливою також стає і радикалізація користувачів шляхом розміщення відповідного контенту в групах, або через прямий контакт з конкретними користувачами. Найбільше звинувачень у радикалізації звучало на адресу платформи YouTube, алгоритм рекомендацій якої пропонував користувачам відео з все більш радикальними поглядами дозволити платформі автоматично програвати наступні відео.[7]

5.3. Реакція платформ на операції впливу після виборів 2016

Як вже було зазначено, вибори Президента США 2016 року стали поворотними у сприйнятті соціальних мереж. Після значної критики їх ролі у виборах, найбільші компанії почали поступово запроваджувати процедури, які обмежують або врегульовують поведінку користувачів на їх платформі. Зусилля соціальних мереж постійно еволюціонують[8] та переважно сконцентровані на англомовному сегменті їх користувачів. Такі обмеження також є предметом постійної критики. Їх критикують, як надто повільні, як надто повільні, як надмірні, як політично вмотивовані, як такі, що нав'язують світу американські норми і таке інше. Разом з тим, варто мати на увазі, що великі технологічні компанії сьогодні намагаються вирішити проблему, яку ніхто до них ніколи не вирішував, адже вони самі її створили, а їх досвід демонструє складність протидії новітнім загрозам.

Найпершим кроком найбільшої мережі Facebook стало запровадження програми співпраці зі сторонніми фактчекерами. Програма стартувала в США в грудні 2016 року, майже одразу після виборів, і поступово розширюється на інші країни. Завдання фактчекерів – перевіряти обрані за певною методологією

6. https://www.theverge.com/2020/5/26/21270659/facebook-division-news-feed-algorithms
7. https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html
8. https://about.fb.com/wp-content/uploads/2020/10/Steps-Weve-Taken-to-Help-Protect-Elections.pdf

повідомлення на FB на достовірність. У разі визнання їх недостовірними, такі повідомлення не прибираються з платформи, а маркуються позначкою, що вони містять недостовірну інформацію. Також, за допомогою алгоритму зменшується вірогідність їх появи у стрічці користувачів.

Скоординована неавтентична поведінка стала наступною практикою, який почав протидіяти FB. Компанія описує таку практику, як «координацію дій груп людей або сторінок з метою введення інших в оману стосовно того, ким вони є, та які цілі переслідують».[9] Інформація, яку вони розповсюджують може бути достовірною, а контент може відповідати стандартам Facebook, але мережа все одно буде прибрана, адже причиною такого рішення є не зміст повідомлень, а саме поведінка на платформі. Наприклад, неприпустимо, коли задіяні у такій діяльності акаунти намагаються ввести інших в оману стосовно свого громадянства. Першу таку мережу FB прибрав з платформи у вересні 2017. У подальшому така практика стала регулярною, а інформацію щодо застосування цієї політики на платформі FB публікують у вигляді звітів.[10]

Через широке використання таргетованої реклами протягом кампанії 2016 року багато зусиль FB було спрямовано на збільшення прозорості рекламної діяльності, а також, на заборону іноземцям розміщувати рекламу щодо соціальних та політичних питань всередині іншої країни. Було запроваджено підтвердження особистості та громадянства тих, хто розміщує рекламу, обмежені можливості створювати рекламні повідомлення для сторінок, які часто розміщують недостовірну інформацію, кожне рекламне повідомлення має містити інформацію стосовно того, хто його оплатив, було запроваджено бібліотеки реклами, в яких можна знайти інформацію про тих, хто розміщує рекламні повідомлення, їх витрати та всі оплачені ними рекламні повідомлення, навіть, якщо вони не були призначені для конкретного користувача і не з'являлися у нього в стрічці. Реклама, яка закликає не брати участі у виборах, або намагається переконати користувачів, що голосувати не має сенсу, була заборонена. Натомість, FB закликав своїх користувачів голосувати та надавав інформацію щодо того, де і, як це можна зробити.

FB також запровадив політику проти фейкових акаунтів.[11] Зважаючи на те, що не кожен фейковий акаунт є шкідли-

9. https://about.fb.com/news/2019/10/inauthentic-behavior-policy-update/
10. https://about.fb.com/news/tag/coordinated-inauthentic-behavior/
11. https://about.fb.com/news/2019/05/fake-accounts/

вим, компанія намагається їх розрізняти та запроваджувати обмеження лише проти тих, які можуть потенційно нести шкоду. Деякі акаунти вдається заблокувати ще до того, як вони будуть зареєстровані, шляхом блокування спроб масового створення з однієї IP адреси. Деякі прибирають вже після того, як їх було створено. Система виявлення таких акаунтів шукає підозрілі адреси електронної пошти, ознаки підозрілої діяльності, схожої на ту, яка вже раніше була виявлена, як ознака фейкових акаунтів. Деякі акаунти таки потрапляють на платформу через те, що не проявляють ознак підозрілої діяльності з самого початку. Їх може бути розпізнано та видалено через певний час завдяки системі виявлення або за скаргами користувачів.

Заходи для підвищення прозорості було застосовано і до сторінок, які на відміну від особистого акаунту, можуть мати сотні тисяч підписників. Тепер підписникам відомо, хто є власником сторінки та, з якої країни вони походять.

Велику роль у розробці та запровадженні таких політик відігравала співпраця із зовнішніми дослідниками, з якими компанія почала ділитися даними щодо того, що відбувається на платформі. FB також започаткував ресурс, який допомагає користувачам навчитися відрізняти недостовірну інформацію від достовірної, а також, програми підтримки та допомоги традиційних ЗМІ.

Функціонал Твіттера не настільки широкий, як FB. У ньому не можна створювати групи та події, а повідомлення мають вкладатися у незначну кількість знаків – 280 від 7 листопада 2017 року і 140 до того. Разом з тим, Twitter є дуже популярним серед американських журналістів та політиків, як джерело інформації про події.

У відповідь на російське втручання у вибори Twitter пішов дещо іншим шляхом, ніж FB. «Відкрита природа Твітера та можливість розміщення інформації у реальному часі є потужною протиотрутою для поширення всіх типів неправдивої інформації», - зазначили в компанії.[12] Twitter не може визначати, чи кожен твіт є правдивим, а також, не має слугувати арбітром правди. Той факт, що журналісти, експерти, політики розміщують твіти поруч один з одним допомагає балансувати публічний дискурс. Зусилля компанії, передусім, було спрямовано на боротьбу із маніпуляціями та розповсюдженням спаму із застосуванням ботів. Також було вжито заходів щодо збільшення

12. https://blog.twitter.com/official/en_us/topics/company/2017/Our-Approach-Bots-Misinformation.html

прозорості реклами, запобігання маніпуляцій трендами Твітера, розпочато співпрацю із зовнішніми дослідниками, а також надана підтримка програмам з медіаграмотності.[13]

Використання YouTube під час виборів 2016 року було обмеженим.[14] Згідно компанії GOOGLE, було ідентифіковано 2 канали, які пов'язані з Агентством досліджень інтернету, які витратили 4 700 доларів на рекламу. Також, було ідентифіковано 1,108 відео, пов'язаних з цією компанією, які розповсюджувалися через 18 каналів, як політичного, так і неполітичного змісту. Ці канали було прибрано з платформи.

5.4. Модерація контенту

Модерація контенту стала значним викликом, пов'язаним насамперед з великою кількістю повідомлень, які користувачі розміщують на платформі. Ще один виклик стосується того, що модерація пов'язана з обмеженням персональної свободи висловлювання, захищеної міжнародним правом прав людини та Конституцією США. Значний виклик становить з встановлення правил, згідно яких той або інший контент має лишатися або бути прибраним з платформи. Рішення стосовно правил, зазвичай, приймають власники та менеджмент компаній. Остаточна відповідь, чи ці правила мають бути встановлені урядами та бути однаковими для всіх компаній, чи кожна компанія має встановлювати свої, залишається відкритою.

Модерація також вимагає значних затрат, чого собі часто не можуть дозволити маленькі фірми, і це ставить їх у невигідне становище у порівнянні з великими компаніями. Проблема розміру стає актуальною і для невеликих країн, які не можуть самостійно вплинути на рішення великих технологічних компаній, які не хочуть нести додаткові витрати розповсюджуючи та адаптуючи свої заходи безпеки та правила поведінки до невеликих ринків.

Недостовірна інформація, або так звані «фейк ньюз» стали першим симптомом проблеми «інформаційного безладу». При більш глибокому вивченні проблеми стало очевидно, що недостовірна інформація лише один з елементів операцій впли-

13. Update: Russian interference in the 2016 US presidential election, Thursday, 28 September 2017, https://blog.twitter.com/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html
14. https://www.zdnet.com/article/google-russian-groups-did-use-our-ads-and-youtube-to-influence-2016-elections/

ву. Як розповідає колишній Голова відділу безпеки компанії Facebook Алекс Стамос, серед повідомлень, які поширювалися на платформі неаутентичним чином були радикальні політичні погляди, базовані на правдивій інформації, або твердження, які не можна спростувати.[15] Можна говорити, що такий контент є «легальним, але шкідливим». Таке поняття запропонував запровадити уряд Британії, але чіткого визначення такого контенту він не дав. До цієї категорії можна віднести і теорії змови.

Велика кількість повідомлень змушує компанії вдаватися до автоматизації модерації шляхом залучення штучного інтелекту. Хоча такий підхід дозволяє обробляти велику кількість інформації, він має низку недоліків.

Центр аналітики та дії «Нова Америка» виділяє такі:

Точність та надійність – точність інструментів, базованих на штучному інтелекті, залежить від даних, на який його тренували. Якщо це стосується контенту, щодо якого існує достатньо даних, і який легко розділити на чіткі категорії, як такий контент, що порушує авторське право, такі інструменти є надійними. У випадках екстремістського контенту, мови ненависті і таке інше, де важливими є нюанси та контекст, значно зростає вірогідність невірної ідентифікації. Також, нема чіткого розуміння, що саме відносити до такої категорії.

Розуміння мови у контексті – те, наскільки образливим є висловлювання часто залежить від контексту, наприклад, хто саме це говорить, чи є висловлювання іронічним. Штучний інтелект не здатен відчувати цей контекст. Також, задані йому критерії доволі швидко застарівають, адже мова та її норми доволі швидко змінюються. Їх необхідно постійно оновлювати. Також, для уникнення ідентифікації та видалення, групи осіб починають адаптувати свій сленг та використовувати слова-замінники.

Упередження створювача та наборів даних. Натреновані на певних наборах даних алгоритми несуть у собі ризик подальшої дискримінації маргіналізованих груп, адже вони відтворюють закладені під час тренування упередження. Так само, особисті та культурні упередження створювачів алгоритму можуть відобразитися на результатах тренування моделі. Вибір, як кодувати те або інше висловлювання під час навчання у подальшому відображатиметься на рішеннях, які приймають алгоритми.

15. https://www.youtube.com/watch?v=ATmQj787Jcc&list=RDCMUCJhehVBcZFRMfNPHVV_-2TA&start_radio=1&rv=ATmQj787Jcc&t=6

Прозорість та підзвітність. Алгоритми часто називають «чорними ящиками», оскільки мало розуміння того, як відбувається кодування даних, на яких наборах даних вони навчаються, як вони визначають кореляції та приймають рішення, наскільки вони надійні та точні. Компанії відмовляються ділитися цією інформацією, адже вважають її комерційною таємницею. Разом з тим, поступово в практику входить публікація звітів щодо кількості перевіреного та прибраного з платформ контенту.[16] Платформи заявляють про дотримання Санта Кларських принципів,[17] прозорості та підзвітності модерації контенту.

FB також залучає до модераторської роботи людей, які розглядають скарги, які надійшли від користувачів або були відмічені алгоритмом. Таких скарг надходить у середньому 3 мільйони на день. За кількості модераторів у 30 тисяч це означає, що кожен з них має приблизно 150 секунд на прийняття рішення щодо відповідності відміченого повідомлення політиці компанії.[18] До того ж, правила платформи часто змінюються. Така практика призводить до великої кількості помилок, в результаті яких користувачів позбавляють можливості користуватися своїм акаунтом. Можливість оскаржити рішення компанії є обмеженою, адже ці рішення приймають ті самі модератори. Так само, платформи часто критикують за те, що вони обмежують свободу слова без звернення до суду, чого вимагає концепція належного процесу.

Разом з тим, активна модерація контенту та прибирання нелегальних матеріалів та повідомлень, поширених на платформах, може ускладнити притягнення до відповідальності тих, хто їх розмістив.[19]

Вперше ідея «Верховного суду FB», як незалежного органу, який буде приймати остаточне рішення щодо контенту на платформі була озвучена Марком Цукербегром на початку квітня 2018 року. 6 травня 2020 року було номіновано перших 20 членів Наглядової ради, а 22 жовтня 2020 року Facebook оголосив про початок її роботи.

16. https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/the-limitations-of-automated-tools-in-content-moderation/
17. https://santaclaraprinciples.org/
18. https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_content_moderation_report_final_version
19. https://www.niemanlab.org/2021/01/after-the-capitol-riots-platforms-archivists-conspiracists-and-investigators-collide

Наглядова рада[20] складається з щонайменше 11 осіб (максимальний склад – 40 осіб), які представляють різні країни та різні культури. Член Ради обирається строком на 3 роки і може служити не більше 3 термінів. Рада має право сама обирати, які скарги розглядати, і перевага надається тим кейсам, які мають найбільше значення для подальшої політики компанії. Рішення Ради є обов'язковими для виконання. Фінансування Наглядової ради здійснюється з трастового фонду, заснованого Фейсбуком, який управляється незалежною радою піклувальників.

28 січня 2021 року Наглядова рада прийняла свої перші тестові рішення щодо 5 постів, які було прибрано з платформи. З одним рішенням вона погодилася, а чотири інші рішення FB щодо видалення контенту були визнані неправильними, і FB підтвердив, що відновив пости.[21] Критики стверджують, що робота Наглядової ради все одно лишається беззубою, адже вона розглядає лише скарги на контент, який було прибрано з платформи, і не чіпає те, що залишається. Також, від жовтня 2020, коли було розпочато прийом скарг, до кінця січня 2021 на адресу Наглядової ради найшло понад 150 тисяч заявок.

5.5. Ефективність застосовування політики платформ

Здатність застосовувати задекларовану політику навіть для великих платформ, таких, як FB, який може дозволити собі інвестувати значні ресурси, як в автоматичну, так і в ручну модерацію, викликає значну критику та сумніви. Дослідження, повторно проведене NATO Strategic Communications Center of Excellence[22] вказує на те, що, незважаючи на політику боротьби зі скоординованою неаутентичною поведінкою на платформах можна доволі легко та недорого скористатися послугами, так званих Ботоферм. Також, фейкові акаунти, або акаунти, використовувані у координованій діяльності, залишаються на платформах протягом довгого часу після того, як на них поскаржилися.

І хоча ситуація у великих соціальних мережах таких, як Facebook та Twitter трошки виправилася, у порівнянні з дослідженням, проведеним за рік до того, різниця в ефективності є навіть між сервісами, які належать одній компанії, а саме між

20. https://oversightboard.com/
21. https://www.politico.eu/article/facebooks-supreme-court-overturns-content-decisions-oversight-board/
22. https://www.stratcomcoe.org/social-media-manipulation-report-2020

Facebook та Instagram. Facebook набагато більш оперативно прибирає Ботоферми та фейкові акаунти. YouTube залишився найменш ефективним у прибиранні мереж та фейкових акаунтів. Китайська мережа TikTok, якої не було у попередньому дослідженні, виявилася найбільш вразливою до маніпуляцій: вона не вжила жодних дій для убезпечення своїх користувачів.

Зменшенню ефективності заходів соціальних мереж сприяє також адаптація інформаційних ресурсів, які просувають свій контент через соціальні мережі. Прикладом такої адаптації може слугувати російський ресурс НьюзФронт. Для обходу обмежень, встановлених FB, його власники використовують дзеркала, які система FB не ідентифікує та продовжують розповсюджувати свої матеріали.[23] Нещодавні дослідження у галузі кібербезпеки продемонстрували, що застосування технології блокчейн до Ботоферм призводить до того, що їх стає набагато важче прибирати.[24] А це означає, що у разі більш широкого розповсюдження такої практики платформи стикнуться з новими викликами у запровадженні власної політики.

Дослідники також наголошують, що ніхто не може перевірити заяви FB щодо того, що вони прибрали певну кількість акаунтів, пов'язаних з тою чи іншою групою, адже діяльність самої компанії у себе на платформі залишається без жодного нагляду та контролю з боку політичних або громадянських механізмів.

23. https://securingdemocracy.gmfus.org/russias-affront-on-the-news-how-newsfronts-persistence-past-social-media-bans-demonstrates-the-need-for-vigilance
24. https://www.zdnet.com/article/this-botnet-is-abusing-bitcoin-blockchains-to-stay-in-the-shadows/

ПАНДЕМІЯ COVID19, ТЕОРІЇ ЗМОВИ ТА ОПЕРАЦІЇ ВПЛИВУ:

ПЕРЕД ОБЛИЧЧЯМ НОВИХ ВИКЛИКІВ

РОЗДІЛ 6

6. ПАНДЕМІЯ COVID19, ТЕОРІЇ ЗМОВИ ТА ОПЕРАЦІЇ ВПЛИВУ: ПЕРЕД ОБЛИЧЧЯМ НОВИХ ВИКЛИКІВ

Як вже неодноразово підкреслювалось у цій доповіді – операції впливу (не важливо ким вони проводяться) завжди спираються на актуальний контекст чи використовують наявні дискусійні теми в суспільстві. Особливу зацікавленість для авторів операцій є теми, які тісно пов'язані із чутками, браком інформації чи здогадками.

Це характерно для цілої низки класичних питань, які характерні майже для будь-якого суспільства:

- діяльність влади (постійне відчуття, що влада щось приховує чи не належить повною мірою широкій громадськості);
- раптові кризові ситуації або події;
- будь-які теми, які пов'язані із нестачею у пересічного громадянина спеціальних знань (медицина, військова справа тощо).

Будь-яка з цих тем дозволяє вкидувати дезінформаційні повідомлення з метою скеровування уваги отримувачів інформації у потрібне русло. Цифрові медіа лише посилюють ці можливості суб'єктів впливу, дозволяючи більш точно таргетувати повідомлення, користуючись цілком законними (комерційно доступними) можливостями платформ.

Сьогодні ми спостерігаємо щонайменше декілька масштабних дезінформаційних кампаній (різного масштабу, впливу та складності), які дають уявлення про те, які операції впливу розгортаються, як вони пов'язані із поточним контекстом.

Безумовно, найліпшим прикладом є інформаційна активність навколо COVID-19, адже має вона відповідати всім вище згаданим рисам: стосується спеціальної сфери (медицини), діяльності влади та є раптово-травмуючою для звичного укладу життя. Одночасно з цим пандемія також викликала змагання між країнами, що відбуваються на одночасно декількох просторах. Безумовно, ключовим з них залишається змагання щодо розробки та розповсюдження вакцини від коронавірусу, що також є специфічним інструментом поширення свого впливу, особливо на тлі дефіциту вакцин. Однак, так само це змагання ефективності різних систем охорони здоров'я, державного управління, економічного та соціального захисту населення в умовах кризи. А також виклик демократичним прав громадян, які зазнають обмежень внаслідок карантинів. Це само по

собі є достатнім предметом для деструктивних інформаційних впливів. Ситуацію не спрощує і очевидний факт – локдауни, суттєво збільшили обсяг онлайн взаємодії, що своєю чергою спричинило зростання можливостей впливу через кіберпростір.

Об'єктивний брак інформації про природу вірусу, неготовність урядів швидко та зрозуміло пояснити громадськості ситуацію (яку уряди і самі не розуміють), часто хаотичні перші дії із протидії (наприклад, повні локдауни змінювались послабленнями та дискусіями щодо їх доцільності і завершувались знову локдаунами із часто незрозумілими обґрунтуваннями їх ефективності), зрозуміла активізація на цьому фармацевтичної сфери – все це створювало можливість для інформаційних вкидів найрізноманітнішої природи. Пандемія перетворилася на інфодемію.

Китай та РФ – одні з ключових країн, які спробували скористатись ситуацією, тісно пов'язавши свої операції впливу не лише щодо дискредитації зусиль Західних урядів із протидії пандемії, але і одночасно просуваючи своє рішення проблеми. На думку деяких експертів, для цих двох країн історія із пандемією та реакцією на неї це можливість не так просунути свій продукт у вигляді вакцини, скільки показати громадськості в демократичних країнах, що авторитарні уряди ефективніші ніж їх демократичні – пропонують швидкі рішення, можуть так само запропонувати ефективну вакцину, допомагати всім бажаючим і таке інше. І для реалізації цього завдання авторитарні країни (і, передусім, маємо казати про Росію) залучили всі наявні сили. Так, зусиллями Російської Федерації з просування вакцини власної розробки Супутник V задіяна вся російська пропагандистська машина включно зі ЗМІ, інтернет-Ботофермами, так і специфічні інструменти, підконтрольні або ті, що симпатизують Росії – іноземні політики.

Європа досить швидко усвідомила проблему і той факт, що мова йде не лише і не стільки про питання здоров'я, але і про цінності, про моделі устрою і про конкуренцію політичних систем. «Китай поширює в Європі меседжі, що авторитарний стиль правління міг би стримувати пандемію ефективніше, ніж демократія»[1], – заявила Віра Юрова (*Věra Jourová*), Віцепрезидентка Єврокомісії з питань цінностей та прозорості на Глобальному медіа-форумі, організованому *Deutsche Welle*.

Державні суб'єкти, такі, як Китай та Росія, максимізують вплив т. зв. «вакцинової дипломатії» у своїх комунікативних зу-

1. https://www.dw.com/de/von-der-mammutaufgabe-desinformation-zu-stoppen/a-54846398

силлях, швидше за все, з метою підвищення своєї репутації та економічної ролі за кордоном. Вони використовують дипломатичні канали, контрольовані державою ЗМІ, мережі підтримуючих та альтернативних ЗМІ, а також соціальні мережі для поширення своїх повідомлень, – йдеться у звіті EUvsDisinfo[2].

Деструктивні інформаційні впливи спрямовані на[3]:

- поширення дезінформації про пандемію коронавірусу, з метою підірвати довіру до наукових порад і викликати розгубленість;
- розділення суспільств та налаштування людей один проти одного, використовуючи расу та клас, як інструменти поляризації та звинувачуючи в поширенні вірусу конкретні етнічні чи соціальні групи;
- створення почуття страху та безвиході, через фокусування на негативних повідомленнях про пандемію та формулювання її таким чином, щоб громадяни сумнівалися, що зможуть захистити себе в рамках європейських демократичних систем;
- атаки на інформаційні системи ЄС та СОТ національних урядів та навіть шкіл й медичних установ. Метою таких нападів є підрив довіри до цих інститутів та формування невдоволення їх діяльністю.

Наслідком поширення Кремлем теорій змови про те, що вірус було створено, як різновид біологічної зброї, стало створення у березні 2020 року спеціальної структури в Уряді Великої Британії, яка має на меті викривати і протидіяти дезінформації щодо розповсюдження коронавірусу[4].

Росія активно використовує антисистемні рухи, які підривають довіру до держави. Наприклад, в Чехії ми дослідили такі групи, які ще влітку казали: «Однозначно, щеплення – ні! Це дуже погана річ! Вам будуть імплантнтувати чіпи під шкіру, вас будуть відслідковувати!...» Зараз ті самі групи і ті самі люди стали великими прихильниками російської вакцини.

Давід Стулік

Казати про неефективність цих зусиль складно, адже зміна дискурсу цілком помітна. Хоча на перших етапах європейські країни не розглядали можливостей застосування російської вакцини, однак завдяки вказаній масштабній операції впливу з боку Москви ситуація

2. https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-may-november/
3. https://carnegieeurope.eu/2020/06/23/democracy-and-coronavirus-infodemic-pub-82115
4. https://www.radiosvoboda.org/a/30485922.html

змінюється. Реальними та потенційними реципієнтами російської вакцини, окрім країн, які традиційно є клієнтами РФ стали такі європейські країни, як Словаччина, Чехія, Угорщина, Італія, Німеччина, тобто країни де традиційно потужним є проросійське лобі.

Україна, як частина Європи є так само об'єктом всіх цих дезінформаційних кампаній (або операцій впливу) з боку Росії. Цей зв'язок виразно підкреслює той факт, що одним з адвокатів російської вакцини в Україні виступив відомий своїми проросійськими поглядами політик В. Медведчук, щодо якого Урядом України були запроваджені спеціальні обмежувальні заходи[5]. Спроби нав'язати Україні вакцину Супутник V підтримувались, окрім проросійських політиків, ще й сталою мережею впливу, яка включає пул журналістів, підконтрольних ЗМІ та інтернет-ресурсів. А сама кампанія по просуванню вакцини мала і має вигляд спланованої спеціальної інформаційної операції.

Безумовно, пандемія додатково показала вразливості цифрового взаємопов'язаного світу. Введені на початку кризи обмежувальні заходи прискорили цифровізацію значної частини населення Європи, змушеного реорганізувати свою роботу, освіту та дозвілля онлайн. У міру того, як цифровізація Європи прискорилася, інформаційна асиметрія, за якої протягом тривалого часу великі технологічні корпорації все більше і більше знали про нас, а ми – мало що про них, зросла. І це не єдиний дисбаланс, який посилився. Наприклад, електоральні процеси через обмеження, зумовлені коронавірусом, багато в чому перенесені в онлайн. Коли в січні 2021 року німецька партія ХДС обирала нове керівництво через Інтернет, хакери зробили спробу низки масових кібератак, щоб зірвати Інтернет-конференцію партії. Зловмисники, переважно з-за кордону, неодноразово атакували веб-сайт партії і в якійсь момент сервер не витримав. Прямий ефір події зупинився[6].

Короновірусна інфодемія стала особливим викликом для платформ, які лише за декілька років до того розпочали впроваджувати практики протидії дезінформації. **В 2020 році платформи постали перед подвійним викликом – пандемією COVID та виборів Президента США,** кульмінацією яких стала атака на Капітолій 6 січня 2021 року. Також, дослідники відмічають, що загроза недостовірної інформації переважно перетво-

5. https://www.president.gov.ua/documents/642021-36753
6. https://www.dw.com/de/cyber-bedrohungen-%C3%BCberschatten-bundestagswahlkampf/a-56772592

рилась із зовнішньої на внутрішню проблему, адже на відміну від виборів 2016 року, коли втручання здійснювалося з-за кордону за допомогою російських Ботоферм, переважна більшість осіб, які розповсюджували недостовірну інформацію та поляризуючі повідомлення, були громадянами США.[7]

Карантин підштовхнув FB та інші платформи до більш широкого застосування штучного інтелекту для визначення неналежного контенту. В результаті, значно зросла кількість акаунтів, яким було тимчасово обмежено можливості користуватися платформами, а також, значно зросла кількість контенту, прибраного з платформ, як проблематичного. Так само зросла і кількість проблематичного контенту, який лишився на платформах.[8] Така практика призвела до постійних звинувачень в цензурі, і деякі користувачі почали переходити до платформ, де майже відсутня модерація.

Ще одним складним викликом стала комунікація колишнього Президента Дональда Трампа. Повідомлення, що не відповідали дійсності, заяви, що результати виборів буде сфальсифіковано задовго до того, як вибори навіть відбулись, нападки на традиційні медіа та соціальні мережі, нападки на опонентів, заяви, які поляризують та виправдовують або заохочують насильство – стали звичними елементами його комунікації, через які його опоненти закликали соціальні мережі обмежувати його свободу висловлювання.

Соціальні мережі дотримувалися точки зору, що свобода політичного висловлювання знаходиться під захистом першої поправки до американської Конституції, і не розповсюджували свою політику щодо недозволеного контенту на Трампа. Лише у розпалі передвиборчої кампанії вони почали маркувати його повідомлення, як такі, що є недостовірними, зменшувати їх видимість, або прибирати їх – Twitter у травні, а Facebook у серпні 2020 року.

У відповідь на поширення недостовірної інформації про COVID, соціальні мережі почали вживати все більш заходів. Такі заходи можна розділити на три широкі категорії[9] – обмеження розповсюдження або прибирання недостовірної інформації з платформ, допомога у поширенні контенту, якому можна довіряти, стимулюючі або обмежувальні фінансові заходи, такі, як заборона реклами або заборона розміщувати мобільні додат-

7. https://stacks.stanford.edu/file/druid:tr171zs0069/EIP-Final-Report.pdf
8. https://www.politico.eu/article/facebook-content-moderation-automation/
9. https://blog.witness.org/2020/05/covid-19-misinformation-response-assessment/#Part2

ки, які не відповідають критеріям якості, у Play Market або App Store, фінансова підтримка журналістики, спрямованої на боротьбу з недостовірною інформацією щодо COVID.

Відповідь платформ еволюціонувала у процесі розвитку кризи, і їх застосування було нерівномірним. Так, протягом довшого часу політики були звільнені від необхідності дотримуватися правил платформ щодо нерозповсюдження недостовірної інформації щодо вірусу. Facebook дозволяв політикам розміщувати рекламу, що містить дезінформацію. Twitter таку практику заборонив і зменшував видимість неправдивих повідомлень, поширюваних Президентом Трампом.

Загалом, всі найбільші мережі запровадили політики, які мали на меті убезпечити процес виборів Президента США. Порівняльний аналіз політик 15 різних платформ станом на 28 жовтня 2020 року зробили фахівці Elections Integrity Project, які вивчали вплив недостовірної інформації на вибори. Такий детальний аналіз не належить до завдань цього дослідження, але варто відмітити, що на різних платформах було запроваджено різні правила, які, до того ж, постійно змінювалися, щоб адаптуватися до нових викликів.[10] Дослідники поділили заходи соціальних мереж на три категорії: такі, що стосуються процедур; такі, що стосуються участі у виборах та такі, що стосуються фальсифікації.

Як вже вказувалось вище, невизначеність стає живильним підґрунтям для різноманітних домислів та теорій змов (конспірології). Останні завжди посилюють свій вплив у часи змін та криз. Хоча є свідчення, що їх поширення та розвиток може бути підживлюваний свідомо авторитарними урядами і для внутрішньополітичних цілей[11].

2020 рік став особливими, створивши численні нові теорії або скорегувавши старі. Дослідники спостерігали за тим, як противники вакцинації, ті, хто не вірять в реальність COVID та ті, хто вірять в теорію змови QAnon поступово формували все більші спільноти, потім ці спільноти змішувалися, а потім теорії змови перетікали у нові спільноти.[12] Так, наприклад, в 2020 році таке зараження сягнуло спільноти тих, хто займається йогою, веде здоровий образ життя та споживає органічну їжу.[13]

10. https://www.eipartnership.net/policy-analysis/platform-policies
11. НАЙТИ ГУСАРОВА
12. https://www.wsj.com/articles/social-media-in-2020-a-year-of-misinformation-and-disinformation-11607712530
13. https://www.wired.co.uk/article/yoga-disinformation-qanon-conspiracy-wellness

Історія теорії **QAnon,** яка набула світового поширення, почалась 27 жовтня 2017 року, коли анонімний користувач під ніком Q почав розміщувати таємничі дописи на сайті без правил 4chan. Просування цієї теорії було побудовано за логікою гри, коли людина або колектив авторів викладають якісь незрозумілі повідомлення і прихильники намагаються зрозуміти, що вони означають.[14] Згідно дослідження Департаменту внутрішньої безпеки США, теорія QAnon поєднує противників вакцинації, прихильників боротьби проти 5G, антисемітські та антимігрантські мотиви та кілька химерних теорій, що світ опинився в полоні групи педофільських еліт, що мріють про глобальне панування, та здійснюють ритуали, під час яких приносять у жертву дітей. 1 серпня 2019 ФБР визначило QAnon та інші теорії змови загрозою внутрішнього тероризму.

Facebook почав більш активно протидіяти розповсюдженню QAnon лише у серпні 2020 року. Тоді акцент було зроблено на групах, які пропагують насильство. А у жовтні компанія оголосила, що буде прибирати будь-які акаунти, які відкрито асоціюють себе з цією теорією змови. «З серпня по 30 листопада 2020 року ми вилучили близько 3200 сторінок, 18 800 груп, 100 подій, 23 300 профілів у Facebook та 7400 акаунтів в Instagram за порушення нашої політики проти мілітаризованих соціальних рухів. Одночасно ми також вилучили близько 3000 Сторінок, 9800 груп, 420 подій, 16200 профілів у Facebook та 25000 акаунтів в Instagram за порушення нашої політики щодо QAnon».[15] Але на той момент вже відбулось настільки глибоке злиття прихильників цієї теорії та прихильників Республіканської партії, що таке втручання сприймалося, як обмеження консервативної точки зору.

Намагання FB боротися з теоріями змови, між іншим, призвело до того, що заявилася тенденція до **мікровпливу.** FB дозволила групам конспірологів залишатися на платформі достатньо довго для того, щоб їх активні члени завели собі сторінки та почали розміщувати на них тематичні матеріали.[16] У порівнянні із закриттям груп, закриття сторінки є більш контраверсійним, адже це вже проблема індивідуальної свободи висловлення. Разом з тим, сторінки мають широке коло підписників та можуть мати значний вплив на них шляхом постійного розміщення неправдивих або маніпулятивних повідомлень. Про

14. https://www.wired.com/story/qanon-most-dangerous-multiplatform-game
15. https://about.fb.com/news/2020/08/addressing-movements-and-organizations-tied-to-violence/
16. https://www.wired.co.uk/article/facebook-antivaxx-qanon-microinfluencers

значну роль інфлюесерів, або «постійних розповсюджувачів» (repeat spreaders) у подіях навколо виборів 2020 року йдеться у звіті Elections Integrity Partnership.[17] Акаунт одного з таких розповюджувачів Майка Ліндела, який відмовлявся припиняти розповсюджувати заяви, що перемогу Трампа було вкрадено, Twitter прибрав з платформи наприкінці січня. Але на той момент це рішення вже не сприймалося, як надто конраверсійне.

В Німеччині намагання Facebook обмежувати розповсюдження недостовірної інформації щодо COVID-19 привело до того, що прихильники місцевого руху Querdenken перейшли в Телеграм. Там офіційний канал набрав 70 000 підписників, і від нього також відгалузилися понад 1200 місцевих груп. Деякі регіональні лідери руху мали 120-150 тисяч підписників.[18] Підхід Твіттера принаймні на початкових етапах полягав у тому, щоб зменшити видимість акаунтів, які поширювали теорії змови.

Атака прихильників Президента Трампа на Капітолій у Вашингтоні під час остаточної сертифікації результатів виборів 2020 року стала переламним моментом для соціальних мереж. Майже одразу після штурму Twitter оголосив про тимчасове призупинення акаунту Трампа. Ввечері його приклад наслідували Facebook та Instagram. 8 січня Twitter прийняв рішення про остаточне видалення Трампа з платформи. Після того, як Twitter прибрав акаунт Трампа, компанія також вирішила прибрати 70 тисяч акаунтів, пов'язаних з QAnon. Після заборони президента, Twitter розпочав боротьбу зі змовами, які «можуть призвести до офлайн-шкоди». Facebook також заявив, що видалить вміст, в якому згадується «#StopTheSteal». Серед причин таких дій були повідомлення, що радикальні групи, які пропагують громадянську війну в США, планують атаки на Капітолії в 17 штатах.[19]

На поведінку прихильників Трампа відреагували і інші компанії. Так, Амазон прибрав додаток Парлер. [20] Після виборів, уникаючи так званої цензури техгігантів в ньому зареєструвалася велика кількість прихильників Трампа, багато з яких стали учасниками нападу на Капітолій. Google та Apple прибрали застосунок зі своїх магазинів, а Амазон припинив надавати компанії послуги хостингу. Інші провайдери хостингових послуг наслідували його приклад. Одночасно, метадані відео, завантаже-

17. https://purl.stanford.edu/tr171zs0069
18. https://www.opendemocracy.net/en/germany-ground-zero-covid-infodemic-russia-far-right/
19. https://www.pbs.org/newshour/nation/fbi-warns-of-plans-for-nationwide-armed-protests-next-week
20. https://www.axios.com/trump-social-media-bans-twitter-facebook-parler-d8e985e0-0c59-4386-95c7-a2aa3ff0096e.html

них на Парлер зсередини Капітолію, були отримані хакером через вразливість в її програмному забезпеченні та передані правоохоронним органам, які розслідували напад на Капітолій.[21]

У продовження політики боротьби з теоріями змови 16 березня Твіттер оголосив, що більш ніж подвоїв кількість акаунтів, прибраних з платформи, за розповсюдження шкідливого контенту. На сьогодні таких акаунтів понад 150 тисяч. Переважна більшість з них були «реальними людьми», звичайними американцями, а не іноземними громадянами, або ботами, хоча багато з них мали по декілька акаунтів. Намагання Твітера зменшити розповсюдження шкідливого контенту через більш м'які обмежувальні заходи, бажаного ефекту не дало.

Реакція європейських лідерів на рішення платформ прибрати акаунт Трампа була переважно негативною. Канцлерка Німеччини Ангела Меркель назвала це рішення проблематичним та наголосила, що будь-які обмеження свободи слова мають відбуватися в рамках законодавства, а не внутрішніх рішень корпорацій. Вона також закликала США наслідувати приклад Німеччини та прийняти закон, який омежуватиме онлайн підбурювання до насильницьких дій. Міністр фінансів Франції Бруно ле Мер заявив, що великі технологічні компанії є однією з загроз демократії, і наголосив, що регулювання належить до обов'язків держави, а не «цифрової олігархії».[22]

У зв'язку з заворушеннями на Капітолійському пагорбі, Єврокомісар з питань внутрішнього ринку Т'єррі Бретон закликав до трансатлантичного союзу для регулювання цифрової сфери. Крім питання цифрового податку, ЄС сподівається підняти питання приватності та спостереження, а також запропонувати загальні способи регулювання соціальних мереж.[23]

Польща запропонувала закон про свободу слова, який забороняє платформам прибирати контент або блокувати користувачів мережі, якщо вони не порушують польське законодавство. Законом пропонують створити «раду зі свободи медіа», яка зможе розглядати скарги на блокування користувачів та видалення контенту, а якщо соцмережі відмовляться відновлювати контент, вони можуть бути оштрафовані на суму між 50 000 та 50 мільйонів злотих.[24]

21. https://gizmodo.com/parler-users-breached-deep-inside-u-s-capitol-building-1846042905
22. https://www.bloomberg.com/news/articles/2021-01-11/merkel-sees-closing-trump-s-social-media-accounts-problematic
23. https://www.politico.eu/article/why-europe-china-investment-deal-will-poison-transatlantic-relations-joe-biden/?mc_cid=0d166ffde7&mc_eid=c551ca99a4
24. https://www.bbc.com/news/technology-55678502

Дослідники зазначають, що праворадикальна партія Alternative fuer Deutschland вже почала розповсюджувати рекламу расистського та нацистського змісту, а також наративи щодо фальсифікації виборів, подібні до тих, що в США розповсюджував Президент Трамп.[25]

25. https://www.dw.com/en/cyber-threat-looms-large-over-german-election/a-56775960