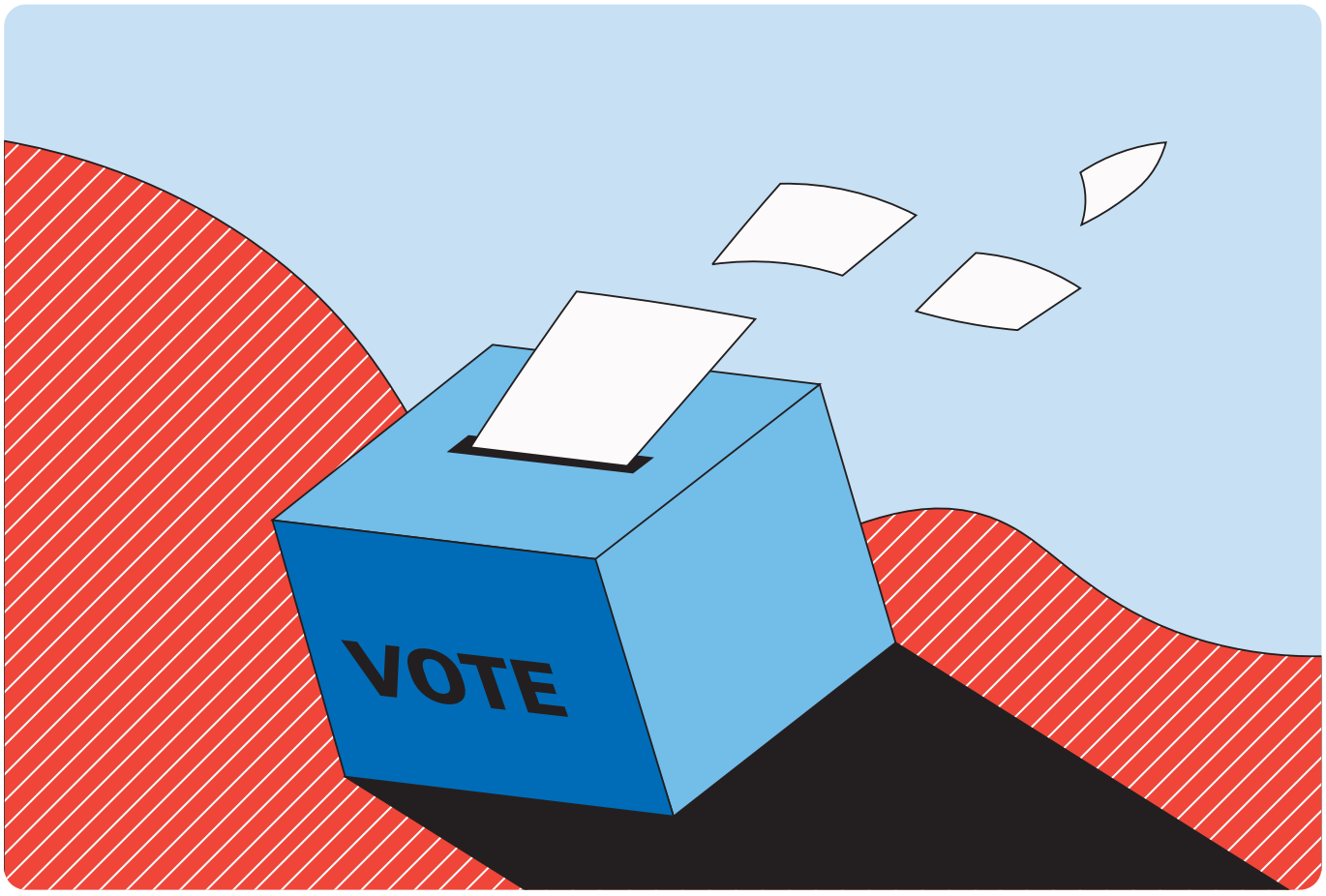
Захист виборів від гібридних загроз: **посібник з протидії**

Себастьян Бей і Каталіна Урібе Бурчер
Вересень 2025 р.



Folke Bernadotte Academy
Шведське агентство з питань миру, безпеки та розвитку

FBA

Подяки

Автори цього звіту хочуть висловити вдячність багатьом особам та командам, чиї внески зробили це можливим.

Передусім ми хочемо подякувати Лізі Орреніус, яка наглядала за процесом від початкової ідеї до його завершення, надавала безперервний зворотний зв'язок та поради. Ми також вдячні колегам з Академії Фольке Бернадота (FBA), які переглянули та прокоментували структуру, зміст і формулювання нашої роботи, в тому числі Карлу Фредріку Біркофу, Філіпі Альмлунд і Кікі Вестін з відділу «Демократія та управління», а також Еммі Хемстрьом і Абдальхаді Аліджі з відділу досліджень.

Ми також висловлюємо вдячність Сюсанні Куянпяа (колишній співробітниці Європейського центру передового досвіду з протидії гібридним загрозам — «Hybrid CoE») за її цінну зовнішню оцінку та аналітику.

Особисту вдячність висловлюємо Айні Борис, яка контролювала всі аспекти процесу публікації та стежила за тим, щоб робота з рукописом, макетом, ілюстраціями та остаточна публікація пройшли вдало. Ми також дякуємо Essen International та Comactiva Language Partner за їхню відмінну роботу з редагування, видавничої підготовки рукопису та роботу з ілюстраціями.

Зміст

Передмова

Вільні вибори є наріжним каменем демократичного урядування. Вони втілюють суспільний договір між громадянами та державою, пропонуючи як засоби управління, так і механізм підзвітності. Сьогодні цей договір все частіше піддається атакам. Гібридні загрози, які поєднують маніпуляції з інформацією, кібератаки та незаконне політичне фінансування, атакують не лише власне виборчі процеси, але й самі довіру та суспільний лад, на яких ґрунтується демократія.

Ці загрози не є ані епізодичними, ані другорядними. Вони представляють стійкий та надзвичайно адаптивний виклик демократичному урядуванню. Ці загрози та атаки не тільки ставлять собі за мету впливати на певне голосування, але й на підрив довіри до інституцій, посилення розколів та послаблення суспільства зсередини. Застосування штучного інтелекту та інших новітніх технологій ще більше прискорило цю тенденцію — воно знижує поріг втручання та збільшує його вплив.

Для Академії Фольке Бернадота (FBA) захист демократії є засадою запобігання конфліктам, а також питанням як національної, так і міжнародної безпеки. Він вимагає більшого, ніж технічні захисні заходи; він потребує політичного бачення, інституційної стійкості та колективної волі. Ефективні відповіді повинні зміцнювати здатність національних суб'єктів на всіх рівнях діяти разом, поділяючи розуміння того, що стійкість демократії залежить від залученості всіх частин суспільства. Водночас ці зусилля мають підтримувати відкритість, прозорість і права, які є визначними для демократичних систем. Протидія гібридним загрозам не може відбуватися за рахунок тих самих цінностей, які ми прагнемо захистити.

Цей звіт відображає відданість FBA підтримці зусиль щодо вільних і законних виборів. У ньому зібрані воєдино практичні знання щодо того, як гібридні загрози проявляються у інформаційних операціях, незаконному фінансуванні та кібератаках, а також як скоординовані, орієнтовані на управління стратегії можуть підтримати чесність виборів. Наведені рекомендації підкреслюють важливість загальноурядових та загальносуспільних підходів, інституціоналізації мереж співпраці та безперервного циклу готовності, який виходить за межі власне дня виборів.

Основоположне твердження звіту — те, що стійкість виборчого процесу невіддільна від стійкості демократії. Побудова захисту від гібридних загроз — це не лише практичний захід у сфері безпеки; це інвестиція у верховенство права, у підзвітне управління та довготривалу довіру до демократичних інституцій.

Приклади та уроки, представлені в цьому звіті, актуальні для всіх країн, разом із нашою власною країною — Швецією. Гібридні загрози не визнають кордонів та не зважають на відмінності між зрілими та молодими

демократіями. Тактики, які спрямовані на підрив чесності виборів у одному контексті, можуть швидко переноситися в інший. Тому побудова стійкості є спільною відповідальністю — як держав, так і інституцій та суспільств. Завдяки навчанню на різноманітному досвіді та сприянню транскордонній співпраці ми можемо зміцнити не лише захист виборів, а й підвалини самої демократії.

Пер Ольсон Фрід
Генеральний директор, Академія Фольке Бернадота

Глосарій термінів

- **Розвинені стійкі загрози («Advanced Persistent Threats», APT):** Цілеспрямовані загрози з великими ресурсами — часто спонсоровані державами або такі, що виконують доручення держав — які проводять тривалі, приховані вторгнення, щоб отримати та зберігати доступ до цільових мереж заради підтримки стратегічних цілей (шпигунства, попереднього розгортання, порушення діяльності або операцій впливу).

- **Координований маніпулятивний вплив («Coordinated Inauthentic Behaviour», CIB):** Координоване використання оманливих або несправжніх облікових записів для введення людей в оману щодо походження, сутності або популярності контенту.

- **Діпфейк («Deepfake»):** Синтетичні або маніпульовані медіа-матеріали (зображення, аудіо чи відео), створені за допомогою методів штучного інтелекту для зображення подій або висловлювань, яких фактично не відбувалося.

- **Дезінформація:** Інформація, яка є неправдивою або вводить в оману і навмисно створена та поширюється з метою завдати шкоди певній особі, соціальній групі, організації або країні.

- **Доксинг («Doxing», іноді пишеться «doxxing»):** Публікація або поширення в мережі Інтернет приватної, особистої або конфіденційної інформації про особу без її згоди, як правило, з метою переслідування, залякування або заподіяння шкоди іншим чином.

- **Техніка «двійника»:** Тактика, у якій використовуються подоби («двійники») інфраструктури — клоновані або якісно підроблені сайти новин та закладів, домени та акаунти соціальних мереж — для «відмивання» неправдивого або оманливого контенту, щоб він виглядав так, нібито походить із вартих довіри джерел. Потім цей контент поширюється та підсилюється через скоординовану маніпулятивну поведінку, платну рекламу та перехресне розміщення на інших платформах.

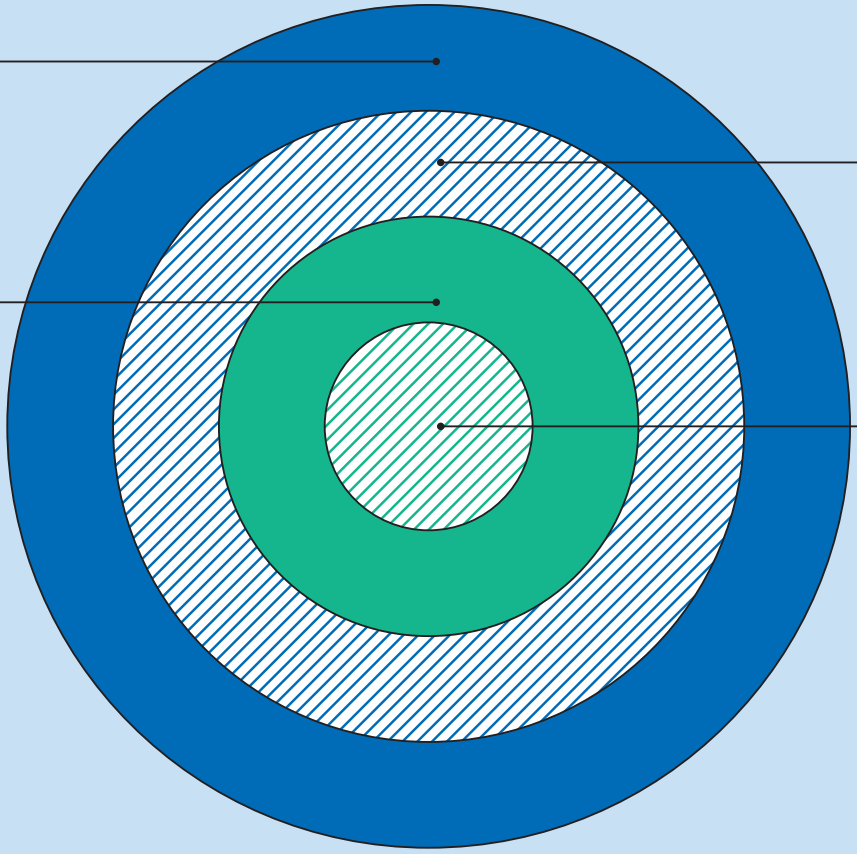
- **Маніпулювання інформацією та зовнішнє втручання («Foreign Information Manipulation and Interference», FIMI):** Здебільшого легальна схема маніпулятивної поведінки, яка проводиться навмисно та скоординовано іноземними державними або недержавними суб'єктами (включаючи їхніх проксі-представників), котра загрожує цінностям, процедурам та політичним процесам або потенційно здатна негативно вплинути на них.

- **Операція «злам та витік» («Hack-and-Leak»):** Координована операція, спрямована на компрометацію систем з метою викрадення даних і публікації окремих, відібраних або маніпулятивних матеріалів у стратегічні моменти для впливу на медійні наративи, суспільну думку або політичні процеси.

ІЄРАРХІЯ ТЕРМІНОЛОГІЇ

Гібридні загрози
Широкий контекст скоординованих, навмисних і шкідливих дій, які включають інформаційні, кібер- та фінансові засоби.

FIMI
Схема маніпулятивної поведінки, що здійснюється іноземними суб'єктами, навмисно та часто скоординовано.



Заходи з інформаційного впливу (ІІА)
Сплановані заходи з формування уявлень, ставлень або поведінки через інформацію та комунікації.

Дезінформація
Неправдива або оманлива інформація, яка поширюється навмисно з метою завдати шкоди.

- **Гібридні загрози:** Скоординовані, навмисні та шкідливі дії, які навмисно спрямовані на системні вразливості демократичних держав та інституцій і здійснюються за допомогою комбінації традиційних і нетрадиційних засобів. Ці дії користуються пороговими рівнями виявлення та встановлення джерела (атрибуції), а також «межею фаз» між війною та миром і внутрішньою та зовнішньою безпекою. Вони зазвичай мають за мету вплив на прийняття рішень на місцевому, державному або інституційному рівнях, залишаючись при цьому нижче порогу збройного конфлікту.

- **Заходи з інформаційного впливу («Information influence activities», IIA):** Сплановані зусилля з формування сприйняття, ставлення або поведінки за допомогою використання інформації та комунікацій. Такі заходи розташовані на проміжку від законних публічних комунікацій та дипломатії до таємних або оманливих практик, як-от видавання себе за когось іншого та скоординованої маніпулятивної поведінки. Заходи з інформаційного впливу (IIA) — це загальне поняття. Воно включає у себе маніпулювання та втручання FIMI, але останні стосуються конкретно маніпулятивної поведінки, що здійснюється іноземними державними або недержавними суб'єктами та проксі-представниками.

- **Випереджувальне розвінчування («Pre-bunking» — «пребанкінг»):** Проактивна комунікаційна стратегія, концептуально подібна до «щеплення», яка заздалегідь попереджає людей про ймовірні тактики маніпуляції або наративи, перш ніж вони з ними зіткнуться. Вона надає прості й точні засоби протидії та допомогу у прийнятті рішень, щоб допомогти людям розпізнавати та протистояти маніпуляціям, коли ті відбуваються. У контексті виборів випереджувальне розвінчування (пребанкінг) часто здійснюється через центр джерел достовірної інформації, через відповіді на часті питання та через публічне інформування, прив'язане у часі до відомих періодів ризику (наприклад, крайніх термінів реєстрації або «періодів тиші»).

- **Хибна інформація («Misinformation»):** Інформація, яка є неправдивою, але не створена або не поширюється з наміром завдати шкоди.

- **Адресний фішинг («Spear-phishing», цільовий фішинг):** Це цілеспрямована атака із застосуванням соціальної інженерії, яка використовує спеціально розроблені «принади», щоб ошукати певну конкретну особу і переконати її розкрити облікові дані, надати доступ або виконати зловмисний код.

- **Вішинг («Vishing», або голосовий фішинг):** Метод атаки за допомогою соціальної інженерії, що здійснюється через голосові дзвінки, часто з використанням підроблених номерів абонента, що викликає, щоб ошукати людей і переконати їх розкрити певну інформацію або надати доступ.

Акроніми

- **ШІ:** штучний інтелект («AI»)
- **РСЗ:** розвинена стійка загроза («Advanced Persistent Threat», «APT»)
- **CaaS:** «кіберзлочинність як послуга» («Cybercrime-as-a-Service»)
- **DDoS:** розподілена атака типу «відмова в обслуговуванні» («Distributed Denial-of-Service»)
- **DSA:** Акт Європейського Союзу про цифрові послуги (Digital «Services Act»); накладає зобов'язання щодо зниження ризиків, прозорості та доступу до даних на дуже великі Інтернет-платформи.
- **ОКВ:** орган, що керує виборами («Election Management Body», EMB)
- **FBA:** Академія Фольке Бернадота (Folke Bernadotte Academy)
- **FIMI:** маніпулювання інформацією та зовнішнє втручання («Foreign Information Manipulation and Interference»):

Зведена пояснювальна записка

Цей звіт містить всебічний аналіз гібридних загроз виборам і способів ефективної протидії цим загрозам. Він зосереджений у першу чергу на змінах, що відбулися з 2024 року в сферах втручання у вибори, в тому числі маніпулюванні інформацією та зовнішньому втручанні (FIMI), незаконному фінансуванні політичної діяльності та кібероперація̈х. Хоча аналіз цих явищ проведений окремо, на практиці вони тісно пов'язані між собою. Звіт просуває практичну методологію захисту, яка поєднує в собі розбудову інституційного потенціалу з мережевою, загальносуспільною системою підтримки.

Основні тенденції (з 2024 року):

- Маніпулювання інформацією та зовнішнє втручання FIMI перетворилося з відокремлених кампаній на безперервні операції, що здійснюються в промислових масштабах під керуванням скоординованих мереж.

- Штучний інтелект і автоматизація прискорили створення та поширення штучного (синтезованого) та оманливого контенту, а також знизили собівартість операцій соціальної інженерії.

- Незаконне фінансування політичної діяльності, включно з фінансуванням через проксі-посередників, міжнародними переказами у криптовалютах та непрозорими онлайн-витратами, все більше застосовується для підтримки маніпуляцій та підкупу виборців.

- Кібероперації порушують роботу виборчої інфраструктури і часто здійснюються на пару з інформаційними операціями, підсилюючи їхній загальний вплив.

Основний наслідок цих тенденцій полягає в тому, що зловмисники використовують «прогалини» між установами, відповідальними за організацію та підтримку виборів. Внаслідок цього ізольоване реагування таких установ виявляється недостатньо результативним. Цей звіт узагальнює найкращі практики щодо контрзаходів та підкреслює ідею того, що захист виборів від таких складних загроз вимагає:

- чіткого визначення відповідальності, ресурсів, повноважень, персоналу та відпрацьованих процедур у кожному урядовому органі.

- постійної, діючої безперервно мережі міждержавної співпраці, у рамках якої буде відбуватися обмін розвідувальною інформацією, проведення спільних навчань та координація заходів із захисту — яка діятиме за принципом «аналізуємо разом, діємо в межах власних повноважень» для збереження організаційної автономії.

- загальносуспільного підходу, який мобілізує незалежні ЗМІ, громадянське суспільство, академічні кола, місцеві органи влади, приватний сектор (включаючи цифрові платформи та телекомунікаційних операторів) і громади для збільшення стійкості через медійну та цифрову грамотність, швидку перевірку фактів

(«фактчекінг»), повідомлення про інциденти та інклюзивні публічні комунікації — заснованого на радикальній прозорості та впровадженого методами, які підтримують права, прозорість і плюралізм.

- надійних механізмів міжнародного співробітництва та підтримки, які надають допомогу в ситуаціях найбільшої потреби, дозволяють видаляти контент за кордоном, у країнах-партнерах, та узгоджують спільні основні плани (наприклад, практику безпеки за архітектурою та концепцією, зазначення походження, коли це можливо, та своєчасне розкриття інформації) — які поєднують національні мережі у ширшу «мережу мереж» для прискорення підтримки, сприянню узгодженості та підзвітності.

У звіті пропонуються практичні рекомендації для органів, що керують виборами, урядів, організацій громадянського суспільства та суб'єктів міжнародної підтримки, у різних виборчих середовищах — від усталених демократій до демократій, що розвиваються. Основні рекомендації включають зміцнення виборчих органів, досягнення операційної досконалості, створення добре забезпечених ресурсами мереж міжнаціональної співпраці у виборчих процесах, вдосконалення нормативно-правової бази щодо відповідальності соціальних платформ та незаконного політичного фінансування, а також прийняття модульного підходу до міжнародної підтримки.

Основний висновок полягає у тому, що в епоху триваючого гібридного конфлікту захист виборів має бути безперервним, адаптивним, проактивним і колективним. Розвиток потужного інституційного потенціалу та підхід із залученням усього суспільства забезпечать найтриваліший захист чесності виборів.

01 Вступ

Під час виборів у Європі гібридні загрози були серйозним випробуванням стійкості виборчих систем. У Словаччині, лише за два дні до виборів 2023 року, під час періоду «медійної тиші» відбулося розповсюдження створеного за допомогою ШІ аудіозапису, в якому нібито кандидат від лібералів Міхал Шімечка та журналіст змовлялися про купівлю голосів ромських громад. У Румунії напередодні президентських виборів 2024 року влада виявила застосування скоординованих гібридних тактик, що включали схеми підкупу виборців, дезінформацію та кібератаки, а також незадеклароване фінансування проросійського кандидата. А в Молдові у вересні 2025 року президент Майя Санду попередила, що Москва веде масштабну гібридну війну напередодні парламентських виборів, використовуючи дезінформацію, підкуп виборців та інші форми незаконного політичного фінансування, а також тактики залякування виборців. [1]

Разом ці приклади ілюструють, як вибори стикаються зі щоразу більшими викликами та втручанням з боку іноземних суб'єктів, котрі здійснюють скоординовану діяльність у сферах інформації, фінансів та кіберпростору, часто підбираючи момент часу так, щоб експлуатувати інституційні та суспільні розбіжності.[2] Оскільки ці загрози постійно розвиваються, захист вільних і чесних виборів від гібридних загроз став не лише більш критичним викликом, ніж будь-коли раніше, але й потребою, що існує безперервно і постійно видозмінюється.[3]

Сучасний ландшафт загроз являє собою результат глибокої еволюції у порівнянні з традиційними дипломатією та пропагандою 20 сторіччя. Тепер «центром тяжіння» є цифрова сфера: антагоністи комбінують кібероперації, методики підривної діяльності в Інтернеті та маніпуляції наративом, а внутрішні гравці можуть свідомо або несвідомо для себе посилювати ці зусилля. Дії Російської Федерації під час виборів в Україні у 2014 році, і зокрема під час президентських виборів у США у 2016 році, стали переломним моментом, який радикально прискорив глобальне визнання вразливості демократичних процесів до складних гібридних загроз такого роду.[4]

Важливим висновком стало те, що сучасні втручання не є ланцюжком окремих операцій; їх сутність — це тривала, підтримувана державами інформаційна війна, яка ведеться складною екосистемою суб'єктів.[5] Розвідувальні служби постійно визначають як основних організаторів Росію, Китай та Іран, які діють через мережу проксі-представників — від державних ЗМІ до груп хактивістів — щоб підтримувати «фасад» правдоподібної непричетності.[6] Ця межа ще більше розмивається внутрішніми (в країні) політичними групами, котрі можуть діяти як свідомі або несвідомі «підсилювачі» іноземних наративів.[7]

Технологічні досягнення, зокрема в галузі штучного інтелекту, значно прискорили цю еволюцію. З 2024 року використання генеративного ШІ стало значним мультиплікатором сил, який дозволяє швидко та з низькими витратами створювати реалістичні синтезовані медіа, включаючи діпфейки та клонування голосу реальних осіб; дає змогу виробляти дезінформацію в промислових масштабах; робить можливим існування зловмисних «роїв» ШІ.[8] Хоча кількісно оцінити безпосередній вплив контенту, створеного ШІ, на результати виборів досі складно, він вочевидь формує інформаційне середовище та посилює поширення існуючих неправдивих тверджень.[9] Це поєднання геополітичної конкуренції, передових технологій та супротивників, що адаптуються, визначає сучасний складний ландшафт націлених на вибори гібридних загроз.

1.1. ВИЗНАЧЕННЯ ГІБРИДНИХ ЗАГРОЗ У ВИБОРЧОМУ КОНТЕКСТІ

Гібридні загрози, спрямовані на вибори, є скоординованими ворожими діями, які поєднують традиційні та нетрадиційні засоби для підриву демократичних процесів, водночас залишаючись нижче порогу збройного конфлікту та часто використовуючи прогалини у виявленні/встановленні джерел та «фазові межі» між війною і миром, а також внутрішньою й зовнішньою безпекою.[10]

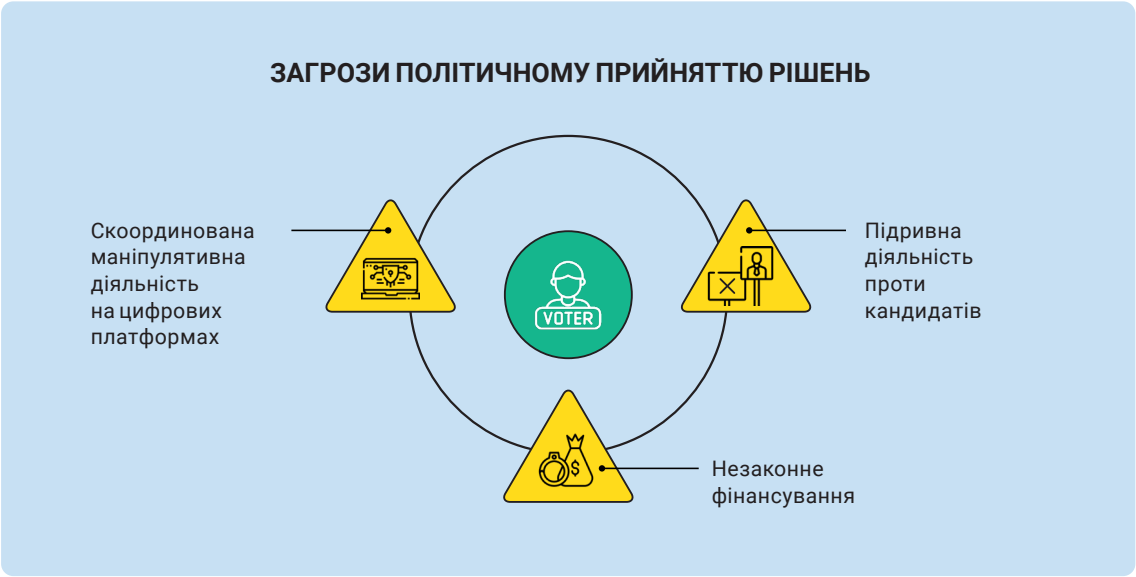
Вау (2024) визначає три категорії загроз, пов'язаних з виборчим процесом: загрози проведенню виборів, довірі до виборів та бажанню і здатності голосувати. Як розвиток цієї процес-орієнтованої структури, у даному звіті застосовується підхід з чотирма категоріями, який також охоплює загрози, спрямовані на політичне прийняття рішень. Для чіткості аналізу загрози, пов'язані з виборами, поділені на чотири групи, що можуть перекриватися: (а) проведення виборів, (б) довіра до виборів, (в) бажання/здатність голосувати та (г) політичне прийняття рішень. Разом ці категорії допомагають відрізнити порушення виборчих процесів від глибших спроб змінити переконання або підірвати легітимність:

- Загрози проведенню виборів: дії, спрямовані на порушення самого виборчого процесу, що впливають на посадових осіб, інфраструктуру або логістику за допомогою інформаційних, фізичних або кіберзасобів.

- Загрози довірі до виборів: спроби підірвати довіру громадськості до легітимності виборів шляхом поширення дезінформації, популяризації теорій змови або створення уявлення про масове шахрайство.

- Загрози бажанню та здатності голосувати: тактика, розрахована на вплив на поведінку виборців шляхом знеохочування брати участь у виборах або підриву здатності виборців віддати свій голос, наприклад, шляхом залякування або поширення неправдивої інформації про процедури.

- Загрози політичному прийняттю рішень: спроби вплинути на переконання виборців із використанням нелегітимних або незаконних засобів, зокрема скоординованої маніпулятивної діяльності на цифрових платформах, незаконного фінансування або підривної діяльності проти кандидатів



1.2. ВПЛИВ НА ЧЕСНІСТЬ ВИБОРІВ, ДОВІРУ ТА ДЕМОКРАТИЧНІ ПРОЦЕСИ

Стратегічна мета гібридних атак проти виборів полягає не лише у тому, щоб вплинути на окремий голос, але й у тому, щоб підірвати демократичні екосистеми шляхом розмивання довіри, загострення поляризації та послаблення інституційних основ демократичних держав.[11] На практиці це втілюється у наративних кампаніях, котрі ставлять під сумнів правила та «суддів», узгоджених заявах про фальсифікації та здійснюваних у заздалегідь визначений момент витоках інформації, які формують порядок денний під час періодів «передвиборчої тиші». Атакуючи авторитет та репутацію посадовців, підриваючи довіру до виборчих систем та поширюючи підбурювальну дезінформацію, такі кампанії становлять за мету поглиблення поляризації та підрив інституційної стійкості самої держави.[12]

«Стратегічна мета гібридних атак проти виборів — не лише вплинути на окремі голоси, але й підірвати демократичні екосистеми шляхом розмивання довіри, загострення поляризації...»

Хоча це не єдина причина, такі загрози, ймовірно, сприяли глобальному зниженню середньої явки виборців приблизно на 10 відсотків за останні 15 років, а також збільшенню частоти конфліктів — між 2020 та 2024 роками результати приблизно кожних п'ятих виборів не визнавалися стороною, що програла.[13]

Нещодавні виборчі цикли також демонструють беззаперечні прояви: післявиборчі заворушення та інциденти з неприйняттям результатів; інформаційні кризи, викликані операціями типу «злам та витік»; адміністративну дезорганізацію, коли кіберінциденти затримують реєстрацію виборців або повідомлення результатів виборів. У ряді випадків міжнародні спостерігачі фіксували скоординований тиск, що поєднував інформаційні впливи, незаконне фінансування та порушення, спричинені кібератаками, що додатково підсилювало вже наявну в середовищах поляризацію.[14]

Таке «розмивання» додатково ускладнюється відтоком досвідчених працівників виборчих комісій, які зіштовхуються з постійними переслідуваннями, що, в свою чергу, послаблює інституційний потенціал.[15] Ефект накопичується за схемою зворотного зв'язку: внаслідок зниження довіри зростає вразливість до маніпуляцій, а це, в свою чергу, додатково зменшує участь у виборах та згоду.[16]

Крім того, наративи про «фальсифікацію виборів» мають конкретні внутрішні наслідки — спричиняють хвилю скарг та запитів на доступ до інформації, тиск щодо проведення додаткового перерахунку голосів або «слідчої експертизи», що інтенсифікує переслідування посадових осіб та зменшує готовність визнати результати виборів. Ці наративи також поширюються за кордонами, де ті самі погляди адаптуються та наново використовуються узгоджено діючими впливовими особами («інфлюенсерами»)та пов'язаними з державами ЗМІ, формуючи очікування задовго до дня голосування.[17]

На додаток до цього ці тактики спрямовані на поглиблення суспільних розколів. Зловмисники нагнітають емоційно заряджену дезінформацію у дискусії про імміграцію, економічну політику та культурні «проблеми, що вбивають клин між людьми», підживлюючи таким чином цілеспрямовану поляризацію.[18] З точки зору механізмів дії ці кампанії підвищують значущість соціальних ідентичностей, подають політику як гру з нульовою сумою («ми проти них»), а також зв'язують емоційно «заряджені» твердження із періодами невизначеності, коли аудиторії більше покладаються на групові сигнали-маркери та спрощені наративи; у цьому стані афективна поляризація посилюється, а коректна інформація не враховується.[19]

В цих кампаніях часто використовуються негативні зображення маргіналізованих ідентичностей, включаючи гендер, расу та сексуальну орієнтацію, щоб збільшити соціальні розколи, а також непропорційно стають мішенями групи меншин та жінки.[20] Оператори також одночасно підсилюють протилежні сторони — ця тактика відома як «конвергенція ідентичностей» — і експлуатують почуття образи на їх перетинах, наприклад, там, де перетинаються релігія та гендер або клас. Це збільшує охоплення та допомагає нормалізувати ворожість між багатьма спільнотами.[21]

Внаслідок цього утворюється небезпечна петля зворотного зв'язку: поляризоване суспільство з низьким рівнем довіри стає менш стійким і ще більш вразливим до гібридних атак у майбутньому. По мірі зниження довіри збільшується суб'єктивне сприйняття загрози, яку певні групи становлять для інших, зростає соціальна дистанція, а на еліти здійснюється тиск щодо вжиття надзвичайних заходів — це умови, які антагоністи знову вводять з новими наративами та більшим впливом.[22]

1.3. ГЕОПОЛІТИЧНИЙ ВИМІР

Гібридні загрози виборам не трапляються ізольовано; вони тісно пов'язані із ширшим геополітичним ландшафтом. Інтенсивне застосування цих тактик з 2024 року підживлюється стратегічною конкуренцією між демократіями та авторитарними

державами, триваючою війною в Україні та низкою інших конфліктів із бойовими зіткненнями.[23] Росія часто розглядає вибори, як можливість послабити підтримку України, підірвати такі альянси, як Організація Північноатлантичного договору (НАТО) та Європейський Союз (ЄС), і просувати ревізіоністський курс, спрямований на зміну світового порядку.[24]

Для цих суб'єктів інформаційна війна — це не доповнення, не додаток до політики, а центральний інструмент державного управління, і вона ведеться наполегливо та асиметрично.[25]

> Демократичним суспільствам, котрі характеризуються відкритими інформаційними середовищами та відданістю свободі слова, притаманні вразливі місця, якими вміло користуються супротивники. На противагу цьому, авторитарні режими отримують перевагу від закритих, жорстко контрольованих інформаційних екосистем — це надає їм значну перевагу в захисті, яка є підґрунтям їхньої стійкості. Ця операційна асиметрія лежить в основі сучасного конфлікту.[26]

Війна в Україні відіграла роль як «лабораторії», так водночас і «каталізатора» для гібридних загроз з боку Росії. Багато тактик, методів і процедур, які застосовувалися проти виборів на Заході (і нещодавно у повному масштабі були продемонстровані в Молдові), безпосередньо пов'язані з геополітичними цілями Москви, а також зі стратегічною метою — підривом міжнародної підтримки України.[27] Відповідно, захист виборів більше не є лише внутрішньополітичним питанням; він є невід'ємною частиною міжнародної безпеки та колективної оборони самої демократичної моделі, про що неодноразово наголошували НАТО та Європейський Союз.[28]

1.4. МЕТА, СФЕРА ЗАСТОСУВАННЯ ТА МЕТОДОЛОГІЯ ЦЬОГО ЗВІТУ

Превентивна протидія викликам, що утворюються гібридними загрозами, вимагає глибокого розуміння тактики, яку застосовують суб'єкти-зловмисники, а також стратегій, необхідних для протидії їм. В рамках зобов'язань Швеції щодо зміцнення демократії та верховенства права, Академія Фольке Бернадота (FBA) підтримує цю мету — для цього вона веде дослідження та ділиться знаннями з міжнародними партнерами, котрі стикаються з такими загрозами, тим самим сприяючи розвитку більш стійких демократій. Ця підтримка виходить за межі спостереження за виборами і охоплює підтримку виборів, спрямовану на підвищення готовності та стійкості виборчого процесу.

У цьому звіті зібрано та представлено експертні знання щодо протидії гібридним загрозам для виборів, причому основна увага приділяється подіям, починаючи з 2024 року. Звіт починається загальним оглядом гібридних загроз виборам, екосистеми, в якій вони розгортаються, та їхнього загального впливу на цілісність виборів, довіру громадськості та демократичні процеси в межах сучасного глобального геополітичного контексту. Наступні розділи детальніше розглядають три ключові підходи, з використанням яких зловмисники впливають на вибори: маніпулювання інформацією та втручання, незаконне політичне фінансування та кібератаки. Далі йде розділ про протидію гібридним загрозам, зосереджений головним чином на досвіді створення мереж виборчої співпраці. Нарешті, у заключній главі представлені основні висновки та рекомендації.

Основна аудиторія цього звіту складається з установ, які беруть участь в організації, сприянні або підтримці виборчих процесів, особливо в державах, що страждають від конфліктів і є нестабільними, а також у країнах, які піддаються гібридним загрозам, особливо у Східній Європі та на Західних Балканах, де FBA діє найбільш активно. Таким чином, звіт також підкріплює практичну програму FBA зі зміцнення стійкості демократії серед суб'єктів виборчого процесу в цих регіонах.

02 Маніпулювання інформацією та зовнішнє втручання (FIMI) у вибори

Маніпулювання та втручання FIMI є основним компонентом сучасних гібридних загроз — складною машиною впливу, розрахованою на «забруднення» інформаційного середовища та маніпулювання громадською думкою. Часто спостерігається стратегія, в рамках якої виробництво контенту в промислових масштабах поєднується з багаторівневим поширенням.[29]

По-перше, зловмисники створюють величезну кількість контенту — від статей і мемів до зображень-діпфейків, створених за допомогою штучного інтелекту — ретельно виробленого для експлуатації суспільних «проблем, що вбивають клин між людьми», таких як імміграція та економічна тривога.[30] По-друге, цей контент поширюється за допомогою низки методик, включаючи автоматизовані мережі ботів, скоординовані несправжні облікові записи та схеми «впливу за винагороду», в яких для відмивання замовлених державами наративів залучаються оплачувані впливові особи-інфлюенсери.[31] При цьому часто застосовується інфраструктура введення в оману, як-от метод «двійників» — створення копій справжніх веб-сайтів новин для придання дезінформації зовнішньої достовірності.[32]

> *«...свідчить про стратегічні наміри, які сягають далеко за межі втручання у вибори, натомість ставлячи за мету ведення тривалої та безперервної інформаційної війни»*

Ці тактичні зусилля спрямовуються у межах загальних стратегічних рамок. Витоки російських документів свідчать про те, що операції спрямовуються за ретельно пропрацьованими «методичками» (посібниками з наративів), в яких детально описується, як слід загострювати внутрішні напруження для досягнення зовнішньополітичних цілей. Це свідчить про стратегічні наміри, які сягають далеко за межі втручання у вибори, натомість ставлячи за мету ведення тривалої та безперервної інформаційної війни.[33]

2.1. ОСТАННІ ТЕНДЕНЦІЇ

Період із початку 2024 року надав низку різких та яскравих прикладів із реального життя, котрі проливають світло на еволюцію тактик і ескалацію інтенсивності гібридних загроз, що спрямовані на демократичні вибори. Ці події, що охоплюють ЄС, Сполучені Штати (США) та східну частину Європи, надають важливі уявлення про поточні операційні тактики та методології суб'єктів-зловмисників, а також про вразливості, якими вони прагнуть скористатися.

Вибори до Європейського парламенту 2024 року: Транснаціональна ціль

Вибори до Європейського парламенту в червні 2024 року були значущою транснаціональною метою для кампаній FIMI: фактчекери виявили різку інтенсифікацію дезінформації, спрямованої на ЄС, щонайменше в одинадцяти країнах.[34] Російське «Агентство соціального проєктування» організувало «Всебічну контркампанію проти Європи», спрямовану на підтримку ультраправих кандидатів та кандидатів-євроскептиків шляхом посилення наративів про економічне розорення та розмивання національних цінностей.[35] Ця кампанія частково реалізовувалася через розгалужену мережу «двійників», у якій були задіяні клоновані веб-сайти ЗМІ та усталені мережі впливу, крізь які дезінформація Кремля нагніталася в інформаційну екосистему Європи.[36]

Скасовані вибори в Румунії: переломний момент

У серйозній демонстрації впливу Конституційний суд Румунії скасував результати першого туру президентських виборів наприкінці 2024 року, пославшись на скоординоване іноземне втручання та непрозоре онлайн-фінансування. Розвідувальні служби виявили складну кампанію, орієнтовану на TikTok, де платні мережі інфлюєнсерів і масштабна маніпулятивна діяльність підсилювали позиції раніше маргінального прокремлівського кандидата, масштаби присутності якого в Інтернеті не відповідали задекларованим витратам на кампанію.[37] На рівні ЄС Комісія ініціювала формальне провадження за Актом про цифрові послуги (DSA) для розслідування щодо зниження пов'язаних з TikTok ризиків та визначення рекомендованих систем у зв’язку з виборами у Румунії.[38]

Аналітики виявили мережу з тисяч неактивних і перехоплених облікових записів, причому для багатьох з них вдалося відстежити зв’язок із Росією та Іраном. Ці записи були активовані для затоплення платформи маніпулятивним контентом. Як описано в розділі 3, це поєднувалося з явними ознаками незаконного іноземного фінансування, оскільки масштаби присутності кандидата в Інтернеті не відповідали офіційно оголошеним витратам на кампанію. Незалежні спостерігачі закликали до обережності, зазначаючи, що довести прямий причинно-наслідковий зв'язок між активністю в Інтернеті та поданими голосами складно, проте цей випадок ілюструє, як добре забезпечена ресурсами кампанія FIMI може підірвати довіру до результатів виборів такою мірою, що їх оголосять недійсними. Водночас румунський випадок викликав критику, оскільки спостерігачі зауважували: якщо покладатися на засекречені розвідувальні дані, утворюються прогалини стосовно прозорості та можливості оскарження. Крім того, вони стверджували, що з такими радикальними засобами виникає ризик вийти за межі поставленої мети.

Боротьба Молдови: вибори «під гібридним вогнем»

Молдова є поточним прикладом країни, яка захищається від інтенсивної та комплексної гібридної атаки. У той час, як атака Росії на Україну в 2014 році заклала основи методики «зламати та транслювати» («hack-and-broadcast»), у якій кібервторгнення поєднується з маніпулюванням інформацією,[39] діяльність Росії в Молдові переросла у стан безперервного тиску в багатьох сферах одночасно, спрямованого на захоплення держави через виборчі урни.[40]

Під час президентських виборів у 2024 році та референдуму щодо вступу до ЄС країна зіткнулася з тим, що іноземні спостерігачі називали «гібридною війною», яка керується з-за кордону.[41] Зовнішнє маніпулювання інформацією та втручання (FIMI) слугувало опорним центром, довкола якого вибудовувалися ці примус та введення в оману у багатьох сферах. Суб’єкти, що діяли узгоджено з Росією, проводили визначену наративом кампанію з формування образу некомпетентного проєвропейського уряду; вона підсилювалася скоординованою діяльністю мереж у Telegram та Молдовської православної церкви.[42] Цей інформаційний наступ фінансувався за рахунок

масштабного незаконного фінансування (за певними оцінками, олігарх-втікач перевів 39 мільйонів доларів США на фінансування підкупу виборців та протестів), а також доповнювався загрозами фізичної дестабілізації, як-от фальшивими повідомленнями про мінування на виборчих дільницях діаспори.[43]

Тактика, що застосовувалася у 2024 році, була попередником ще більш інтенсивної кампанії, спрямованої на ключові парламентські вибори у вересні 2025 року. Витік документів з Кремля розкрив багатофакторну стратегію, спрямовану на підрив руху Молдови до ЄС і, зрештою, на усунення президента Санду від влади.[44] У цьому плані детально розкривалася типова модель гібридної загрози, в тому числі наступне:

- Широкомасштабна кампанія дезінформації у соціальних платформах, як-от Telegram, TikTok і Facebook, з використанням наративів, що зображали президента Санду іноземною маріонеткою, яка штовхає країну до війни.[45]

- Масштабне незаконне фінансування для купівлі голосів і фінансування проросійських партій.[46]

- Використання компрометуючих матеріалів (компромату) для тиску на посадовців і вербування молдавської діаспори для поїздок і голосування.[47]

- Вербування молодих чоловіків зі спортивних клубів і кримінальних мереж для організації провокацій з насильством та руйнівних протестів.[48]

Цей план активно впроваджувався в життя. 22 вересня 2025 року, лише за кілька днів до виборів, молдовська влада провела масштабну операцію з демонтажу підтримуваного Росією плану дестабілізації. Поліція затримала 74 особи та провела понад 250 обшуків, розкривши мережу, яка, ймовірно, діяла за підтримки російської розвідувальної служби ГРУ та керувала медіагрупою «Траст», поширюючи пропаганду.[49] Це відбулося після попередніх спроб вжити жорстких заходів на інформаційному фронті, включно з офіційним запитом на блокування 443 каналів у TikTok.[50]

Перелічені дії відбувалися на додаток до постійного кібертиску. З 2022 року проросійські хакерські групи розпочали кібератаки на державні установи, створили сайти для публікації витоків інформації та здійснили злам серверів електронної пошти парламенту в рамках підготовки до операцій «злам та витік» («hack-and-leak»).[51] У відповідь на цю ескалацію загроз, що відбувалася, Молдова отримала суттєву міжнародну підтримку. У 2023 році в Республіці Молдова була створена Партнерська місія Європейського Союзу в Молдові (EUPM) з метою підвищення стійкості Молдови до гібридних загроз, включаючи загрози з кібербезпеки та FIMI. Крім того, у 2025 році Європейський Союз розгорнув у Кишиневі Групу швидкого реагування на гібридні загрози та Резерв кібербезпеки ЄС (це була перша в історії активація механізму швидкої кібердопомоги ЄС) для підтримки захисту виборів у країні.[52]

У сукупності випадок Молдови демонструє реальність сучасного втручання у вибори: це не серія відокремлених інцидентів, а цілком інтегрована гібридна війна. Він підкреслює для держав необхідність використовувати міжнародний досвід, вчитися одна в одної та будувати загальносуспільний захист, щоб зміцнювати свої критично важливі демократичні системи.

Україна: інформаційна війна як інструмент звичайного конфлікту

Оскільки вибори в Україні в умовах воєнного стану призупинені, кампанії маніпулювання та втручання FIMI Росії проти України грають роль випереджувального нападу на майбутні демократичні процеси останньої. «Комплексна контркампанія проти України» Агентства соціального проєктування є прямим інструментом воєнних зусиль, спрямованим на підрив керівництва України,

деморалізацію її збройних сил та погіршення соціальної згуртованості.[53] Посилюючи наративи про корупцію та розпалюючи політичну конкуренцію, ця довгострокова кампанія прагне забезпечити роздробленість електорату та його сприйнятливість до проросійських альтернатив тоді, коли будуть проводитися післявоєнні вибори.[54]

Нинішні зусилля розвинулися на основі попередніх методик, у яких кібервторгнення поєднувалися з маніпулюванням інформацією. Перед і під час президентських виборів в Україні у 2014 році політичні мережі, медіа-активи та посередники олігархів, орієнтовані на Москву, були мобілізовані, щоб просувати прокремлівську повістку та уповільнити рух України до Європи. Проросійські партії та фігури відігравали роль векторів для узгодження політик та посилення меседжів, в той час як бізнес-інтереси, пов'язані з Росією, розширювали вплив Москви.[55] Паралельно кібервтручання було спрямоване на механізми виборів: вторгнення у Центральній виборчій комісії призвели до видалення файлів та встановлення шкідливого програмного забезпечення, призначеного для відображення сфабрикованих результатів; вони були доповнені атаками типу «розподілена відмова в обслуговуванні» (DDoS), щоб затримати звітування; російське державне телебачення у подальшому транслювало підроблені графіки — це був ранній приклад об'єднання кібервторгнення із маніпулюванням інформацією.[56] Очікується, що наступні вибори в Україні відбуватимуться у складних умовах, оскільки країна, ймовірно, зіткнеться з посиленими зовнішніми спробами вплинути на виборчий процес або зірвати його.

Президентські вибори у США 2024 року: масова атака багатьох суб'єктів

Вибори в США у 2024 році стали центром уваги для багатьох іноземних суб'єктів з різними планами та програмами дій.[57] Росія вибудувала широкий арсенал заходів, починаючи від фальшивих повідомлень про мінування на виборчих дільницях до створених ШІ діпфейків, подальшого використання своєї мережі впливу «двійників» та мобілізації своїх проксі-представників усередині країни.[58] Міністерство юстиції США зірвало діяльність мережі «двійників», вилучивши 32 домени та пред'явивши звинувачення російським оперативникам, пов'язаним із російськими державними ЗМІ.[59] Діяльність Китаю була більш цілеспрямованою, вона зосереджувалась на лініях розлому «культурної війни» в США та на місцевих виборах замість президентських перегонів.[60] Іран поєднував онлайн-розвідку з операціями «злам та витік» («hack-and-leak»), при цьому влада США звинувачувала осіб, пов'язаних з Іраном, у спробі компрометації президентської кампанії шляхом викрадення та організації витоку матеріалів.[61] У відповідь американські агентства зайняли позицію «випереджувального розвінчування» (пребанкінгу) та застосували комбінацію висунення обвинувачень, санкцій і конфіскацій, щоб підвищити витрати зловмисників на діяльність та зруйнувати їхню інфраструктуру.[62]

Незалежні оцінки вказують, що, хоча сукупні зусилля зі впливу були значними та дедалі більше підкріплювалися штучним інтелектом, операційний вплив на основні механізми виборів був обмеженим — проте шкода від інформаційних загроз (плутанини, поляризації, цинізму) залишається центральним ризиком для майбутніх циклів.[63]

2.2. ПРОБЛЕМИ ВИЯВЛЕННЯ, ВСТАНОВЛЕННЯ ДЖЕРЕЛ ТА РЕАГУВАННЯ

У захисті проти FIMI існує декілька дуже серйозних складностей. Критичною проблемою залишається атрибуція (встановлення джерела атаки), оскільки використання проксі-посередників та складні методики «відмивання» інформації навмисно розроблені з розрахунком на неоднозначності та перешкоджання своєчасному, пропорційному реагуванню.[64] Величезні швидкість та масштаби сучасних кампаній атак, що підсилюються штучним інтелектом, часто перевантажують традиційні засоби протидії, як-от перевірку фактів (фактчекінг).[65] Крім того, перед демократіями постає складна проблема досягнути балансу між безпекою та свободою слова — дилема, яку зловмисники експлуатують, подаючи дії з захисту, як цензуру.[66]

Центральною проблемою є підзвітність платформ, адже бізнес-моделі багатьох компаній соціальних мереж винагороджують поляризуючий контент, який максимізує залучення.[67] Забезпечення значущої прозорості щодо алгоритмів ранжування, правил модерації контенту та доступу дослідників до даних залишається суперечливим регуляторним і політичним викликом.[68] Акт про цифрові послуги (DSA) ЄС — це значуща регуляторна відповідь, яка перекладає зобов'язання на дуже великі онлайн-платформи задля оцінки системних ризиків та підвищення прозорості. Забезпечення виконання цього Акту вже почалося, із формальними процедурами, пов'язаними з цілісністю виборів у 2024 році, проте його дотримання залишається нерівномірним.[69] Паралельно платформи переглядають свій підхід: Google і Meta оголосили про плани обмежити або припинити політичну рекламу в ЄС, посилаючись на новий регуляторний ландшафт.[70]

У той час як регулювання посилюється, інші форми прозорості руйнуються. Внаслідок припинення компанією Meta експлуатації свого інструменту CrowdTangle, який надавав у реальному часі аналітику про публічний контент у соціальних мережах, прозорість мереж впливу напередодні важливих виборів 2024 року погіршилася.[71] Добровільні галузеві ініціативи, як-от «Технічна угода» («Tech Accord») щодо протидії оманливому використанню ШІ на виборах, піддаються критиці за відсутність підзвітності та вимірюваних орієнтирів.[72]

У напрямку визначення та підтвердження походження матеріалів від ШІ відкрився новий «фронт» підзвітності. Хоча для маркування автентичних медіа-матеріалів приймаються відкриті стандарти, як-от C2PA Content Credentials, вони стикаються з динамікою «кота і миші» внаслідок неповноти охоплення.[73] Водночас такі інструменти, як SynthID від Google DeepMind, вбудовують непомітні та надійні водяні знаки безпосередньо в медіа, згенеровані ШІ, під час їх створення.[74] Однак навіть у власних чатботах ШІ Google цей стандарт ще не впроваджений, і виявляти створений ними контент досі ще неможливо. Це підкреслює нагальну потребу в сильних і сумісних стандартах щодо зазначення походження контенту, дотримання яких забезпечувалося б примусово.

Оскільки генеративний ШІ продовжує знижувати витрати на операції впливу, навіть коли платформи додають захисні засоби проти такого застосування, підтримання регуляторного контролю та нагляду за цими операціями залишатиметься складною проблемою.[75] Дослідження також задокументували випадки, коли пов'язані з державами або такі, що знаходяться під санкціями суб'єкти могли придбати або розмістити контент впливу всупереч політиці платформ, що підкреслює потребу в можливості аудиту технічних засобів керування показом реклами рекламою та санкційного контролю, які працювали б на практиці.[76]

2.3. ЩО МОЖНА ЗРОБИТИ? СТРАТЕГІЇ ПРОТИДІЇ АТАКАМ FIMI НА ВИБОРИ

Еволюція втручання у вибори — від епізодичних атак до стану хронічного, системного інформаційного конфлікту — вимагає принципової зміни оборонної стратегії. Швидкість і масштаб сучасних кампаній FIMI, котрі підсилюються штучним інтелектом, часто випереджають традиційні контрзаходи, як-от перевірку фактів (фактчекінг), що відбувається реактивно. Тому ефективне реагування має бути проактивним, багатошаровим і здійснюватися у співпраці, спрямоване на інституційну, регуляторну та технологічну сфери джерела загрози. Надзвичайно важливо те, що протидія загрозам FIMI потребує концептуальної відповіді, яка буде сумісна з демократичними нормами. Сучасний підхід з повагою до прав людини, прийнятий у Європейському Союзі, орієнтується на поведінку. Він зосереджується на виявленні спостережуваної маніпулятивної поведінки, такої як мережі ботів або скоординовані маніпулятивні облікові записи. Це дає змогу державному органові протидіяти ворожим операціям на міцній, доказовій основі, не підриваючи при цьому свободу слова.[77]

«Надзвичайно важливо те, що протидія загрозам FIMI потребує концептуальної відповіді, яка буде сумісна з демократичними нормами»

Загальноурядовий підхід через мережі співпраці

У цьому звіті підкреслюється, що зловмисники свідомо експлуатують розриви між обов'язками різних державних органів, внаслідок чого ізольоване та розрізнене реагування на загрози безпеці виявляється недостатнім. Фундаментальна стратегія протидії маніпулюванню та втручанню FIMI, націленому на вибори, полягає у створенні нарівно інтегрованого та мережевого захисту, як це робилося у декількох країнах під час недавніх виборів (що детально описано в розділі 5).

Посилення нормативно-правової бази

Центральною проблемою у протидії маніпуляціям FIMI є підзвітність платформ. Акт DSA ЄС надає провідну модель регулювання інформаційного середовища, незважаючи на існуючі дебати щодо його застосовності. Закон перекладає на «дуже великі інтернет-платформи» зобов'язання щодо оцінки системних ризиків для демократичних процесів, підвищення прозорості систем рекомендацій цих платформ та надання перевіреним дослідникам доступу до даних. Гарантоване застосування таких принципів є критично важливим для створення інформаційного середовища, котре буде менш вразливе до маніпуляцій за своєю архітектурою.

Цей регуляторний підхід також має поширюватися на незаконне політичне фінансування, яке є центральним напрямком фінансування кампаній FIMI. Дуже важливо перекрити лазівки, пов'язані з анонімними онлайн-пожертвами, нерегульованим використанням сторонніх активістів і непрозорими витратами на рекламу в соціальних мережах (як детально описано в розділі 3).

Сприяння стійкості всього суспільства

Орієнтований виключно на державу захист є недостатнім, оскільки довгострокова демократична стійкість залежить від поінформованого, критично налаштованого та залученого суспільства. Тому ключовою стратегією є інвестування у загальносуспільний підхід, який надає громадянам більше можливостей і зміцнює суспільний інформаційний простір «знизу догори».

Невід'ємною частиною цього підходу є екосистеми незалежних ЗМІ. Проте вони часто працюють у складних умовах — фінансова нестабільність, ринкова концентрація, політизована державна реклама, правовий або фізичний тиск — що загрожує як сталості їх діяльності, так і редакційній незалежності. Для вирішення цих проблем потрібно докласти зусиль за додатковими напрямками.

Національні ініціативи з підвищення медіаграмотності та грамотності в галузі ШІ необхідні для надання громадянам навичок з критичного розпізнавання та оцінки маніпулятивного контенту, що зміцнить «когнітивний захист» населення. Вони мають бути доповнені стійкою підтримкою незалежних ЗМІ, оскільки різноманітний і добре забезпечений ресурсами медіапростір є життєво важливим бар'єром проти дезінформації, адже він пропонує громадянам надійні, засновані на фактах альтернативи пропаганді, яка фінансується державою.

Важливим елементом цієї підтримки є спеціальні інвестиції у журналістику розслідувань. Журналістські розслідування знову та знову виявляються найефективнішими у викритті механізмів гібридних загроз — від розкриття складних схем незаконного фінансування та картографування мереж дезінформації до виявлення суб'єктів, що стоять за операціями «зламу та витоку» («hack-and-leak»). Така робота є надзвичайно важливою не лише для розуміння ситуації громадськістю, але й для забезпечення доказової бази, необхідної для офіційних кроків з боку уряду.

Побудова проактивного захисту та технологічної стійкості

Враховуючи складність видалення дезінформації після того, як її вже буде поширено, необхідна проактивна позиція. Проте мета полягає не у протидії кожному неправдивому твердженню, що циркулює в мережі. Основна увага приділяється радикальній і повсякденній прозорості, яка зменшує неоднозначність і надає підтверджувані факти, на які можуть покладатися інші.[78]

На практиці це реалізується через публічно доступний центр «джерел достовірної інформації» («source-of-truth»), який містить процедури, часті запитання та відповіді на них, виправлення та журнали змін і створює еталон для пошуку громадськістю та ЗМІ достовірної інформації, а також слугує довготривалою точкою відліку під час інцидентів.[79] Такі практики значно скорочують інформаційні прогалини, якими користуються зловмисники, і з часом зміцнюють довіру до інституцій.[80]

У рамках цього підходу до прозорості випереджувального розвінчування (пребанкінг) використовується вибірково та обмежується певними проміжками часу, що перекривають відомі періоди ризику (реєстрація, голосування, оприлюднення результатів виборів), щоб превентивно здійснювати «щеплення» від тактик, а не спростовувати кожен окремий наратив, водночас враховується нерівномірність засвоєння та неповнота документування джерел походження інформації.[81] Акцент робиться на стислих поясненнях «чого очікувати/як перевірити/куди повідомляти», які допомагають аудиторії розпізнавати шаблони маніпуляцій (наприклад, підроблений вміст, тактику подання «злам та витік») і спрямовують увагу на канонічну сторінку.[82] Такий підхід до розвінчування дезінформації заздалегідь є економічно ефективним стимулятором прозорості, а не паралельною війною конкуруючих версій контенту.[83]

Цей підхід визнає існування обмежень. Протидіяти кожному фрагменту дезінформації неможливо, а мотивована аудиторія іноді віддаватиме перевагу брехні, котра виглядає послідовною та узгодженою. Тому стратегія полягає в тому, щоб контролювати факти, зменшувати неоднозначність і протидіяти маніпулятивній поведінці — так надійні діячі матимуть стабільну точку відліку, а громадськість — прогнозований ресурс для перевірки інформації.[84]

Ця стратегія прозорості повинна поєднуватися з планом вирішення проблеми технологічної гонки озброєнь, зокрема проблеми синтетичних медіа, що створюються за допомогою ШІ. Захист від діпфейків та імітації голосу вимагає виходу за межі простого виявлення, яке «застрягло» в динаміці, приреченій постійно наздоганяти супротивників.[85] Перспективна стратегія полягає в інвестуванні та впровадженні обов'язковості технологій відстеження джерел походження вмісту та його маркування водяними знаками. Відкриті стандарти, такі як стандарт метаданих контенту C2PA Content Credentials, котрі слугують цифровою міткою автентичності, а також надійні інструменти маркування водяними знаками, як-от SynthID від Google DeepMind, котрий вбудовує непомітний для людини, але доступний машинам підпис у медіа, згенеровані ШІ, під час їх створення, є надзвичайно важливими для відновлення базового рівня довіри у цифровій екосистемі.[86]

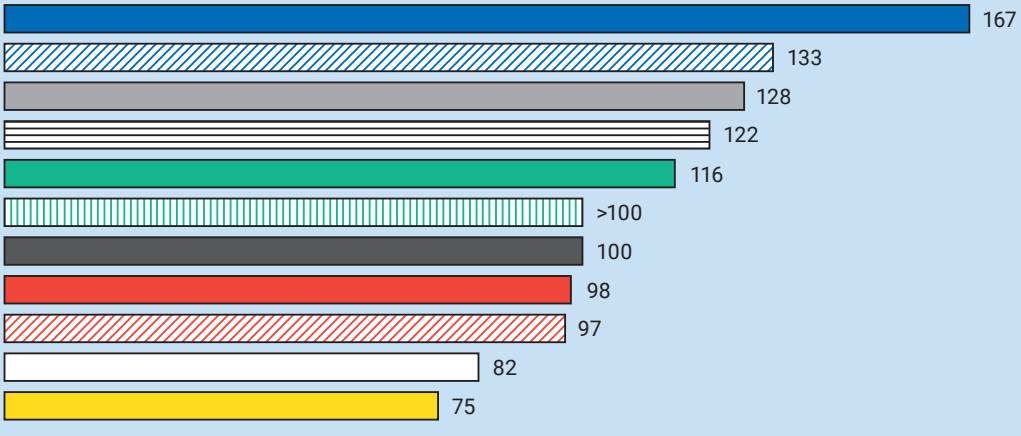
У кінцевому підсумку ці стратегії повинні бути інтегровані між собою. Як зазначено у всеосяжних висновках звіту, захист виборів у сучасну епоху має бути безперервним, адаптивним, проактивним і здійснюваним у співпраці процесом.

03 Незаконне політичне фінансування та гібридні загрози

Гроші самі по собі не є корупційним чинником для виборів; навпроти, вони є необхідними. Партії використовують їх для просування ідей, набору членів і підготовки кандидатів, в той час як виборчим органам вони потрібні для громадянської освіти та адміністрування логістики виборів. Проте гроші в політиці створюють серйозні ризики для демократії — від нерівного доступу до фінансування та корупційних стимулів до незаконного або забороненого фінансування, спрямованого на вплив на вибори.[87]

Це включає кошти, які незаконно або неправомірно використовуються для втручання у вибори в країні та за кордоном. Останнє явище викликає особливу стурбованість, якщо враховувати спотворення, які воно спричиняє у демократичній системі, ерозію довіри громадськості, яку воно породжує, і геополітичні наслідки, які воно тягне за собою.

ОСНОВНІ ПРАВИЛА ПОЛІТИЧНОГО ФІНАНСУВАННЯ
(за кількістю країн)



Іноземне втручання у вибори через незаконне політичне фінансування визнається дедалі частіше, хоча це не нове явище. Наприклад, у Чорногорії, під час парламентських виборів 2016 року були озвучені звинувачення в іноземному фінансуванні кампанії, із твердженнями, що опозиція служить іноземним інтересам, в той час як у Молдові в 2021 році спостерігачі аналогічно висловлювали занепокоєність щодо іноземного фінансування під час позачергових виборів.[88]

3.1. НЕЗАКОННЕ ПОЛІТИЧНЕ ФІНАНСУВАННЯ ЯК ВЕКТОР ВТРУЧАННЯ

Існує три критичні напрямки, за якими зловмисники зазвичай намагаються впливати на вибори за допомогою незаконного політичного фінансування. Це: (1) підкуп виборців; (2) іноземні та анонімні пожертви, у тому числі в криптовалютах; та (3) внески третіх сторін, фінансування реклами у соціальних мережах та інфлюенсерів.

Підкуп виборців

Хоча підкуп виборців заборонений у 167 країнах, він залишається поширеним засобом впливу на вибори.[89] Під час парламентських виборів у Молдові 2025 року міжнародні спостерігачі відзначали широкий масштаб виявлених схем підкупу, спрямованих на вплив на виборців, причому ці зусилля координувала організована мережа, фінансована Росією.[90]

Країна вже мала діло з подібними проблемами на попередніх виборах. Наприклад, на місцевих виборах 2023 року політичних діячів, пов'язаних з Росією, звинувачували у спробі переказу коштів в країну з метою підкупу виборців, що просувало російські інтереси.[91] Ще гірше те, що на президентських виборах 2024 року та конституційному референдумі міжнародні спостерігачі відзначали, як правоохоронні органи, багато суб'єктів міжнародних відносин та представників громадянського суспільства описували Молдову, як об'єкт поточної «гібридної війни», що включала незаконне політичне фінансування, дезінформацію та кібератаки.[92]

Вважається, що ці схеми включали роздачу Росією платіжних карток. Аналітики описували ймовірний спосіб дій наступним чином:

> Повідомляється, що мільйони доларів готівкою завозяться контрабандою в країну особами, пов'язаними з втікачем-олігархом із санкційного списку США Іланом Шором, якому вдалося обійти зусилля правоохоронних органів з припинення незаконного руху коштів. Влада організувала обшуки в аеропорту, щоб зупинити цей конвеєр осіб, які подорожували до Москви та поверталися із контрабандними грішми. Проте Росія знайшла інші способи переводити кошти у Молдову. Через російську платіжну систему «Мир» фінансові ресурси, як повідомляється, спрямовуються молдовським виборцям, зокрема через економічні мережі у регіоні Придністров'я — сепаратистській території, яка давно служить базою для операцій впливу Москви.
>
> Влада Молдови підняла тривогу через масштабний підкуп виборців, причому Генеральний інспекторат поліції задокументував випадки підкупу за участю щонайменше 130 000 громадян, а також незаконні перекази з Росії на суму понад п'ятнадцять мільйонів доларів США лише у одному вересні. У дійсності масштаби могли бути набагато більшими; деякі посадові особи оцінюють їх приблизно у 100 мільйонів доларів США за всю кампанію.
>
> Кошти спрямовуються на схеми, розраховані на створення загальнонаціональної мережі підкупу виборців, подібно до фінансових пірамід — із складними шарами транзакцій, розрахованими на уникнення перевірок.

Призначення коштів варіюється від «соціальних виплат» молдовським пенсіонерам до «премій» до заробітної плати для працівників місцевих державних структур у автономному територіальному утворенні Гагаузія. Зараз гроші також, за даними поліції та незалежними повідомленнями, потрапляють до рук так званих місцевих «координаторів» і «прихильників» виборчого блоку «Перемога» — політичного утворення, створеного в Москві і, як повідомляється, контрольованого з неї (Olari 2024).

Іноземні та анонімні пожертви

Заборона або обмеження на іноземні та анонімні пожертви є одним із найпоширеніших правил політичного фінансування. Станом на 2025 рік 128 країн забороняють іноземним донорам перераховувати пожертви політичним партіям, а понад 100 країн поширюють цю заборону також на кандидатів. Анонімні пожертви також обмежені — у 100 країнах для партій і у 75 країнах для кандидатів.[93]

Заборона на іноземні пожертви зазвичай ґрунтується на тому положенні, що зовнішні інтереси не мають впливати на національну політику. На противагу цьому, заборона на анонімні пожертви зазвичай спрямована на блокування внесків, котрі без анонімності виявилися б незаконними. Проте впровадження цих правил є одною із найскладніших задач наглядових органів. Іноземні внески для втручання у вибори можуть потрапляти крізь кордони здебільшого непоміченими, часто проходячи транзитом через офшорні юрисдикції та «податкові оази»-офшори, де їхнє справжнє джерело легко приховати; це надзвичайно ускладнює відстеження коштів і однозначну ідентифікацію їхнього іноземного походження.[94]

Криптовалюти додатково ускладнюють ситуацію, роблячи можливими непрозорі фінансові потоки, зокрема ті, що надходять від суб'єктів-зловмисників, які прагнуть впливати на вибори за кордоном. Їхнє використання швидко зросло за останнє десятиліття: хоча Bitcoin зберігає лідерство, зараз на більш ніж 1300 біржах торгується понад 16 000 видів криптовалют, а кількість їх користувачів у всьому світі оцінюється в 861 мільйон — близько 11 відсотків населення світу у більш ніж 150 країнах.[95] Очікується, що цей ринок продовжуватиме зростати, а вартість торгівлі криптовалютами, за прогнозами, зросте з 71,35 мільярда доларів США у 2025 році до понад 260 мільярдів доларів США у 2032 році.[96]

На політичне фінансування це впливає безпосередньо, оскільки анонімність більшості транзакцій з криптовалютами надзвичайно ускладнює відстеження пожертв з-за кордону.[97] Одним із помітних прикладів стали президентські вибори в США у 2016 році, коли обвинувальний акт журі присяжних визначив, що російські кошти, як стверджується у ньому, спрямовувалися через біржі криптовалют.[98] Цей випадок підкреслив обмеженість нагляду, продемонструвавши, що навіть системі з відносно надійними засобами безпеки було складно впоратися з криптовалютами, оскільки законодавство дозволяло політичним комітетам приймати внески, вживаючи лише «мінімально інвазивні» заходи для перевірки національності донорів.

Внески третіх сторін, фінансування реклами у соціальних мережах та інфлюенсерів

Витрати третіх сторін можуть слугувати каналом постачання іноземних коштів, насправді призначених для впливу на вибори, коли організації або особи, включаючи фіктивні компанії, неурядові (НУО) або благодійні організації, виступають як підставні організації-«ширми», проводять кампанії за або проти певних партій і кандидатів та стають провідниками зовнішнього впливу.[99]

Реклама в соціальних мережах є ще одним потужним інструментом для збору коштів і політичних операцій, причому витрати на цифрові кампанії різко зростають у всьому світі, особливо після пандемії COVID-19.[100] Реклама в онлайн-медіа надає іноземним суб'єктам легкий спосіб втручатися у вибори, що забезпечується фізичною відстанню між джерелами реклами та їхніми цілями, а також можливістю здійснювати мікротаргетинг і персоналізовувати згенерований контент.[101] Наприклад, іноземний суб'єкт може купувати послуги обміну повідомленнями в соціальних мережах на користь кампанії, поза межами нагляду всередині країни, в той час як непрозорість онлайн-платежів дає змогу донорам залишатися анонімними.[102]

Скандал із Cambridge Analytica у 2018 році був раннім прикладом цього явища, пов'язаним із неналежним використанням приватних даних Facebook понад 50 мільйонів користувачів цієї соціальної мережі під час виборів у США 2016 року. Під час нього також було викрите незаконне працевлаштування десятків іноземних громадян, чия робота над формуванням повідомлень кампанії, аналізом даних і рекламою була визнана незаконним закордонним внеском у натуральній формі.[103]

Вибори в США 2024 року слугують одним прикладом. В рамках «Операції "двійник"» («Operation Doppelganger») Міністерство юстиції США вилучило 32 інтернет-домени, які використовувалися російським урядом для кампаній зловмисного впливу. За результатами розслідування, операція спиралася на оплачуваних інфлюенсерів, платну рекламу в соціальних мережах, частина якої була згенерована ШІ та використовувала підроблені профілі в соціальних мережах, що видавали себе за громадян США або інших країн, але не Росії, щоб спрямувати користувачів на сайти, які були незаконно зареєстровані на чужі доменні імена (кіберсквоттинг) і маскувалися під справжні новинні видання.[104]

Того ж року на виборах у Румунії спостерігалася подібна картина, що врешті-решт призвело до їх анулювання. Один із кандидатів не повідомив про витрати на кампанію, незважаючи на значну присутність в інтернеті, в той час як розвідувальні дані свідчили про наявність незадекларованого фінансування із зовнішніх джерел. Ця справа висвітлила ширші ризики стратегічної корупції, включно з фінансуванням від третіх сторін через проксі-посередників цифрової реклами без розкриття її походження або дотримання встановлених законом максимальних обмежень; гібридною політичною «фінансовою війною», що збільшує вплив у Інтернеті з-за кордону; а також недостатнім наглядом з боку виборчих органів, які не здатні відстежувати складні мережі цифрової реклами.[105]

Зовсім недавно, під час другого туру президентських виборів у Польщі у 2025 році, міжнародні спостерігачі повідомили про підозри щодо фінансування оголошень у

Facebook з-за кордону. Між серединою квітня та серединою травня два нові профілі витратили приблизно 500 000 злотих (139 000 доларів США) на понад 100 рекламних відеороликів, які підтримували одного кандидата та критикували інших, причому ця сума перевищила витрати на політичну рекламу самих кандидатів. Розгляд цієї справи щодо ймовірного іноземного фінансування наразі триває. Спостерігачі розкритикували затримку з реакцією з боку влади, в той час як Meta заявила, що відповідні оголошення не порушували ані її стандартів, ані національного законодавства. Інший обліковий запис, як виявилось, розмістив рекламу на суму 388 000 злотих (приблизно 108 000 доларів США), ймовірно, за кошти, переведені з-за кордону через організацію громадянського суспільства. І хоча до Національної виборчої комісії та прокуратури було подано скарги на ймовірне незаконне іноземне фінансування, спостерігачі відзначили наступне: «хоча Meta застосовує (автоматизованими засобами) обмеження витрат рекламодавців, втілення соціальною платформою її внутрішніх правил наразі виходить за межі поточних повноважень органу, який здійснює нагляд за фінансуванням виборчих кампаній».[106] Цей випадок підкреслює зростаючу проблему, яку іноземне фінансування онлайн-кампаній становить для національних механізмів нагляду, а також обмеження існуючих нормативних рамок щодо забезпечення прозорості та підзвітності у цифровій політичній рекламі.

3.2. ЩО МОЖНА ЗРОБИТИ? СТРАТЕГІЇ З ПОСИЛЕННЯ РЕГУЛЮВАННЯ ПОЛІТИЧНОГО ФІНАНСУВАННЯ ТА НАГЛЯДУ ДЛЯ ПРОТИДІЇ ІНОЗЕМНОМУ ВТРУЧАННЮ

Враховуючи численні вищезазначені виклики, чи не слід зосередити реагування на встановленні більш суворих правил політичного фінансування або на посиленні нагляду?

Посилення регулювання

Типовою реакцією є зниження лімітів пожертвувань і обмеження витрат на кампанії. Хоча іноді це необхідно і навіть бажано, надмірні обмеження ризикують створити нові дисбаланси і в кінцевому підсумку вплинути на результат виборів. Як згадувалося вище, партії та кандидати потребують доступу до законних коштів для ведення своєї діяльності без втручання; без цих коштів вони можуть вдатися до прихованої іноземної підтримки або заниження звітності про доходи та витрати.[107]

Незважаючи на це, жорсткіші нормативи часто потрібні для запобігання або пом'якшення гібридних загроз виборам, хоча такі заходи мають бути ретельно пропрацьовані, щоб гарантувати, що ці заходи протидії в свою чергу не призведуть до нових спотворень або обмежень, які будуть підривати основні демократичні принципи.

Заборони та обмеження

Важливим кроком є заборона іноземних та анонімних пожертв партіям і кандидатам там, де вони ще не заборонені.[108] Регулюючі нормативи також можуть бути вдосконалені шляхом узгодження періодів звітування із фактичними термінами проведення кампанії (не покладаючись на штучно або вузько визначені періоди звітності, які виключають більшу частину часу, який реально триває кампанія), коли ризик іноземного втручання, ймовірно, є найбільш значним. Виявлення розбіжностей між доходами та витратами може допомогти виявити незаконні джерела фінансування.

Іншою проблемою контролю за іноземним втручанням у вибори є використання третіх сторін для проведення через них витрат на кампанії — цю практику все ще не обмежено у 97 країнах.[109] Реклама у соціальних мережах представляє собою значну лазівку: 133 країни не встановлюють обмежень на вартість рекламу кампаній в Інтернеті, а 122 не застосовують й інших обмежень. Тому для обмеження іноземного

впливу потрібно посилити регулювання політичної реклами в Інтернеті, включаючи впровадження більш точних визначень цифрової агітації та суворіших вимог до прозорості.[110]

Міжнародне узгодження

Іншим пріоритетом є посилення регулювання у різних юрисдикціях та просування міжнародних норм і механізмів для підвищення прозорості транснаціональних фінансових потоків. Це надзвичайно важливо, оскільки незаконне політичне фінансування часто здійснюється через «податкові оази» та офшорні структури, щоб приховати його походження. Центральним елементом цих рамок є Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF) та її стандарти протидії відмиванню грошей, зокрема ті, що стосуються політично значущих осіб (PEP) та офшорних юрисдикцій.[111]

Вирішення питань, пов'язаних з криптовалютами

Протидія гібридним загрозам для виборів також вимагає більш чітких правил щодо використання криптовалют у політичному фінансуванні, враховуючи притаманні їм їхню анонімність та відсутність надійного регулювання. Контроль часто ускладнюється через нечіткість їх правового статусу (чи вони вважаються активами, цінними паперами або фіатною валютою?) і, в зв'язку з цим, через різні правові режими стосовно грошових внесків та внесків у натуральній формі. У більшості систем криптовалюти вважаються активами і тому розглядаються як внески у натуральній формі; однак це не завжди так, що ускладнює для контролюючих органів визначення застосовного правового режиму та їх відстеження.[112]

У якості реакції деякі країни обмежили або цілком заборонили використання криптовалют у політичному фінансуванні, що узгоджується із ширшими обмеженням на іноземні та анонімні пожертви. Наприклад, Ірландія ухвалила у 2022 році закон, що забороняє пожертви у криптовалютах партіям.[113] Такі заходи особливо актуальні для тих криптовалют, які за своєю суттю є анонімними — до них належать деякі з найпопулярніших.[114] Інший (опосередкований) спосіб обмежити використання криптовалют і зменшити пов'язані з ними ризики у політичному фінансуванні — це вимога проведення пожертв через банківську систему, як це робиться у 82 країнах.[115]

Покращення державного нагляду

Більш важливим, ніж посилення регулюючих норм, є забезпечення дотримання вже існуючих норм. Проте нагляд залишається найслабшою ланкою, оскільки діяльність відповідних органів часто ускладнюється нечіткими повноваженнями, обмеженими можливостями та слабкою координацією. Це особливо важливо у контексті необхідної співпраці між виборчими органами та підрозділами фінансової розвідки, враховуючи привілейований доступ останніх до ключової інформації, яка потрібна для моніторингу потоків фінансування політичних партій.[116]

«Більш важливим, ніж посилення регулюючих норм, є забезпечення дотримання вже існуючих норм»

Більш потужні можливості та співпраця є життєво важливими для органів нагляду, які контролюють операції з криптовалютами, зокрема це стосується співпраці з віртуальними «обмінниками» валют. Як фінансові посередники, ці суб'єкти здатні надавати ключову інформацію для виявлення іноземних донорів, а в деяких

юрисдикціях на них вже розповсюджуються правила протидії відмиванню грошей.[117] Так само важливим є надання органам нагляду ширших можливостей з моніторингу витрат на інтернет-рекламу.[118]

Важливо відзначити, що відносини між державним і недержавним наглядом є взаємопідсилюючими. Коли органи влади публікують інформацію без затримок та надають доступ до неї, громадянське суспільство може краще перевіряти звітність про витрати у порівнянні з власним моніторингом.[119] Хоча такі звіти публікує більшість країн (116), розкриття осіб донорів обов'язкове у меншій їх кількості (98). Водночас останнє є критичною складовою для викриття іноземних суб'єктів, котрі прагнуть вплинути на вибори через фінансування партій або кандидатів.[120]

Посилення громадянського суспільства та моніторинг ЗМІ

Громадянське суспільство, журналісти та викривачі («whistleblowers») відіграють важливу роль у викритті незаконного політичного фінансування, особливо коли воно пов'язане з іноземними зловмисними суб'єктами, які прагнуть вплинути на вибори. Проте свобода та дотримання етичних принципів медіа погіршилися за останні роки — Інститут з різноманітності демократій (V-Dem) повідомив про посилення цензури в 44 країнах у 2024 році та про зростання загроз для журналістів.[121] Та сама тенденція явно спостерігається в Європі, де погіршенню сприяють цифрове стеження, дезінформація та політичний вплив на суспільні медіа.[122]

Якщо дивитися більш широко, суб'єкти громадянського суспільства стикаються з низкою викликів, включаючи обмежений доступ до інформації та ресурсів, політичний тиск і обмеження простору громадянської активності. Ці фактори стримують їхню здатність ефективно виконувати роль наглядового органу.[123] Це підкреслює потребу як у стабільній прозорості з боку органів влади, так і у захисті незалежного нагляду, гарантіях доступу до інформації, заходах проти SLAPP (судових позовів з метою залякування), у справедливому доступі до державних ринків реклами та безпечних каналах доступу для дослідників.[124]

Важливо також зазначити, що й самі ЗМІ можуть бути об'єктом іноземного втручання (див. розділ 3 про маніпуляції і втручання FIMI та вибори). У таких випадках ЗМІ можуть не лише не виконувати свою наглядову функцію щодо незаконного фінансування політичної діяльності, але й ставати каналами для поширення хибної інформації та дезінформації.[125]

04 Кібербезпека на виборах

Цифрова сфера залишається дуже критичним вектором втручання у вибори, в якому відбувається запекла боротьба. Кібероперації рідко відбуваються як ізольовані події; натомість вони часто інтегруються у ширші кампанії гібридних загроз, де регулярно слугують основним інструментом для маніпуляцій інформацією та психологічних операцій. Загрози можна умовно розділити на такі, що спрямовані на основну виборчу інфраструктуру, і такі, що спрямовані на кампанії, партії та посадовців, які беруть участь у виборчому процесі.

Період з 2024 року відзначився двома трансформаційними тенденціями: зближенням операцій, спонсорованих державами, із екосистемою кіберзлочинності та виходом ШІ у роль потужного мультиплікатора сил для зловмисників.[126] Це зближення спричинило зростання складності та взаємозв'язку загроз, розмиваючи межі між шпигунством, дестабілізацією та злочинністю із грошовими мотивами, що зумовлює потребу в безперервному зміцненні кібербезпеки.[127]

4.1. ЕВОЛЮЦІЯ ЛАНДШАФТУ ЗАГРОЗ: КОНВЕРГЕНЦІЯ, КОМЕРЦІАЛІЗАЦІЯ ТА ШІ

Зміни на макрорівні у середовищі кіберзагроз визначають поточні виклики для безпеки виборів. Щоб пояснити підвалинну динаміку, яка робить зловмисників більш здібними, здатними адаптуватися та стійкими до протидії, аналіз має вийти за межі простої каталогізації загроз.

Екосистема «кіберзлочинності як послуги» (CaaS): стратегічний симбіоз

Традиційне розрізнення між розвиненими стійкими загрозами («Advanced Persistent Threats», APT), що підтримуються державами, та кіберзлочинцями з фінансовою мотивацією звужується, хоча різниця й не зникає повністю. Протягом багатьох занепокоєння викликало політичне використання кібератак, пов'язаних із організованою злочинністю, наприклад, коли під час скандалів розкривалося створення мереж для шпигунства за журналістами.[128] Нещодавнє дослідження Європолу додатково підкреслює розмиття межі між операціями, що проводяться за підтримки держав, і організованою злочинністю у випадках, коли злочинні угрупування залучаються задля їхніх технічних навичок та інфраструктури.[129]

Це призвело до виникнення професійного ринку кіберзлочинності як послуги («Cybercrime-as-a-Service», CaaS), який сприяє суб'єктам із державних орбіт, надаючи їм спеціалізовані компетенції та додатковий шар правдоподібної непричетності.[130] Ці послуги все частіше використовуються в геополітично вмотивованих кампаніях, що дозволяє державним суб'єктам розширювати свої можливості, проводити руйнівні атаки та брати участь у складних інформаційних операціях.[131]

Що насправді змінюється? Ця конвергенція відбиває дві взаємопов'язані динаміки:[132]

- Аутсорсинг для імітації непричетності: держави ставлять злочинним та проксі-операторам задачі, дають їм змогу вести діяльність або толерують таку діяльність, щоб створювати додаткові шари відокремлення та ускладнювати встановлення джерел.

- Зумовлене ринком розсіювання можливостей: злочинні екосистеми тепер пропонують інструменти рівня APT (розвинених стійких загроз) за моделлю «як послуга» («as-a-service»), що знижує витрати та прискорює операції, не змінюючи основних стратегічних цілей держав.

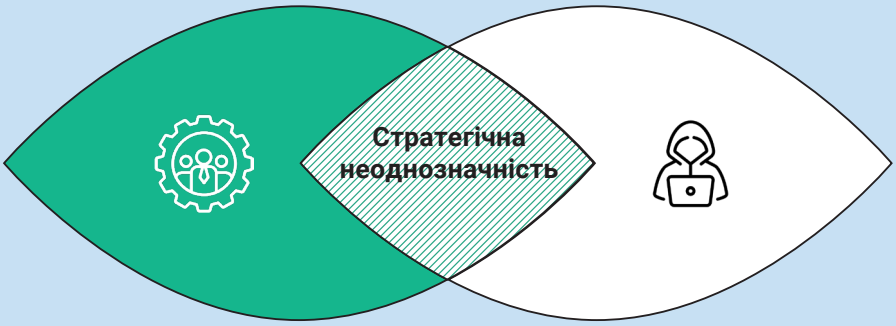
По суті, це менше догматична зміна намірів держав, а більше еволюція операційних методик, котра розширює асортимент варіантів для імітації непричетності та збільшення пікових потужностей.[133]

Державні суб'єкти, зокрема Росія, Китай та Іран, постійно визначаються основними іноземними загрозами для критичної інфраструктури, включаючи виборчі системи.[134] Тепер вони можуть залучати потенціал цієї екосистеми CaaS із суттєвим ефектом. Наприклад, у липні та серпні 2024 року, під час виборчого циклу в США, ReliaQuest — компанія з кібербезпеки, що спеціалізується на виявленні загроз та реагуванні на інциденти — розслідувала скоординовану фішингову кампанію, організатори якої видавали себе за групу активістів. У листах адресатам-мішеням пропонувалося «підписати петицію», після чого вони перенаправлялися на інфраструктуру, пов'язану з конкретною родиною шкідливого ПЗ. Мета полягала у тому, щоб звабити користувача перейти за посиланням, а на скомпрометованих сайтах відбувалася кібератака типу «drive-by», що автоматично ініціювала підробний запит на «оновлення браузера» — в результаті здійснювалися встановлення троянської програми для віддаленого доступу або викрадення облікових даних.[135] Цей випадок ілюструє професіоналізм та «передачу естафетної палички», характерні для даної екосистеми, проте сам по собі не демонструє наявності керування з боку держави.

Цей симбіоз держави та злочинців є навмисною рисою сучасної гібридної війни, що спрямована на ускладнення стримування та встановлення джерел атаки. Коли державний суб'єкт діє через проксі-посередника з кримінального світу, він утворює стратегічну невизначеність. Атака може бути здійснена відомою групою, що оперує програмами-вимагачами («ransomware»), проте спрямована, уможливлена або толерована розвідувальною службою певної держави. Це легко паралізує традиційні механізми реагування. Стає незрозуміло, чи є такий інцидент справою правоохоронних органів, які мають переслідувати злочинне угрупування, чи органів національної безпеки, які займаються стримуванням ворожої держави. Ця неоднозначність надає державі-спонсору можливість заперечувати свою причетність і сповільнює досягнення міжнародного консенсусу, який потрібен для скоординованого реагування, тим самим максимізуючи руйнівний вплив операції.[136]

Політичні наслідки полягають у тому, що у реагуванні мають поєднуватися порогові критерії, засновані на поведінці (які «спрацьовують» в першу чергу за шкодою та індикаторами), а також чіткі стандарти визначення джерел та правові шляхи, котрі забезпечать збереження належної правової процедури, водночас уможливлюючи вчасні захисні дії.

ЗОНА НЕВИЗНАЧЕНОСТІ У ГІБРИДНІЙ ВІЙНІ



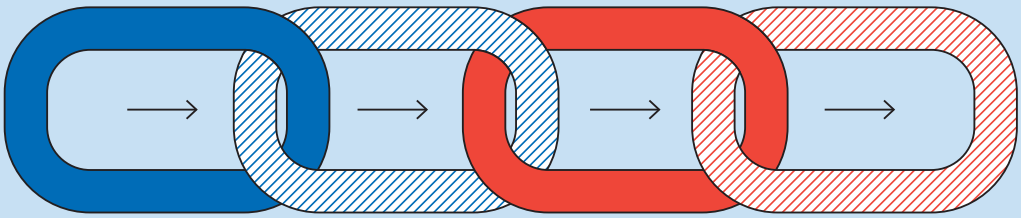
Державні суб'єкти
Керовані урядами операції спецслужб

Злочинні проксі-посередники
Групи-оператори програм-вимагачів та кіберзлочинні угрупування

ШІ як мультиплікатор сил зловмисників: використання для нападу та оборони

За оцінкою Агентства з кібербезпеки та захисту інфраструктури США (CISA), в період 2024–2025 років генеративний ШІ не створив цілком нових категорій ризиків, але значно посилив існуючі.[137] Проте штучний інтелект наразі використовується для збільшення масштабів, швидкості та витонченості атак соціальної інженерії. Це включає створення більш витончених фішингових електронних листів, котрі враховують контекст, створення високореалістичних підроблених зображень і відео з використанням технології діпфейків, а також створення підроблених профілів у соціальних мережах для підтримки операцій впливу.[138]

ЛАНЦЮЖОК АТАКИ ЗА ДОПОМОГОЮ ШІ



ШІ підвищує якість принад
ШІ вдосконалює фішингові принади за допомогою NLP (обробки природних мов) та персоналізованого контенту

Крадіжка облікових даних
Жертви вводять облікові дані на підроблених сторінках входу

Бічний зсув
Нападники переміщуються по мережі, використовуючи викрадені облікові дані

Витік даних/ порушення діяльності
Нападники викрадають дані або порушують операційну діяльність

Водночас багато тих самих методів ШІ застосовуються в цілях оборони, як-от для виявлення аномалій, сортування та автоматичного маркування фішингових повідомлень — це підкреслює той факт, що сама по собі технологія не є проблемою.

Натомість проблема полягає в якості впровадження, управління та в еволюції «гонки озброєнь» між її наступальним і оборонним використаннями.

Широко відомий експеримент, який проводився компанією з кібербезпеки Hoxhunt з 2023 по 2025 рік, емпірично продемонстрував цю еволюцію. На початку 2025 року фішинговий агент на основі ШІ цієї компанії став на 24 відсотки більш ефективним у обмані користувачів, ніж елітні «червоні команди», що складалися з людей, тобто уповноважені тестувальники, які імітували справжніх зловмисників для виявлення слабких місць.[139] Хоча результати можуть відрізнятися у залежності від конкретної організації та рівня базової підготовки, це свідчить про те, що ШІ тепер здатен створювати високоефективні атаки адресного фішингу («spear-phishing») у великих масштабах, що на практиці знижує бар'єри доступу до можливостей, які раніше були доступні лише найбільш передовим супротивникам.

Дослідження на прикладах із 2024 року вже продемонстрували використання діпфейкових аудіо- та відеофайлів у масштабних фінансових шахрайствах, включаючи інцидент, у якому компанія втратила 25 мільйонів доларів США — це демонструє зрілість для використання у цілях обману технології, яку також можна перепрофілювати або адаптувати у політичних цілях.[140] Тим не менш, окремі випадки із великими втратами не слід надмірно узагальнювати на всі виборчі контексти.

Цей технологічний зсув має ґрунтовні наслідки для безпеки виборів, оскільки він ефективно знижує «вхідний бар'єр» для проведення складних атак. Тепер менш кваліфіковані зловмисники можуть створювати дуже переконливий, персоналізований вміст для адресного фішингу, хоча раніше це було прерогативою добре забезпечених ресурсами APT-груп. Такий розвиток подій збільшує як обсяг, так і загальну якість загроз. Класичні ознаки фішингових електронних листів, як-от погана граматика або універсальні привітання, тепер часто видаляються за допомогою ШІ.

Внаслідок цього захист, орієнтований на людей, як-от навчання обізнаності користувачів, хоч і залишається необхідним, але стає значно складнішим та менш надійним. Для команд з кібербезпеки та персоналу, що займається повсякденним забезпеченням виборів, проблема ще збільшується, оскільки величезні обсяги та якість потенційних зламів збільшують ймовірність успішної атаки.

Це потребує змін в оборонній стратегії у бік багаторівневих технічних засобів контролю, які менше покладаються на людське судження і більше — на інфраструктуру з нульовою довірою, де кожен користувач і пристрій перевіряються постійно, підтримуваних сильними технічними засобами захисту. До них належать стійка до фішингу багатофакторна аутентифікація, доступ з мінімальними привілеями та умовний доступ, які надають користувачам лише мінімальні необхідні права доступу й лише за певних умов.

Вони також включають керування згодою OAuth, тобто ретельне управління тим, які із зовнішніх програм підключатися до центральних систем, а також ізоляцію вкладених файлів і посилань, коли потенційно ризикований вміст відкривається у безпечних карантинних середовищах. Ведення списків дозволених програм — це ще один необхідний захід, який дозволяє запуск лише схваленого програмного забезпечення, як і блокування макросів, котре вимикає автоматизований код у документах.

Інші заходи включають забезпечення відповідності пристроїв вимогам та атестацію (гарантує, що усі пристрої, які підключаються, відповідають стандартам безпеки), а також адміністрування за потребою («just-in-time»), яке надає права адміністратора лише на короткий період, поки в цьому існує потреба, та розважливе фізичне відокремлення критичних процесів, щоб найбільш чутливі системи залишалися від'єднаними або працювали у відокремлених мережах. Коли це можливо, ці заходи слід поєднувати з уніфікованим і спрощеним повідомленням про інциденти та чіткими протоколами комунікації для обмеження подальших наслідків у інформаційній сфері.[141]

4.2. ЗАГРОЗИ КРИТИЧНІЙ ВИБОРЧІЙ ІНФРАСТРУКТУРІ (МЕРЕЖАМ, БАЗАМ ДАНИХ І ТЕХНОЛОГІЯМ ГОЛОСУВАННЯ)

Технічна інфраструктура виборів (яка включає все від баз даних-реєстрів виборців до офіційних веб-сайтів для публікації результатів) залишається ключовою мішенню зловмисників. Хоча безпосереднє втручання у роботу машин для голосування з метою зміни кількості голосів зазвичай вважається складним для непомітної реалізації у великих масштабах, особливо в системах із надійним паперовим контрольним журналом, інфраструктура, що їх оточує, має численні вразливості.[142]

За останні роки одна з найпоширеніших тактик, що спостерігалася — це атаки типу «розподілена відмова в обслуговуванні» (DDoS). Вони розраховані на перевантаження веб-сайтів виборів та інформаційних порталів для виборців стороннім трафіком, внаслідок чого ресурси стають недоступними. Іншою суттєвою загрозою є атаки з використанням програм-вимагачів. Ці атаки, які шифрують критичні системи та вимагають виплати за їх розблокування, можуть спричинити серйозні порушення.[143]

Злами виборчих систем

Злами виборчих баз даних становлять особливо підступну загрозу, оскільки вони можуть не порушувати роботу служб одразу, проте підривати довіру громадськості. Будь-який злам, справжній чи уявний, може бути перетворений на інформаційну зброю в кампаніях маніпулювання FIMI для підриву довіри громадськості до виборчого процесу.[144] У 2023 році стало відомо, що відбувся злам Виборчої комісії Великої Британії, ймовірно, пов'язаним з державою суб'єктом, що призвело до компрометації даних 40 мільйонів виборців. Атака, яку у 2024 році приписали групі, пов'язаній з Китаєм, протягом багатьох місяців залишалася непоміченою. Хоча чиновники заявили, що вона не вплинула на голосування чи підрахунок голосів, оприлюднення такого величезного реєстру виборців підкреслює цінність розвідувальних матеріалів, які супротивники вбачають у виборчих даних.[145]

Сумнозвісний випадок також стався під час президентських виборів в Україні у 2014 році. Російські хакери проникли в мережу Центральної виборчої комісії та розмістили підроблені результати голосування, які показували перемогу маргінального націоналіста; хоча українські підрозділи кібербезпеки без затримки нейтралізували шкідливе ПЗ, російські державні ЗМІ все одно транслювали «новини» про його нібито перемогу, щоб ввести громадськість в оману.[146] Цей інцидент підкреслює, що навіть зірваною кібератакою можна скористатися в інформаційній війні, щоб піддати сумніву законні результати.

У зонах конфлікту та регіонах з високою напруженістю кіберзагрози для інфраструктури часто супроводжують фізичні операції та операції з маніпуляції і впливу FIMI. Виборча інфраструктура України зазнавала неодноразових атак з 2014 року в рамках гібридної війни з боку Росії. Окрім випадку 2014 року, виборчі ІТ-системи в Україні постійно піддавалися «розвідці боєм»; чиновники повідомляли про хвилі фішингу атак та атак шкідливого ПЗ на персонал виборчих комісій напередодні виборів 2019 року.[147] Відкрита війна, що триває з 2022 року, ще більше посилила занепокоєння: будь-які майбутні вибори в Україні (наразі вони призупинені на час воєнного стану), ймовірно, відбудуться на тлі надзвичайно високого рівня кіберзагроз, включно з можливістю атак, що порушують роботу енергомереж або мереж зв'язку під час голосування.[148]

Висновки, отримані на досвіді України та інших держав на передовій лінії конфлікту полягають в тому, що захист виборчої інфраструктури — це не просто технічна операція, а нагальна потреба національної безпеки, котра вимагає планування стійкості на випадок найгірших сценаріїв, включаючи умови воєнного часу.

«Виборчі системи є центром тяжіння для оперативних та інформаційних загроз. Супротивнику не обов'язково змінювати хоча б один голос, щоб досягти стратегічної перемоги»

Виборчі системи є центром тяжіння оперативних та інформаційних загроз. Супротивнику не обов'язково змінювати хоча б один голос, щоб досягти стратегічної перемоги. Успішним зламом бази даних виборців зловмисник може досягти двох цілей одночасно. По-перше, він порушить виборчий процес, заважаючи посадовим особам перевіряти виборців та ефективно керувати процесом. По-друге, і що більш важливо, він створить потужні, автентичні «докази», якими можна скористатися для підживлення кампаній маніпуляції FIMI, спрямованих на підрив довіри до легітимності виборів. Це обґрунтовано робить такі бази даних найціннішою мішенню для суб'єкта гібридних атак, адже їх компрометація слугує одразу декільком стратегічним цілям.

Довготривала вразливість баз даних реєстрації виборців

Системи реєстрації виборців є основною мішенню для кібератак і зламів. У минулому атаки з використанням програм-вимагачів безпосередньо впливали на адміністрування виборів, коли вони були спрямовані на ці системи. У 2024 році в США внаслідок інциденту округ був змушений розірвати своє підключення до системи реєстрації виборців штату в якості запобіжного заходу.[149] Подібним чином наприкінці 2024 року атака програм-вимагачів, пов'язаних з Росією, на секретаріат округу Джефферсон в штаті Кентуккі, хоча й не поставила під загрозу саму систему голосування, порушила функціонування та висвітлила вразливість взаємопов'язаних урядових систем.[150]

Бази даних реєстрації виборців визначають, хто і де може голосувати. Якщо зловмисники порушать доступ до них (за допомогою програм-вимагачів або атаки типу «відмова в обслуговуванні») або потайки змінять записи, такі як адреси чи прапорці проходження ідентифікації, ймовірні наслідки включатимуть довші черги, більше використання умовних бюлетенів (для осіб, які відсутні у списках виборців відповідної

дільниці), потрапляння виборців на неправильні виборчі дільниці та суперечки щодо права голосування — навіть якщо власне підрахунок голосів не постраждає.

Мотивація для нападників потроюється — це, по-перше, доступність, адже кібератака може блокувати реєстрацію виборців або порушувати синхронізацію електронного журналу виборців («e-pollbook», загального списку виборців для дільниць та центральних систем, який унеможливлює подвійне голосування); по-друге, цілісність — редагування або видалення записів можуть утворювати суперечки або вибіркове позбавлення громадянських прав; і, нарешті, конфіденційність, яка вразлива до крадіжки персональних даних з метою залякування або адресного фішингу («spear-phishing»). Викрадені облікові дані також можуть використовуватися для переведення напрямку атаки на інші виборчі системи.

Широко розповсюдженою проблемою є крадіжка даних виборців. За оцінками, викрадені з облікових записів у штатах США дані становлять приблизно 78 відсотків усіх даних виборців, що циркулюють у темній мережі («dark web»), причому злами відбувалися щонайменше у 23 штатах. Ця розкрита інформація потім використовується в атаках — для цілеспрямованої дезінформації, у тактиках створення штучних перешкод для виборців, а також для маніпуляцій з ідентифікаційною інформацією; вона дає змогу надсилати оманливі повідомлення про місця проведення голосування або навіть спробувати організувати шахрайське голосування.[151]

Подвійна загроза програм-вимагачів та атак DDoS

Атаки типу «розподілена відмова в обслуговуванні» («DDoS») надалі залишаються поширеною тактикою для порушення доступу до веб-сайтів, пов'язаних із виборами, в тому числі порталів з інформацією для виборців та сайтів, де оприлюднюються результати виборів.[152] У виборчому циклі 2024 року в США спостерігалося значне збільшення кількості таких атак, спрямованих на веб-сайти кампаній, політичні партії та інфраструктуру на рівні округів. Компанія з кібербезпеки Cloudflare повідомляла, що за перші шість днів листопада 2024 року вона заблокувала понад 6 мільярдів зловмисних запитів, спрямованих на пов'язані з виборами у США ресурси, причому деякі атаки досягали пікової інтенсивності в 700 000 запитів на секунду.[153] Подібні політично вмотивовані DDoS-кампанії спостерігалися під час виборів до Європейського парламенту 2024 року, коли сайти голландських політичних партій були виведені з ладу.[154]

Стратегічна мета цих атак часто виходить за межі технічного порушення функціонування. Як відкрито зазначали Агентство з кібербезпеки та захисту інфраструктури (CISA) та Федеральне бюро розслідувань США, хоча атаки типу DDoS навряд чи завадять будь-якому виборцю віддати свій голос, вони можуть ефективно перешкоджати громадському доступу до офіційної інформації та створювати враження хаосу і некомпетентності.[155] Цим враженням, в свою чергу, буде легко скористатися у кампаніях з дезінформації, котрі можуть посилювати сприйняття інциденту, щоб підірвати довіру громадськості до загальної чесності виборів і, внаслідок цього, до демократичних принципів, цінностей та процесів.[156]

Подібним чином, атаки програм-вимагачів на місцеві органи влади, навіть якщо вони не спрямовані безпосередньо на виборчі комісії, можуть спричинити значні супутні втрати. У другому кварталі 2024 року зареєстровано зростання кількості інцидентів з атаками програмам-вимагачів на державні, регіональні, племінні та територіальні органи влади. Ці атаки можуть перешкоджати діяльності співробітників виборчих комісій, які залежні від функціонування спільної IT-інфраструктури округу.[157] Інциденти — це не просто технічні проблеми; вони є інструментами операцій з інформаційного впливу. Їхня основна мета — це не сервер, а громадська думка. Успіх зловмисника вимірюється не кількістю виведених з ладу серверів, а кількістю написаних про це новин і публікацій у соціальних мережах, які поширюють наративи про «зламані вибори». Це робить реагування зі стратегічної комунікації у відповідь на подібні інциденти таким же важливим, як і технічне реагування.

Компрометація ланцюжка постачання виборчих технологій

Безпека виборчих технологій значною мірою залежить від складного ланцюжка постачання програмного забезпечення, який став основною мішенню для кваліфікованих зловмисників.[158] У даному контексті частота атак на ланцюжок постачання програмного забезпечення продовжує зростати; з кінця 2024 року до середини 2025 року кількість інцидентів зросла на 25%.[159]

Характер цих загроз значно еволюціонував. Окрім класичної вставки шкідливого коду в оновлення програмного забезпечення, або «підробки пакетів», у звіті за 2025 рік підкреслюється більш підступна, прихована тенденція: на 12% збільшилася кількість розкриттів секретних даних розробників (як-от жорстко закодованих паролів, маркерів і ключів доступу API, що використовуються для автентифікації між службами), вбудованих у комерційні продукти.[160] Розглядаючи ці закономірності у сукупності, можна зробити висновок, що зловмисники націлюються на весь життєвий цикл розробки програмного забезпечення, а не лише на кінцевий продукт. Водночас широке застосування програмного забезпечення з відкритим вихідним кодом і поширення інструментів розробки на базі ШІ збільшили поверхню складних атак, якими можна скористатися.[161]

Резонансні випадки зламів великих постачальників програмного забезпечення та послуг демонструють каскадний вплив на третіх сторін компрометації одного ланцюжка постачання — він може зачепити тисячі клієнтів нижчих рівнів.[162] Ці випадки грають роль попередження для сектору виборчих технологій, котрий покладається на подібні компоненти та послуги третіх сторін. В контексті систем голосування це означає, що ризики поширюються через спільних постачальників і компоненти. Загроза зсунулася від простого «зараження продукту» до систематичного «компрометування процесу». Викрадаючи облікові дані розробників або використовуючи вразливу архітектуру, зловмисник може отримати постійний доступ та ряд напрямків для здійснення атак у майбутньому.

Іншими словами, це більш стратегічний, довгостроковий компроміс, який покладає значну відповідальність на відповідальних за вибори осіб під час процесу закупівель. Вони більше не можуть просто довірятися сертифікації постачальника; їм також потрібно ретельно вивчати практики розробки постачальника, продукт якого має бути безпечним за архітектурою та концепцією («secure-by-design» — безпека за задумом). Таким чином, критична вразливість може знаходитися не у коді, безпосередньо пов'язаному з виборами, а у сторонній бібліотеці, від якої він залежить, що робить виявлення та усунення вразливостей значно проблематичнішим.

4.3. КІБЕРАТАКИ, СПРЯМОВАНІ НА КАМПАНІЇ, ПАРТІЇ ТА ВІДПОВІДАЛЬНИХ ЗА ВИБОРИ ПОСАДОВЦІВ

Політичні кампанії, партії та посадові особи є основними цілями кібератак, спрямованих на вплив на вибори.[163] Найефективнішою тактикою є операція «злам та витік», коли викрадені матеріали, як-от електронні листи та документи, стратегічно публікуються в Інтернеті, щоб підживлювати дезінформацію та завдати максимальної політичної шкоди.[164] Ця схема дій використовувалася багаторазово, від російських операцій на виборах у США у 2016 році та у Франції у 2017 році до зламу під час президентської кампанії у США в 2024 році хакерами, пов'язаними з Іраном. Ці атаки часто ініціюються через адресний фішинг («spear-phishing»), який включає надсилання електронних листів, великою мірою адаптованих під конкретного отримувача, щоб ошукати його і змусити розкрити свої облікові дані.[165]

Зростає вагомість нової загрози — клонування голосу за допомогою ШІ, також відоме як «вішинг» («vishing»), коли зловмисник користується ШІ, щоб видавати свій голос за голос довіреної особи по телефону; ця тактика, як попереджає CISA, може застосовуватись для видавання себе за високопоставлених посадовців виборчих комісій.[166]

Посадовці виборчих комісій також стикаються зі шквалом загроз, в тому числі фішингом та доксингом («doxxing» — зловмисна публікація персональної інформації) з боку як іноземних, так і вітчизняних суб'єктів, які прагнуть їх залякати або викрасти їхні облікові дані.[167] Ці інструменти неспівмірно активно використовуються проти жінок у політиці та журналістиці для переслідувань та створення діпфейк-порнографії без згоди зображених у ній осіб.[168]

Такий розвиток ситуації означає, що організаторам кампаній, партіям та посадовим особам слід очікувати, що вони безперервно будуть цілями атак протягом усього виборчого циклу, та планувати запобігання крадіжкам облікових даних і спробам атак типу «злам та витік» («hack-and-leak»). Коли розвідка повідомляє про неминучий витік, обачне сповіщення про його джерело «на випередження» може пом'якшити вплив. Оскільки ШІ підвищує якість принад та дає змогу імітувати голоси, державним органам необхідно заборонити схвалення рішень лише по голосовому зв'язку і вимагати зворотного виклику або підтвердження через інший канал. Також потрібно захищати людей і системи, щоб забезпечити юридичні шляхи захисту та процеси підтримки для жінок, яких атакують за допомогою гендерно-орієнтованих діпфейків, та захищати посадових осіб від доксінгу та переслідування.[169]

4.4. ЩО МОЖНА ЗРОБИТИ? ВЗІРЦЕВІ ПРАКТИКИ ЗІ СТІЙКОСТІ КІБЕРБЕЗПЕКИ ВИБОРІВ

Ефективний захист від сучасних кібер- та інформаційних загроз вимагає безперервного, адаптивного та заснованого на співпраці підходу.[170] Досягнуто широкого консенсусу щодо набору взірцевих практик, які становлять основу стійкості виборів у контексті кібербезпеки.[171] У сукупності ці шари перетворюють технічну стійкість на легітимність виборів. Принципи управління та безпеки за архітектурою і концепцією («secure-by-design») зменшують ймовірність помилок та усувають окремі точки відмови; проактивні операції та відпрацьовані сценарії реагування мінімізують час перебування нападників у системах та помітність порушень роботи, усуваючи періоди «інформаційної порожнечі»; а безперервні партнерські відносини забезпечують вартий довіри зв'язок між багатьма агентствами і установами та незалежну перевірку.

Результатом є безперервність надання послуг, яка гарантує, що громадяни матимуть можливість проголосувати, у поєднанні з доказами чесності, які гарантують, що громадськість розумітиме, що сталося і чому. Ці три умови підтримують як суб'єктивну (в особистому сприйнятті), так і фактичну легітимність виборів.

Фундаментальне управління та технології

Стійкість починається зі всебічної оцінки ризиків для всієї електоральної екосистеми — від реєстрації виборців до звітування про результати.[172] Базуючись на цій основі, виборчі органи повинні прийняти та впровадити технології, які є безпечними за своєю архітектурою та концепцією, вимагаючи від постачальників вбудовувати безпеку протягом усього життєвого циклу розробки програмного забезпечення.[173] На практиці це все частіше включає впровадження архітектури «нульової довіри» («Zero Trust»), яка виключає презумптивну довіру та безперервно перевіряє кожного користувача, пристрій та робоче навантаження, підключені до критичних систем.[174] Такі фундаментальні вибори зменшують кількість одиничних точок відмови та роблять подальші заходи з контролю більш ефективними.

Проактивні операції та реагування

Захисна стратегія має бути проактивною. Це означає: постійне зміцнення систем за допомогою технічних заходів контролю, таких як багатофакторна автентифікація та сегментація мереж; моніторинг загроз за допомогою систем виявлення вторгнень (IDS) і активний пошук раніше розміщеного шкідливого ПЗ задовго до виборів.[175] Не менш важливо мати добре відпрацьовані плани реагування на інциденти, які поєднуватимуть технічне стримування зі стратегічними комунікаціями, запобігаючи переростанню операційних проблем у кризи легітимності.[176] Така операційна дисципліна перетворить технічну стійкість на довіру громадськості.

Тривалі партнерські відносини

У кінцевому підсумку ефективний захист неможливо забезпечити в ізоляції. Стійкість залежить від наявності безперервних, постійних партнерських відносин та організації надійних мереж співробітництва у сфері виборів. Ці структури формалізують співпрацю між органами, що керують виборами (EMB), агентствами з кібербезпеки, розвідувальними службами та правоохоронними органами, утворюючи спільну обізнаність, необхідну для швидкого, скоординованого реагування на нові загрози.[177] Поєднуючи прогресивне управління, операційну діяльність та партнерства, органи влади можуть раніше виявляти загрози, швидше реагувати на них та комунікувати більш переконливо, тим самим зміцнюючи як суб'єктивну (сприйману), так і фактичну легітимність виборів.

05 Протидія гібридним загрозам для виборів: аргументи на користь створення мереж виборчої співпраці

Багатоплановий характер гібридних загроз та велика кількість причетних сторін роблять традиційні, ізольовані заходи з безпеки недостатніми. Супротивники навмисно користуються перекриванням обов'язків агентств (наприклад, під час виборів), атакуючи кіберінфраструктуру, інформаційне середовище та фізичну безпеку одночасно. Орган, що керує виборами, може бути підготовленим до логістичних викликів, агентство з кібербезпеки — до кібератак, а правоохоронне агентство — до загроз для фізичної безпеки, проте жоден з них окремо не може впоратися з синхронізованою атакою, яка поєднує всі три вектори.[178] Зловмисники усвідомлюють ці інституційні розбіжності та розробляють свої операції так, щоб скористатися ними, створюючи стратегічний виклик, який можна подолати лише за допомогою дзеркально інтегрованого та мережевого захисту.[179] Тому ефективний захист вимагає фундаментального зсуву в напрямку створення надійних, постійних мереж співпраці стосовно виборчих процесів як на національному, так і на міжнародному рівнях.[180]

Ці мережі є необхідними для інституціоналізації співробітництва, щоб вийти за межі ситуативного кризового менеджменту і перейти до побудови проактивної та стійкої захисної позиції. Основна мета цих мереж полягає у виробленні спільної картини оперативної ситуації для всіх ключових суб'єктів, що сприяє швидкому, скоординованому виявленню нових загроз та реагуванню на них. Комплексна платформа протидії гібридним загрозам для виборів, розроблена Європейським центром з протидії гібридним загрозам (Hybrid CoE), визначає ключові функції, на яких ці мережі повинні зосередитися, в тому числі оновлення законодавства, проведення оцінок вразливості, підвищення стійкості, покращення комунікації, проведення спільних навчань та посилення можливостей виявлення та реагування.[181]

Цей проактивний, мережевий підхід узгоджується з офіційними рекомендаціями на європейському рівні. Європейська Комісія прямо рекомендувала державам-членам створити національні мережі співпраці у сфері виборів, визнавши їх критично важливими платформами для співпраці виборчих органів з іншими ключовими суб'єктами безпеки. Така співпраця, як зазначає Комісія, є необхідною для оперативного виявлення загроз та ефективного забезпечення дотримання правил.[182]

Важливий урок, отриманий в результаті нещодавніх зусиль із захисту виборів, полягає у тому, що співпраця під час криз не може бути імпровізованою. Відносини, довіра та

протоколи спільного доступу до інформації повинні бути вибудовані та відпрацьовані заздалегідь, із запасом часу, оскільки ситуативні зусилля груп, утворених під тиском, часто виявляються неефективними. Тому інституціоналізація постійних мереж формалізованої співпраці є не лише взірцевою практикою, а й фундаментальною передумовою для побудови стійкості, котра необхідна для протистояння хронічному тиску сучасних гібридних загроз.[183]

5.1. АРХІТЕКТУРИ НАЦІОНАЛЬНОЇ СПІВПРАЦІ

Хоча принцип кооперативного захисту широко визнається, універсальної моделі мережі виборчої співпраці не існує. Національні структури формуються унікальним устроєм урядування країни та її унікальним сприйняттям загроз, з котрими вона стикається. Наведені нижче приклади узагальнюють основні механізми та сферу застосування кожної моделі.

- **Шведські** децентралізований уряд та культура, заснована на консенсусі, формують багаторівневу мережу, засновану на моделі співпраці. На національному рівні Шведська виборча комісія очолює національну мережу виборчої співпраці, яка доповнюється регіональними та місцевими мережами.[184] Її практичні аспекти включають постійні групи для обміну інформацією, регулярні спільні навчання та чітке розмежування ролей між національним «керівництвом» та муніципальним «виконанням».

- Великою мірою федералізована структура **Сполучених Штатів Америки** диктує потребу в децентралізованій моделі, у якій федеральні агентства координують свою діяльність із 50 незалежно керованими виборчими системами штатів. Координація забезпечується за допомогою добровільних механізмів, таких як Центр обміну інформацією та аналізу виборчої інфраструктури («Elections Infrastructure Information Sharing and Analysis Center», EI-ISAC), спільних програм дій і методичних посібників, а також підтримки у реагуванні на інциденти, а не за рахунок централізованого керування.[185]

- У **Франції**, з її давніми державницькими традиціями, створили спеціальний державний орган, який уповноважений публічно визначати іноземне втручання. Цей орган, Viginum («Service de vigilance et de protection contre les ingérences numériques étrangères» — служба нагляду та захисту від іноземних цифрових втручань), втілює централізовану модель, яка віддає пріоритет слідчим повноваженням, оперативній публікації загальнодоступних сповіщень та загальноурядовій постановці завдань оперативним підрозділам.[186]

- **Канада** розробила модель, керовану розвідувальною інформацією, яка ретельно ізольована від безпосередньо політичної сфери.[187] Ця модель зосереджена на Робочій групі з питань загроз безпеці та розвідки для виборів («Security and Intelligence Threats to Elections Task Force», SITE), яка здійснює комплексну оцінку загроз, і Комісії з публічного протоколу щодо критичних інцидентів, пов'язаних з виборами, яка відповідає за інформування громадськості про достатньо важливі ситуації. Канадське виборче агентство, Elections Canada, не є членом ні Робочої групи, ані Комісії; воно залишається незалежним, проте координує свою діяльність з органами безпеки та отримує від них зведення.[188]

Ці приклади показують, що хоча основні функції співпраці є загальними, її інституційна форма має бути адаптована до національного контексту. Незалежно від своїх конкретних структур, ефективні мережі співпраці у виборчих процесах мають

спільний набір основних операційних функцій і взірцевих практик, які необхідні для успішної діяльності. Ці практики перетворюють захисну стратегію країни з реактивної, керованої подіями, що відбуваються, на проактивну та безперервну. Аналіз різних національних моделей дає змогу сформулювати стандартизований набір методів, яких ці мережі мають дотримуватися, щоб бути ефективними.

Створення спільної картини оперативної ситуації: концепція міжвідомчої групи

Основоположною практикою ефективної співпраці є створення «об'єднаної інформаційної міжвідомчої групи» (т. зв. «Fusion cell»). Ця концепція передбачає сумісне розміщення аналітиків та офіцерів зв'язку з усіх залучених агентств, особисто або віртуально, щоб забезпечити обмін інформацією в режимі реального часу та сприяти спільному розумінню середовища загроз.[189] Руйнуючи кордони між ізольованими сховищами інформації окремих підрозділів, об'єднані міжвідомчі групи — від кіберреагувальників до аналітиків розвідки та стратегічних комунікаторів — можуть синтезувати з численних потоків загроз єдину, цілісну «спільну картину оперативної ситуації».

Щоб досягти балансу між аналітичною інтеграцією та інституційною автономією, об'єднані міжвідомчі групи повинні діяти за принципом: «аналізуємо разом, діємо в межах власних повноважень»: аналіз виконується спільно, тоді як власні оперативні рішення та повноваження залишаються прерогативою кожною з окремих установ. Ця спільна обізнаність є підґрунтям скоординованої відповіді та може бути організована з урахуванням операційної самостійності органів, що керують виборами (ОКВ).[190]

На практиці баланс підтримується за рахунок обмеженого метою обміну даними та доступу на основі ролей, формальних меморандумів про порозуміння, суворого розмежування між аналізом і операційною діяльністю та ведення реєстрів спільного доступу, котрі підлягають аудиту. Рішення полягає в організаційному плануванні, а не у фізичній відстані: міжвідомчі об'єднані групи повинні залишатися суто аналітичними, з обміном інформацією, що обмежується метою і залишає оперативні рішення в межах повноважень кожної з установ — це гарантує, що ОКВ зберігає виключні повноваження стосовно процесів виборів.

У разі реалізації за цією схемою, міжвідомчі об'єднані групи забезпечують відчутні переваги, в тому числі швидше виявлення загроз та їх сортування за пріоритетом («час виявлення»), зменшують дублювання зусиль між установами та посилюють довіру й узгодженість повідомлень у спільному реагуванні.

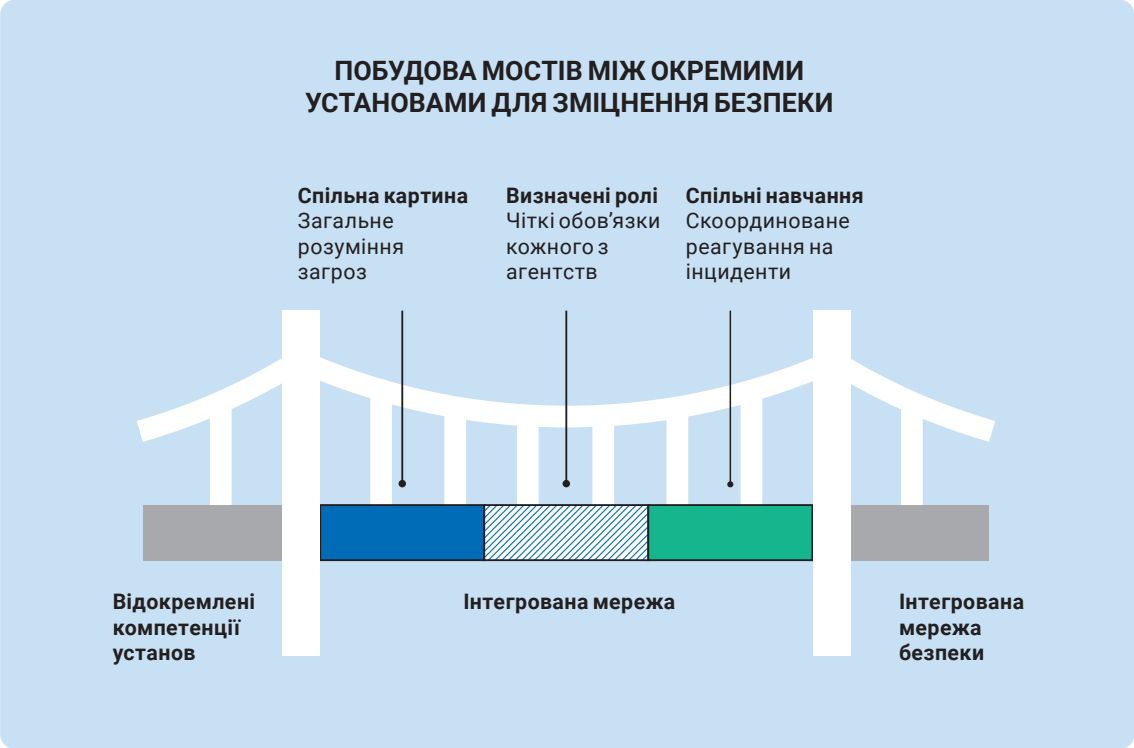
Проактивна, безперервна робота між виборчими циклами

Ефективні мережі працюють безперервно, а не лише у місяці, що передують голосуванню. Основні проактивні заходи включають:

- **Спільні оцінки ризиків і вразливостей:** регулярна та систематична побудова карти виборчої екосистеми для виявлення ризиків та їх ранжування за пріоритетами, перш ніж ними хтось скористається.[191]

- **Планування на основі сценаріїв та спільні навчання:** регулярне проведення штабних (теоретичних) та функціональних навчань для перевірки планів реагування, виявлення прогалин у координації та формування інституційної «м'язової пам'яті».[192] Репрезентативним прикладом можуть слугувати спільні навчання ЄС з кібербезпеки перед парламентськими виборами.[193]

- **Формалізовані протоколи обміну інформацією та реагування:** Встановлення чітких, заздалегідь узгоджених протоколів, які регулюють те, як про загрози повідомляється, як відбувається їх оцінка та реагування на них. Це дає змогу уникнути імпровізації під час кризи та допомагає виключити політику з процесу прийняття рішень.[194]



5.2. МЕРЕЖА МЕРЕЖ

В умовах глобалізованого інформаційного середовища суто національні засоби захисту є недостатніми, тому потрібна «мережа мереж», яка з'єднує національні органи з надійними міжнародними структурами.

Європейський Союз має найскладнішу регіональну екосистему. Його Європейська мережа співпраці у сфері виборів («European Cooperation Network on Elections», ECNE) слугує для національних органів влади центральною точкою з обміну взірцевими практиками з усіх відповідних питань, від кібербезпеки до протидії дезінформації.[195] Вона пов'язана зі спеціалізованими мережами, такими як Система швидкого оповіщення про загрози FIMI («Rapid Alert System»), і підтримується Спільним механізмом виборчої стійкості («Joint Electoral Resilience Mechanism»), який може направляти групи експертів до держав-членів. Ця інтегрована система продемонструвала свою незамінність під час виборів до Європарламенту парламенту у 2024 році, які пройшли без ускладнень.[196]

Ширші рамки співпраці організовуються через альянс НАТО, який визначає гібридні загрози одним з основних викликів для безпеки та працює над покращенням обміну розвідданими між союзниками, а також через Механізм швидкого реагування G7 («Rapid Response Mechanism», RRM), котрий координує реагування на дезінформацію, яка спонсорується іноземними державами.[197] На глобальному рівні міжурядові організації, такі як Міжнародний інститут демократії та сприяння виборам («International IDEA»), відіграють ключову роль у формуванні норм і культивації спільноти практиків через такі ініціативи, як Глобальна мережа захисту чесності виборів («Global Network for Securing Electoral Integrity», GNSEI).[198]

5.3. ПРОБЛЕМИ, ЩО ПЕРЕШКОДЖАЮТЬ ЕФЕКТИВНІЙ СПІВПРАЦІ

Незважаючи на значний прогрес, досягнутий у створенні механізмів колективного захисту, їхня довгострокова ефективність і життєздатність стикаються з глибинними та стійкими викликами. На практиці їх перелік включає політичні зміни та поляризацію, бюджетні обриви, правову невизначеність і повсякденні складнощі з обміном даними та координацією.

Ключовий парадокс стійкості гібридних загроз полягає в тому, що самі ті механізми, які створені для протидії скоординованим інформаційному, кібер- та фінансовому тиску, можуть в свою чергу стати цілями — вразливими до делегітимізації, поляризації та юридичних або бюджетних атак внаслідок маніпуляцій та впливу FIMI, здійснюваних тими самими суб'єктами, протидіяти котрим ці механізми призначені. Простіше кажучи, захисні бар'єри, які ми будуємо, можуть бути ослаблені тими самими силами, котрі вони призначені стримувати.

Ці перешкоди, які охоплюють політичну, фінансову та оперативну сфери, загрожують підірвати саме ті структури, що створені для захисту демократичних процесів. Вирішення цих проблем є критично важливим для побудови стабільної, а не епізодичної стійкості.

> *«Шлях до стабільної, довгострокової стійкості вимагає не лише побудови цих мереж, але й ширших суспільних зусиль задля деполітизації безпеки виборів та її впровадження як ключового, непорушного національного інтересу»*

Таким чином, довгострокова життєздатність залежить від практичної організаційної ізоляції установ — чітких повноважень, міжпартійної підтримки та захищених бюджетів — у поєднанні з широкою політичною підтримкою, яка триватиме довше, ніж термін роботи будь-якого окремо взятого уряду. Шлях до стабільної, довгострокової стійкості вимагає не лише побудови цих мереж, але й ширших суспільних зусиль задля деполітизації безпеки виборів та її впровадження як ключового, непорушного національного інтересу. Вона повинна бути вкорінена у загальному суспільному договорі та громадській довірі, а також втілюватися у реальність через загальносуспільний підхід.

06 Висновки та рекомендації

Період з 2024 року й донині підтвердив, що гібридні загрози становлять стійкий, адаптивний і дедалі складніший виклик для чесності виборів у всьому світі. Аналіз нещодавніх випадків гібридних атак, спрямованих на вибори, підкреслює еволюцію цих загроз — від епізодичних втручань до хронічної, системної форми конфлікту, яка тепер діє як кампанія по всьому спектру. У рамках цих кампаній синхронно відбуваються маніпуляції та вплив FIMI, кібероперації, незаконне політичне фінансування, використання супротивником правових механізмів та фізичний тиск, які скоординовано розподіляються між державними суб'єктами, проксі-посередниками та кримінальними суб'єктами, а час кожної з атак протягом виборчого циклу підбирається для експлуатації меж «на стиках» між компетенціями різних установ.

Аналіз нещодавніх подій підкреслює кілька ключових спостережень:

- **Перехід до хронічного конфлікту:** Втручання у вибори переросло з нерегулярних інцидентів у безперервний інформаційний конфлікт. Державні суб'єкти-зловмисники наполегливо працюють над підривом демократичних систем шляхом підриву довіри громадськості, розпалювання поляризацію та послаблення інститутів.[199]

- **Операції в промисловому масштабі та нові технології:** Зловмисники тепер діють у промисловому масштабі, використовуючи складні, централізовано керовані мережі пропаганди.[200] «Прийом на озброєння» ШІ став значним мультиплікатором сил, який дозволяє швидко та дешево створювати синтетичні медіа-матеріали та надзвичайно реалістичну дезінформацію, що принципово збільшило як обсяг, так і якість загроз.[201]

- **Інтеграція векторів загроз:** Успішні гібридні операції рідко покладаються лише на один метод. Натомість вони інтегрують інформаційні маніпуляції, незаконне політичне фінансування та руйнівні кібератаки в цілісну кампанію. Незаконні кошти — часто проведені крізь криптовалюти та через третіх сторін — підтримують діяльність з інформаційного впливу та підкуп виборців. Водночас кібератаки використовуються для крадіжки даних для операцій «злам і витік» («hack-and-leak») і для порушення виборчих процесів, сіяння плутанини та недовіри.[202]

- **Виявлення, встановлення джерел та підзвітність залишаються вузькими місцями:** Використання проксі-посередників, відмивання інформації та фрагментований доступ до даних перешкоджають своєчасним і пропорційним реакціям. Тим часом нестала прозорість платформ обмежує зовнішній контроль. Прогрес у відкритих стандартах для зазначення походження та доступі до даних для дослідників має поєднуватися з підконтрольними рекламними технологіями та ефективною перевіркою по санкційних списках.[203]

6.1. РЕКОМЕНДАЦІЇ

Ці висновки підкреслюють необхідність побудови та зміцнення мережевої оборони. Оскільки зловмисники цілеспрямовано використовують розриви між повноваженнями різних установ, традиційні ізольовані заходи реагування з безпеки тепер виявляються недостатніми.

Наступні рекомендації адресовані зацікавленим сторонам, відповідальним за захист демократичних процесів. Вони впорядковані навколо чотирьох основних дій, спрямованих на зміцнення стійкості на національному та міжнародному рівнях.

1. **Розвиток внутрішнього потенціалу установ:** Окремі інституції повинні взяти на себе відповідальність за власний захист; він має підтримуватися чіткими повноваженнями та професійно розробленими процедурами.

Це починається з чітко визначених обов'язків стосовно карти ризиків, управління під час інцидентів, інформування громадськості та управління постачальниками, причому все це має бути задокументоване у практичних, зручних для виконання планах. Ці плани мають бути інтегровані у повсякденну практику за допомогою регулярних навчань, які імітують сценарії гібридних загроз; зокрема, це включає відпрацьований набір планів дій з реагування на витоки із заздалегідь затвердженими повідомленнями, а також заходи з ліквідації наслідків після завершення вправи, які мають відстежуватися до завершення.

Технології та процедури повинні відповідати принципам безпечності за архітектурою та концепцією («secure-by-design»), таким як доступ з мінімальними привілеями, безперервна перевірка користувачів і пристроїв, а також створення автономних резервних копій для критично важливих операцій, щоб забезпечити безперервність роботи під навантаженням. Стандарти закупівель повинні вимагати підтвердження безпечних практик розробки, оперативного сповіщення про інциденти та прозорості щодо компонентів від третіх сторін, щоб виключити наявність одиничних точок відмови.

Показники успіху включають швидші виявлення та локалізацію, своєчасне та прозоре інформування громадськості, а також всебічні контрольні журнали, які прояснюють інциденти, не розкриваючи конфіденційної інформації.

2. **Розбудова національної екосистеми підтримки:** Внутрішній потенціал має бути посилений за рахунок надійної загальноурядової мережі, оскільки жоден окремий орган не зможе досягти успіху в ізоляції.

Постійна мережа співпраці має працювати безперервно, рік за роком, зв'язуючи відповідальний за вибори урядовий орган із технічними, регуляторними, безпековими та наглядовими партнерами. Модель малих об'єднаних міжвідомчих груп дає змогу обмінюватися інформацією у реальному часі («аналізуємо разом, діємо в межах власних повноважень»), забезпечуючи спільне розуміння ситуації для всіх сторін при одночасному збереженні операційної самостійності. Спільно використовувана інфраструктура може включати службу підтримки для місцевих органів влади та менших організацій, канали швидкої ескалації для звернення до головних онлайн-

платформ та механізм перевірки підозрілих аудіо- та відеозаписів, який допоможе журналістам і громадськості отримувати доступ до достовірних джерел.

Законне та пропорційне співробітництво має гарантуватися за допомогою письмових протоколів, доступу на основі ролей та прозорих записів про надання доступу до інформації. Такі мережі дають змогу швидше розсилати попередження між установами, скорочують дублювання зусиль і сприяють більш послідовному публічному інформуванню тоді, коли це найважливіше.

3. **Загальносуспільний підхід:** Демократична стійкість залежить від залучення незалежних ЗМІ, громадянського суспільства, академічних кіл, місцевих органів влади, приватного сектора та громад для покращення грамотності, верифікації та інклюзивної публічної комунікації — які мають здійснюватися шляхами, що підтримують права, прозорість та плюралізм.

Прозорість має стати стандартною практикою за допомогою спеціальних, легкодоступних веб-сторінок для кожного з ключових процесів. Використання упереджувальних повідомлень має бути обмеженим і узгоджуватися з виборчим циклом, зосереджуватись на чітких підказках — «чого очікувати, як перевіряти та куди повідомляти?» — і послідовно спрямовувати аудиторію до офіційних джерел.

Довірені місцеві ЗМІ та організації можуть допомогти розширити охоплення, надаючи заготовлені роз'яснення, придатні для повторної публікації. Підтримка незалежних ЗМІ та журналістських розслідувань має бути розширена, але зі збереженням дистанції, щоб захистити редакційну незалежність; також її потрібно доповнити чіткими процедурами для боротьби з переслідуваннями, доксингом та гендерно зумовленими порушеннями прав людини. Під час співпраці з приватними постачальниками має забезпечуватися безпечна перевірка конфіденційних запитів, швидке реагування у разі поширення шкідливого контенту, а також збільшена прозорість стосовно політичної реклами.

У кінцевому підсумку такий підхід сприятиме більшій обізнаності та залученості громадськості, швидшому виправленню неправдивих чуток та ширшому повторному використанню достовірної інформації.

4. **Створення механізмів міжнародного співробітництва та підтримки:** національні системи повинні інтегруватися з транскордонною допомогою, спільними стандартами та сумісними діями, що дасть змогу масштабувати підтримку, якщо атаки перевищать внутрішній потенціал реагування.

Механізми взаємодопомоги мають бути підготовлені заздалегідь і охоплювати технічне реагування, підтримку з експертизи та публічні комунікації протягом виборчих періодів. Практичні канали для видалення контенту за кордоном або пов'язаних з цим дій мають бути організовані із попередньо затвердженими шаблонами, щоб мінімізувати затримки. Стандартні основні плани для захисту систем, пов'язаних з виборами, та для розкриття інцидентів мають бути узгоджені, а базові практики підтвердження походження для офіційних ЗМІ мають бути прийняті там, де це можливо, щоб спростити верифікацію та збільшити прозорість.

Знання слід передавати до початку основних циклів через обміни та прикомандирування персоналу, тоді як мережі співпраці повинні вивчати досвід закордонних, обмінюватися показниками та наборами планів. Результати: швидша допомога тоді, коли це найважливіше, чіткіше інформування через межі між юрисдикціями та сильніші докази, коли на кону стоїть підзвітність — стійкість перетворюється на легітимність як всередині країни, так і для міжнародних партнерів.

Усі контрзаходи повинні мають бути законними, необхідними та пропорційними і базуватися на підході, який враховує права людини. На практиці це означає, що потрібно боротися з маніпулятивною поведінкою, але не з дозволеною законом свободою слова, і надавати пріоритет процесуальним засобам захисту — прозорості, підтвердженню походження та підзвітності — замість видалення вмісту. Це також передбачає впровадження мінімізації збирання та зберігання даних і конфіденційності за архітектурою та концепцією систем; здійснення обмежених у часі та за призначенням дій з незалежним наглядом, веденням документального сліду та реєстрацією аудиту і юридичними можливостями відновлення порушених прав; а також підтримання проактивної прозорості за допомогою взірцевого джерела достовірної інформації, яке дасть змогу громадськості перевіряти твердження.

Ці гарантії відповідають гарантіям доступу до інформації (Конвенція Тромсе), стандартам свободи вираження поглядів (МПГПП/Загальний коментар 34) і управлінню платформами з повагою до прав (Акт про цифрові послуги DSA). У той же час плюралізм ЗМІ та редакційна незалежність слугують противагою надмірному втручанню, гарантуючи, що захисні заходи будуть оберігати ті самі демократичні цінності, котрі гібридні загрози виборам прагнуть підірвати.

Для урядів і законодавців

1. **Створіть і підтримуйте національну мережу виборчої співпраці:** Зробіть це пріоритетом національної безпеки, створивши формально заснований, постійний орган, який об’єднуватиме орган, що керує виборами, агентства з кібербезпеки, розвідувальні служби, правоохоронні органи та підрозділи стратегічних комунікацій. Ця мережа повинна працювати постійно, виконуючи спільні оцінки ризиків, проводячи імітаційні навчання та розробляючи спільні протоколи реагування.

2. **Посилюйте законодавчу та нормативно-правову бази:**

    - **Незаконне фінансування політичної діяльності:** якщо це ще не зроблено, забороніть анонімні та іноземні пожертви політичним діячам. Оновіть правові норми, щоб врегулювати використання криптовалют, підвищите прозорість інтернет-реклами та вимагайте проведення політичних пожертв через офіційну банківську систему для підвищення відстежуваності та нагляду.

- **Підзвітність платформ:** впровадьте та забезпечте дотримання надійної нормативно-правової бази для платформ соціальних мереж, зосереджених на прозорості алгоритмічного відбору контенту, політичної реклами та доступу до даних для перевірених дослідників.

- **Виборче та кримінальне законодавство:** проведіть вичерпну перевірку виборчого законодавства з метою виявлення та усунення лазівок, вразливих до гібридних загроз. Модернізуйте кримінальний кодекс, щоб в ньому чітко були визначені та каралися правопорушення, спрямовані на виборчий процес, такі як скоординовані кампанії дезінформації та кібератаки на інфраструктуру, щоб забезпечити ефективне притягнення до кримінальної відповідальності.

3. **Інвестуйте у стратегію загальносуспільної стійкості:** фінансуйте та підтримуйте національні ініціативи, які підвищують стійкість суспільства за допомогою двобічного підходу. По-перше, розширюйте можливості громадян і громадянського суспільства, інвестуючи у довгострокові кампанії з підвищення медіаграмотності та ШІ-грамотності, а також шляхом надання постійної підтримки сектору різноманітних та незалежних ЗМІ. Важливим компонентом цього є виділення коштів на журналістику розслідувань, яка необхідна для викриття механізмів дії гібридних загроз. По-друге, ці суспільні зусилля повинні мають доповнюватися власними зобов'язаннями уряду щодо проактивної комунікації, які будуть втілюватися шляхом розвінчування заздалегідь ймовірних наративів та створення офіційних центрів джерел достовірної інформації, які будуть надійним джерелом відомостей для населення та допоможуть «прищепити» громадянам стійкість до маніпуляцій.

4. **Забезпечте спільні технічну інфраструктуру та послуги:** створіть і фінансуйте централізований механізм для надання спільних послуг у сфері кібербезпеки та захищеного зв'язку для ключових демократичних інститутів. Вони мають включати найнеобхідніші засоби захисту, такі як протидія атакам типу «розподілена відмова в обслуговуванні» (DDoS), для веб-сайтів органів, що керують виборами, та високопріоритетних цілей, щоб гарантувати, що ці ресурси залишаться доступними для громадськості, зокрема під час криз.

Для органів, що керують виборами (ОВК)

5. **Забезпечте постійну стратегію з кібербезпеки:** розглядайте безпеку виборів як безперервний, рік за роком, процес. Впровадьте модель проактивного захисту, яка включатиме розгортання базових засобів технічного контролю, як-от стійку до фішингу багатофакторну автентифікацію для всіх критично важливих облікових записів, впровадження архітектури «нульової довіри» («Zero Trust») і вимогу дотримання принципів безпеки за архітектурою та концепцією («secure-by-design») для всіх технологій, що закупаються.

6. **Розробіть і відпрацюйте інтегровані плани реагування:** створіть і регулярно оновлюйте плани реагування на інциденти, які поєднуватимуть технічне стримування зі стратегічними комунікаціями. Державні органи мають бути готові чітко і прозоро спілкуватися з громадськістю під час інцидентів з кібербезпеки або інформаційних інцидентів, щоб упередити дезінформацію та зберегти довіру.

   Важливий перший крок у розробці таких планів — встановити прозоре внутрішнє управління шляхом призначення старшого керівника з повноваженнями збирати юридичний, IT- та комунікаційний персонал і брати на себе одноосібну відповідальність за управління реагуванням під час інциденту. Ці плани також повинні підготувати установу до розкриття ворогами конфіденційної інформації. Така готовність включає набір планів на випадок розголошення таємних матеріалів, де визначені чіткі правові протоколи дій з розкриття інформації з мінімальними негативними наслідками в умовах нестачі часу протягом операції «зламу та витоку» («hack-and-leak»), щоб установа могла відреагувати контрольованим, правомірним чином.

7. **Беріть активну участь у мережах співпраці:** будьте залученим і послідовним партнером у національній мережі виборчої співпраці. Використовуйте цей форум, щоб ділитися і отримувати розвіддані про загрози, підвищувати обізнаність про ширший ландшафт ризиків, а також координувати дії з захисту із органами розвідки та контррозвідки.

Для суб'єктів міжнародної підтримки

8. **Сприяйте створенню «мережі мереж»:** надавайте пріоритет зміцненню міжнародних платформ співпраці, таких як співпраця ЄС-НАТО та Механізм швидкого реагування G7 (RRM). Сприяйте обміну взірцевими практиками та розвідданими про загрози між національними мережами співпраці заради створення глобальної спільноти практик із захисту демократії.

9. **Забезпечуйте адаптовану під конкретні потреби технічну та стратегічну підтримку:** пропонуйте цільову допомогу країнам-партнерам, щоб допомогти їм впровадити власні мережі національної співпраці. Підтримка має бути адаптована до національного контексту та зосереджена на практичній реалізації, має включати сприяння сумісним імітаційним навчанням та надання експертного досвіду зі спеціалізованих галузей, як-от кібербезпека та протидія маніпуляціям FIMI.

10. **Впровадьте модульний підхід до фінансування:** щоб забезпечити практичність підтримки та її орієнтованість на результати, донори повинні розглядати можливість фінансування окремих модулів з високим рівнем віддачі. Стратегічні інвестиції у спільні послуги можуть забезпечити вирішальні економічні переваги за рахунок масштабу. Основні модулі можуть включати:

    - Секретаріат національної мережі виборчої співпраці — для управління координацією.

    - Основний комплекс кібербезпеки — для надання спільно використовуваних послуг, таких як захист від DDoS-атак для веб-сайтів виборчих органів виборчої влади та інших критично важливих установ.

    - Пакет можливостей на рівні установ — для фінансування створення центрів джерел достовірної інформації та методичних посібників з реагування на інциденти в ключових установах.

    - Готовність країн-господарів до міжнародної підтримки — для підготовки правової, організаційної та технічної бази, наприклад, визначеного національного контактного пункту та заздалегідь затверджених правових шаблонів, задля отримання експертної допомоги під час кризи.

    - Спеціалізовані міжнародні групи пікової підтримки — для швидкого розгортання вузькоспеціалізованих ресурсів протидії складним тактикам гібридних загроз, наприклад, спеціальні групи, що реагують на кібератаки, на операції типу «злам та витік» або надають підтримку зі стратегічних комунікацій. Підтримка повинна бути практичною, орієнтованою на потреби та зосередженою на справжній співпраці.

Однак у кінцевому підсумку довгостроковий успіх полягає в першу чергу в тому, щоб не дозволити загрозам взагалі реалізуватися. Цього можна досягнути лише завдяки досконалій операційній діяльності: бездоганному виконанню виборчих процесів, радикально прозорим комунікаціям та чесному визнанню помилок. Саме ця поступова упевнена робота з розбудови міцного інституційного потенціалу та добутої ціною важких зусиль довіри громадськості є найсильнішим захистом проти тих, хто прагне підірвати демократичний процес.

07 Посилання

Agrawal, H., Hamada, Y., & Fernández Gibaja, A. (2021). *Regulating Online Campaign Finance: Chasing the Ghost?* International IDEA. https://www.idea.int/publications/catalogue/regulating-online-campaign-finance

Alihodžić, S. (2023). *Protecting elections: Risk management, resilience-building and crisis management in elections.* International IDEA. https://www.idea.int/publications/catalogue/protecting-elections-risk-management-resilience-building-and-crisis

Alliance for Securing Democracy. (2019). Russian hackers behind surge in cyberattacks targeting Ukrainian election. https://securingdemocracy.gmfus.org/incident/russian-hackers-behind-surge-in-cyberattacks-targeting-ukrainian-election/

Anghel, V. (2024). Why Romania just cancelled its presidential election. *Journal of Democracy* (доступно лише онлайн). https://www.journalofdemocracy.org/online-exclusive/why-romania-just-canceled-its-presidential-election/

Antoniuk, D. (2023, January 7). Moldova's government hit by flood of phishing attacks. *The Record*. https://therecord.media/moldovas-government-hit-by-flood-of-phishing-attacks

Antoniuk, D. (2024, October 21). 'Unprecedented' interference targets Moldova's elections. *The Record / Recorded Future News.* https://therecord.media/unprecedented-interference-moldova-elections-cyberattack

Antoniuk, D. (2025, September 22). Russia steps up disinformation efforts to sway Moldova's parliamentary vote. *The Record*. https://therecord.media/russia-steps-disinfo-moldova-election

Atlantic Council. (2018, September 11). Defining Russian election interference: An analysis of select 2014–2018 cyber-enabled incidents. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/defining-russian-election-interference-an-analysis-of-select-2014-to-2018-cyber-enabled-incidents-2/

Atlantic Council. (2023, February 24). *Narrative warfare: How the Kremlin and Russian news outlets justified a war of aggression against Ukraine.* https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Narrative-Warfare-Final.pdf

Atlantic Council / DFRLab. (2024, November 4). Trends in China's US election interference illustrate its longer game. https://dfrlab.org/2024/11/04/china-us-election-interference/

Bakken, M. (2025, February 3). Election observation and hybrid threats. *European Democracy Hub.* https://europeandemocracyhub.epd.eu/election-observation-and-hybrid-threats/

Balmforth, T., & Dysa, Y. (2024, November 2). Moldova says Russia plans to disrupt expatriate voting in Sunday's runoff. *Reuters.* https://www.reuters.com/world/europe/moldova-claims-russia-plans-disrupt-expatriate-voting-sundays-runoff-2024-11-02/

Barata, J., & Lăzăr, E. (2025, January 27). Will the DSA save democracy? The test of the recent presidential election in Romania. *Tech Policy Press*. https://techpolicy.press/will-the-dsa-save-democracy-the-test-of-the-recent-presidential-election-in-romania

Bateman, J., & Jackson, D. (2024). *Countering disinformation effectively: An evidence-based policy guide.* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/05/countering-disinformation-effectively-policy-guide

Bay, S. (2024). *Countering hybrid threats to elections: From updating legislation to establishing collaboration networks* (Hybrid CoE Research Report 12). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-research-report-12-countering-hybrid-threats-to-elections-from-updating-legislation-to-establishing-collaboration-networks/

Bay, S. (2025). *Protecting electoral integrity: The case of Sweden.* International IDEA. https://www.idea.int/publications/catalogue/protecting-electoral-integrity-case-sweden

Bay, S., Appelgren, J., Isaksson, E., Lindgren, J., & Thunholm, P. (2022). *Threats to Swedish public elections – Examples and scenarios for the Election Administration* (FOI-R--5298--SE). FOI. https://foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R--5298--SE

Bing, C., & Vicens, A. J. (2024, October 23). Iranian hacker group aims at US election websites and media before vote, Microsoft says. *Reuters*. https://www.reuters.com/technology/cybersecurity/iranian-hacker-group-focuses-us-election-websites-media-ahead-vote-microsoft-2024-10-23/

Bjola, C. (2025, February 7). Algorithmic invasions: How information warfare threatens NATO's eastern flank. *NATO Review.* https://archives.nato.int/nato-review-algorithmic-invasions-how-information-warfare-threatens-natos-eastern-flank

Brennan Center for Justice. (2020, October). *2020's lessons for election security.* https://www.brennancenter.org/our-work/research-reports/2020s-lessons-election-security

Bryjka, F. (2024). Russian interference nearly overwhelmed Moldovan presidential election–referendum vote. *Polish Institute of International Affairs* (PISM). https://pism.pl/publications/russian-interference-nearly-overwhelmed-moldovan-presidential-election-referendum-vote

C2PA. (2024). Content credentials & C2PA overview. https://c2pa.org

Canada (Government of Canada). (2025, July 8). *Multi-stakeholder insights: A compendium on countering election interference.* https://www.canada.ca/en/democratic-institutions/services/paris-call-trust-security-cyberspace/multistakeholder-insights-compendium-countering-election-interference.html

The Carter Center. (2025, July 8). Democracy program. https://www.cartercenter.org/peace/democracy/

Center for an Informed Public, Digital Forensic Research Lab, Graphika, & Stanford Internet Observatory. (2021). *The long fuse: Misinformation and the 2020 election.* Election Integrity Partnership. https://purl.stanford.edu/tr171zs0069

Center for Internet Security. (2025a, July 8). EI-ISAC. https://www.cisecurity.org/ei-isac

Center for Internet Security. (2025b, July 8). The IT lifecycle – The CIS guide to election technology procurements. https://election-procurement.docs.cisecurity.org/en/latest/IT_product_services_lifecycle.html

Center for Internet Security. (2025c). Election security spotlight – DDoS attacks. https://www.cisecurity.org/insights/spotlight/election-security-spotlight-ddos-attacks

Cerulus, L. (2025, June). EU comes to Moldova's defense against Russian hacking. POLITICO. https://www.politico.eu/article/eu-moldova-election-cyber-security-russia-hacking/

Chainalysis. (2024a). *2024 cryptocurrency adoption index*. https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/

Chainalysis. (2024b). Malign Interference and Crypto: How Crypto Transaction Tracing Can Expose and Disrupt Malign Influence Efforts. https://www.chainalysis.com/blog/malign-interference-and-crypto/

Chan, K. (2024, December 17). EU investigates TikTok over Romanian presidential election safeguards. AP News. https://apnews.com/article/0638e90cb3898fc61619e8aed4731a53

Chan, K. (2025, July 25). Meta will cease political ads in European Union by fall, blaming bloc's new rules. AP News. https://apnews.com/article/meta-instagram-facebook-eu-european-union-political-89efeac96723308d2a0469740d24d433

CISA (Cybersecurity and Infrastructure Security Agency). (2024a, January 18). Risk in focus: Generative A.I. and the 2024 election cycle. https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle

CISA. (2024b). #Protect2024: Election security. https://www.cisa.gov/topics/election-security/protect2024

CISA. (2025, July 8). Join the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). https://www.cisa.gov/resources-tools/groups/join-elections-infrastructure-information-sharing-and-analysis-center-ei-isac

CISA, & EAC. (2024a). *Election infrastructure incident response communications guide*. https://www.eac.gov/sites/default/files/2024-10/Election_Infrastructure_Incident_Response_Comms_Guide_508.pdf

CISA, & EAC. (2024b). *Enhancing election security through public communications*. https://www.eac.gov/sites/default/files/2024-06/Enhancing_Election_Security_Through_Public_Communications.pdf

Cisco (Outshift). (2025, July 8). Top 15 software supply chain attacks: Case studies. https://outshift.cisco.com/blog/top-10-supply-chain-attacks

Clayton, M. (2014, June 17). Ukraine election narrowly avoided 'wanton destruction' from hackers. *The Christian Science Monitor*. https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers

Cloudflare. (2025, July 8). Exploring Internet traffic shifts and cyber attacks during the 2024 US election. https://blog.cloudflare.com/exploring-internet-traffic-shifts-and-cyber-attacks-during-the-2024-us-election/

CNN. (2024a, April 26). Cyberattack forces Georgia county to sever connection to state voter registration system. https://edition.cnn.com/2024/04/26/politics/georgia-coffee-county-cyberattack-voter-system/index.html

CNN. (2024b, August 19). US concludes Iran is behind hacking attempts targeting Trump and Biden-Harris campaigns. https://edition.cnn.com/2024/08/19/politics/us-concludes-iran-behind-trump-biden-harris-hacking/index.html

Coherent Market Insights. (2025, March 17). Crypto exchange market size and forecast, 2025–2032. https://www.coherentmarketinsights.com/industry-reports/crypto-exchange-market

CoinGecko. (2025). Cryptocurrency prices, charts and market capitalizations. https://www.coingecko.com

Columbia University, SIPA IGP. (2025, July 8). French official outlines government approach to countering foreign online operations. https://igp.sipa.columbia.edu/news/french-official-outlines-government-approach-countering-foreign-online-operations

Communications Security Establishment Canada. (2025, March). CSE releases 2025 update to report on cyber threats to Canada's democratic process. https://www.canada.ca/en/communications-security/news/2025/03/communications-security-establishment-canada-releases-2025-update-to-report-on-cyber-threats-to-canadas-democratic-process.html

Constella Intelligence. (2025, July 8). Voter database leaks threaten the 2024 U.S. election. https://constella.ai/2024-u-s-election-voter-database-leaks/

Council of Europe. (2024). Internet voting in post-war elections in Ukraine: risks and challenges – results of the study presented. https://www.coe.int/en/web/kyiv/-/internet-voting-in-post-war-elections-in-ukraine-risks-and-challenges-results-of-the-study-presented

Council of Europe. (2025, July 8). Foreign interference in electoral processes at local and regional levels. https://rm.coe.int/0900001680b4cb53

County of San Luis Obispo, Clerk-Recorder. (2024, August 1). Federal agencies say cyber attack could hinder public access to election information, not election itself. https://www.slocounty.ca.gov/departments/clerk-recorder/news-announcements/federal-agencies-say-cyber-attacks-could-hinder-public-access-to-election-information-but-not-to-ele

CrowdStrike. (2025a). Zero Trust Security Explained: Principles of the Zero Trust Model. https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/

CrowdStrike. (2025b). Press release: CrowdStrike releases 2025 threat hunting report. https://www.crowdstrike.com/en-us/press-releases/crowdstrike-releases-2025-threat-hunting-report/

Csernatoni, R. (2024). Can democracy survive the disruptive power of AI? *Carnegie Endowment*. https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai

Cyble. (2024). EU cybersecurity in 2024: Insights from ENISA's latest report. https://cyble.com/blog/eu-cybersecurity-in-2024-insights-from-enisa-latest-report/

Cyble. (2025, July 8). Software supply chain attacks surged in April and May. https://cyble.com/blog/supply-chain-attacks-surge-in-april-may-2025/

Deloitte. (2024). ENISA threat landscape 2024: Cyber threat landscape in the financial sector. https://www.deloitte.com/ro/en/our-thinking/articles/raportul-enisa-threat-landscape-2024-peisajul-amenintarilor-cibernetice-sectorul-financiar.html

Electoral Commission (UK). (2024). Electoral Commission response to cyber-attack attribution. https://www.electoralcommission.org.uk/media-centre/electoral-commission-response-cyber-attack-attribution-0

Elections Canada. (2025, July 8). Our work with security agencies and partners – Media guide for the 45th general election. https://www.elections.ca/content.aspx?section=med&dir=guide&document=p19&lang=e

Electionline. (2024, October). *2024 election threat landscape*. https://electionline.org/wp-content/uploads/2024/10/2024-Election-Threat-Landscape-TLP-CLEAR.pdf

ENISA / NIS Cooperation Group. (2024). *Compendium on elections cybersecurity and resilience*. Press release: https://www.enisa.europa.eu/news/safeguarding-eu-elections-amidst-cybersecurity-challenges

Euromaidan Press. (2014). Russian hacking attempt fails, but fake election news airs. https://euromaidanpress.com/2014/05/26/russian-hacking-attempt-fails-but-fake-election-news-airs/

European Commission. (2016). *Joint framework on countering hybrid threats: A European Union response* (JOIN(2016) 18 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016JC0018

European Commission. (2024). Commission opens formal proceedings against TikTok under the DSA (IP/24/6487). https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487

European Commission. (2025a). Hybrid threats – Defence Industry and Space. https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en

European Commission. (2025b). European cooperation network on elections. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/european-cooperation-network-elections_en

European Commission. (2025c, June 12). Commission services and Moldovan authorities conduct a stress test on potential digital hybrid threats to election integrity ahead of Moldova's parliamentary elections. *Shaping Europe's Digital Future*. https://digital-strategy.ec.europa.eu/en/news/commission-services-and-moldovan-authorities-conduct-stress-test-potential-digital-hybrid-threats

European Digital Media Observatory (EDMO). (2024). *Final report – Outputs and outcomes of a community-wide effort (EP elections)*. https://edmo.eu/publications/final-report-results-and-outcomes-of-a-community-wide-effort/

European External Action Service (EEAS). (2024). *Second EEAS report on Foreign Information Manipulation and Interference (FIMI) threats*. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

European External Action Service (EEAS). (2025a). *Third EEAS report on Foreign Information Manipulation and Interference (FIMI) threats*. https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

European External Action Service (EEAS). (2025b). Information integrity and countering FIMI. https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

European External Action Service (EEAS). (2025c). About the EU Partnership Mission in the Republic of Moldova (EUPM Moldova). https://www.eeas.europa.eu/eupm-moldova/about-eu-partnership-mission-republic-moldova_en

EUvsDisinfo. (2024a). *Doppelgänger strikes back: FIMI activities targeting European Parliament elections*. https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections/

EUvsDisinfo. (2024b). Who is afraid of the European Moldova? https://euvsdisinfo.eu/who-is-afraid-of-the-european-moldova/

Europol. (2025, February 28). The DNA of organised crime is changing – and so is the threat to Europe. https://www.europol.europa.eu/media-press/newsroom/news/dna-of-organised-crime-changing-and-so-threat-to-europe

FBI. (2024, November 5). Statement on bomb threats to polling locations. https://www.fbi.gov/news/press-releases/fbi-statement-on-bomb-threats-to-polling-locations

Forbes. (2025, March 10). AI-driven phishing and deepfakes: The future of digital fraud. https://www.forbes.com/councils/forbestechcouncil/2025/03/10/ai-driven-phishing-and-deepfakes-the-future-of-digital-fraud/

Freedom House. (2024). *Freedom in the world 2024: The mounting damage of flawed elections and armed conflict*. https://freedomhouse.org/report/freedom-world/2024/mounting-damage-flawed-elections-and-armed-conflict

GAO (US Government Accountability Office). (2020, February). Election security: *DHS plans are urgently needed…* https://www.gao.gov/assets/gao-20-267.pdf

Gavin, W. (2025, September 23). Moldova arrests 74 in plot to disrupt election. *BBC News*. https://www.bbc.com/news/articles/c4g5kl0n5d2o

Gilbert, D. (2024, April 11). Election workers are already burned out—and on high alert. *WIRED*. https://www.wired.com/story/election-officials-threats-disinformation/

Global Witness. (2024, December 6). TikTok pushes far-right candidate content in Romanian election, investigation shows. https://www.globalwitness.org/en/press-releases/tiktok-pushes-far-right-candidate-content-romanian-election-global-witness-investigation-shows/

Global Witness. (2025, May 15). Ahead of the second round, TikTok continues to push far-right content in Romania. https://globalwitness.org/en/campaigns/digital-threats/tiktok-algorithm-continues-to-push-multiple-times-more-far-right-content-to-users-ahead-of-romanian-election/

Google Cloud. (2023, August). *Poll Vaulting: Cyber Threats to Global Elections*. https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections

Google DeepMind. (2025). SynthID – A tool to watermark and identify content generated through AI. https://deepmind.google/science/synthid/

Hedenskog, J., & Hjelm, M. (2020, October 25). Propaganda by Proxy: Ukrainian oligarchs, TV and Russia's influence (FOI Memo 7312). FOI. https://www.foi.se/rest-api/report/FOI%20Memo%207312

Hedling, E. (2025, April 15). *Social identities and democratic vulnerabilities: Learning from examples of targeted disinformation* (Hybrid CoE Paper 24). Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2025/04/20250415-Hybrid_CoE_Paper-24-WEB.pdf

Hoffman, F. G. (2022). *Towards a fifth wave of deterrence theory and practice* (Hybrid CoE Paper 12). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-deterring-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/

Hollis, D. B., & Ohlin, J. D. (2021). *Defending democracies: Combating foreign election interference in a digital age.* Oxford University Press. https://global.oup.com/academic/product/defending-democracies-9780197556979

Hoogensen Gjørv, G., & Jalonen, O. (2023). *Identity as a tool for disinformation* (Hybrid CoE Strategic Analysis 34). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-34-identity-as-a-tool-for-disinformation-exploiting-social-divisions-in-modern-societies/

Hoxhunt. (2025, July 8). AI-powered phishing outperforms elite cybercriminals in 2025. https://hoxhunt.com/blog/ai-powered-phishing-vs-humans

Huo, J. (2024, November 12). Foreign influence efforts reached a fever pitch during the 2024 elections. *NPR*. https://www.npr.org/2024/11/09/nx-s1-5181965/2024-election-foreign-influence-russia-china-iran

Hybrid CoE. (2024, January). *Frequently asked questions on hybrid threats*. https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf

Hybrid CoE. (2025). Hybrid threats. https://www.hybridcoe.fi/hybrid-threats/

International Foundation for Electoral Systems (IFES). (2024, December 20). The Romanian 2024 election annulment: Addressing emerging threats to electoral integrity. https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity

IGP (Inspectoratul General al Poliției). (2025, September 22). Trust Media responsabil de propaganda pro-rusă și dezinformare, finanțat printr o schemă complexă de spălare de bani, vizat în percheziţiile de astăzi. *Poliția Republicii Moldova*. https://www.igp.gov.md/ro/politia-actiune/trust-media-responsabil-de-propaganda-pro-rusa-si-dezinformare-finantat-printr-o

IGP (Inspectoratul General al Poliției). (2025, August 13). Autoritățile intensifică acțiunile împotriva dezinformării în spațiul digital: peste 400 de canale TikTok vizate pentru blocare. *Poliția Republicii Moldova*. https://politia.md/ro/noutati/autoritatile-intensifica-actiunile-impotriva-dezinformarii-spatiul-digital-peste-400-de

International IDEA. (2019). Inter-agency Collaboration on Cybersecurity in Elections: Roundtable Discussion. https://www.idea.int/news/inter-agency-collaboration-cybersecurity-elections-roundtable-discussion

International IDEA. (2023, November 28). Mauritius: Inter-agency collaboration against hybrid threats. https://www.idea.int/news/mauritius-inter-agency-collaboration-against-hybrid-threats

International IDEA. (2024, September 17). The Global State of Democracy 2024: Strengthening the legitimacy of elections in a time of radical uncertainty. https://www.idea.int/publications/catalogue/global-state-democracy-2024-strengthening-legitimacy-elections

International IDEA. (2025). Political finance database. https://www.idea.int/data-tools/data/political-finance-database

ISACA. (2025, July 8). The 2025 software supply chain security report. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/the-2025-software-supply-chain-security-report

Ivanti. (2025, July 8). Software supply chain attacks risk on the rise. https://www.ivanti.com/blog/software-supply-chain-attack-risk

Kovalčíková, N., & Spatafora, G. (2024, December 17). The future of democracy: Lessons from the US fight against foreign electoral interference in 2024 (EUISS Brief). *EU Institute for Security Studies*. https://www.iss.europa.eu/publications/briefs/future-democracy-lessons-us-fight-against-foreign-electoral-interference-2024

Kubica, L. (2024). *Moldova's struggle against Russia's hybrid threats* (Hybrid CoE Working Paper 28). Hybrid CoE. https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-28-moldovas-struggle-against-russias-hybrid-threats-from-countering-the-energy-leverage-to-becoming-more-sovereign-overall/

Ledford, H. (2024). Deepfakes, trolls and cybertroopers: How social media could sway elections in 2024. *Nature,* 626(7902), 463–464. https://www.nature.com/articles/d41586-024-00274-7

Levin, D. H. (2020). *Meddling in the ballot box: The causes and effects of partisan electoral interventions.* Oxford University Press. https://academic.oup.com/book/36920

Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, M. A., Kendeou, P., & Zaragoza, M. S. (2020). *The Debunking Handbook 2020*. https://www.climatechangecommunication.org/wp-content/uploads/2020/10/DebunkingHandbook2020.pdf

Liberties (Civil Liberties Union for Europe). (2025). *Rule of law report 2025*. https://dq4n3btxmr8c9.cloudfront.net/files/vdxw3e/Liberties_Rule_of_Law_Report_2025_v.pdf

Lopatka, J. (2024, March 27). Czechs sanction Medvedchuk, website over pro-Russian EU political influence. *Reuters.* https://www.reuters.com/world/europe/czechs-sanction-medvedchuk-website-over-pro-russian-eu-political-influence-2024-03-27/

Lores, R. (2025). *Global Crypto User Index 2025.* Statista. https://www.statista.com/outlook/fmo/digital-assets/cryptocurrencies/worldwide?srsltid=AfmBOorgqEAOLng7cSMAFDInxing0Kw13xMpvwg1gJcvm_ZC590gOuQg

Martin, T. (2022, November 11). Russia's cyberattacks aimed at 'destabilizing' Moldova, PM says. *The Record.* https://therecord.media/russias-cyberattacks-aimed-at-destabilizing-moldova-pm-says

McGrath, S. (2025, September 22). Moldova says it has foiled a Russian-backed plot to disrupt its parliamentary election. *AP News.* https://apnews.com/article/moldova-russia-arrests-plot-election-293ee902e878ce1efcca339759eb06d0

McGrath, S., & Alexandru, A. (2025, September 9). Moldova's president accuses Russia of conducting 'hybrid war' ahead of key elections. *AP News.* https://apnews.com/article/moldova-elections-russia-influence-europe-8cc882551dd52957491e3cfd112cc878

McGrath, S., & Dumitrache, N. (2025, May 13). Romania's redo of a presidential election is a high-stakes test of a battered democracy. *AP News.* https://apnews.com/article/romania-constitutional-court-annuls-election-2nd-round-6e5a089462c10f5079e0812c908736aa

Meaker, M. (2023, October 3). Slovakia's election deepfakes show AI is a danger to democracy. WIRED. https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/

Microsoft. (2025, October). *Microsoft Digital Defense Report 2025*. https://aka.ms/Microsoft-Digital-Defense-Report-2025#page=1

Microsoft Threat Analysis Center. (2024a, April 4). Same targets, new playbooks: East Asia threat actors employ unique methods. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/east-asia-threat-actors-employ-unique-methods

Microsoft Threat Analysis Center. (2024b, September 27). Russia-linked operators engaged in expansive efforts to influence US voters. https://www.microsoft.com/en-us/security/security-insider/threat-landscape/russia-linked-operators-engaged-in-expansive-efforts-to-influence-us-voters

Molas, B. (2024, December 15). Doxing: A literature review. *The International Centre for Counter-Terrorism*. https://icct.nl/publication/doxing-literature-review

Moldpres – State News Agency. (2025, August 13). Moldova's Intelligence and Security Service, Police, ANRCETI ask to block over 400 TikTok channels. https://www.moldpres.md/eng/society/moldova-s-intelligence-and-security-service-police-anrceti-ask-to-block-over-400-tiktok-channels

Militära underrättelse- och säkerhetstjänsten (Must). (2025). *Annual Report 2024*. https://www.forsvarsmakten.se/contentassets/546bbe13064a4c739e1cbc4b5e4571f7/2024-must-annual-report.pdf

Nakamura, D., Belton, C., & Sommer, W. (2024, September 4). Justice Dept. charges two Russian media operatives in alleged scheme. *The Washington Post*. https://www.washingtonpost.com/national-security/2024/09/04/justice-department-election-security/

Nardelli, A. (2025, September 22). Revealed: Putin's secret plan to hack Moldova's pivotal election. *Bloomberg*. https://www.bloomberg.com/news/articles/2025-09-22/moldova-elections-russia-s-plan-to-hack-the-vote

National Task Force on Election Crises. (2025a, July 8). National Task Force on Election Crises. Protect Democracy. https://protectdemocracy.org/work/national-task-force-on-election-crises/

National Task Force on Election Crises. (2025b, July 8). Lessons from the 2024 general election. https://electiontaskforce.org/lessons-from-the-2024-general-election/

NATO. (2022). *Strategic concept*. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO. (2024). Countering hybrid threats. https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO. (2025). NATO's approach to counter information threats (official text). https://www.nato.int/cps/en/natohq/official_texts_231905.htm

NCSC (UK). (2025). *Cyber Assessment Framework v4.0*. https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf

Newman, N., Fletcher, R., Robertson, C. T., Ross Arguedas, A., & Nielsen, R. K. (2024). *Digital News Report 2024*. Reuters Institute. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf

National Institute of Standards and Technology (NIST). (2020). SP 800-207: *Zero Trust Architecture*. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

National Institute of Standards and Technology (NIST). (2022). *SP 800-218: Secure Software Development Framework (SSDF) v1.1*. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-218.pdf

National Institute of Standards and Technology (NIST). (2023). SP 800-207A: *A Zero Trust Architecture model for access decisions*. https://csrc.nist.gov/pubs/sp/800/207/a/final

National Institute of Standards and Technology (NIST). (2024). SP 800-218A: *Secure software development practices for generative AI & dual-use foundation models*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.pdf

O'Brien, M., & Swenson, A. (2024, February 16). Tech companies sign accord to combat AI-generated election trickery. *AP News*. https://apnews.com/article/ai-generated-election-deepfakes-munich-accord-meta-google-microsoft-tiktok-x-c40924ffc68c94fac74fa994c520fc06

Ohlin, J. D. (2020). *Election interference: International law and the future of democracy*. Cambridge University Press. https://doi.org/10.1017/9781108859561

Olari, V. (2024, October 18). What to know about Russian malign influence in Moldova's upcoming election. *Atlantic Council*. https://www.atlanticcouncil.org/blogs/new-atlanticist/what-to-know-about-russian-malign-influence-in-moldovas-upcoming-election/

Olari, V. (2025a, March 6). Telegram network seeks to manipulate Moldova's local political discourse. *DFRLab*. https://dfrlab.org/2025/03/06/telegram-network-moldova/

Olari, V. (2025b, March 26). Cross-platform campaign sows anti-Europe division in Moldova. *DFRLab*. https://dfrlab.org/2025/03/26/cross-platform-campaign-sows-anti-europe-division-in-moldova/

OSCE/ODIHR. (2017). Montenegro, Parliamentary Elections, 16 Oct 2016: Final report. https://www.osce.org/odihr/elections/montenegro/295511

OSCE/ODIHR. (2021). *Republic of Moldova, Early Parliamentary Elections, 11 July 2021: Final report*. https://www.osce.org/odihr/elections/moldova/501518

OSCE/ODIHR. (2024). *Moldova, Presidential Election and Constitutional Referendum, 20 Oct 2024: Statement of preliminary findings and conclusions*. https://www.osce.org/odihr/elections/moldova/578815

OSCE/ODIHR. (2025a, February 20). *Poland, Presidential Election, Run-off, 2025: Final report*. https://www.osce.org/odihr/elections/poland/591761

OSCE/ODIHR. (2025b, September 28). *Republic of Moldova, statement of preliminary findings and conclusions*. https://www.osce.org/files/f/documents/4/7/597800.pdf

OSCE/ODIHR. (2025c, March 14). *Republic of Moldova: Presidential election and constitutional referendum, 20 Oct & 3 Nov 2024, Final report*. https://www.osce.org/files/f/documents/3/9/587451_0.pdf

OSCE/ODIHR. (2025d, May 5). Notable efforts to address electoral integrity but certain aspects… (Romania). https://www.osce.org/odihr/elections/romania/590330

Pamment, J., Nothaft, H., Agardh-Twetman, H. & Fjällhed, A. (2018). *Countering Information Influence Activities: The State of the Art*. MSB. https://rib.msb.se/filer/pdf/28697.pdf

Pamment, J., & Tsurtsumia, D. (2025, May). *Beyond Operation Doppelgänger: A capability assessment of the Social Design Agency (SDA)*. Lund University & Swedish Psychological Defence Agency. https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2025-05/Beyond%20Operation%20Doppelg%C3%A4nger.pdf

Pamment, J., & Isaksson, E. (2024). *Psychological Defence: Concepts and Principles for the 2020s* (MPF Report Series 6/2024). Lund University & Swedish Psychological Defence Agency. https://www.mpf.se/wp-content/uploads/2024/03/mpf_rapport_6_2024_psychological_defence.pdf

Perdomo, C., & Uribe Burcher, C. (2017). Money, influence, corruption and capture: can democracy be protected?. *The Global State of Democracy 2017 Exploring Democracy's Resilience*. International IDEA. https://www.idea.int/gsod-2017/files/IDEA-GSOD-2017-REPORT-EN.pdf

Popescu-Zamfir, R. (2025, September 26). *Moldova's Election Is a Test for Russian Influence in Europe. Carnegie Endowment for International Peace.* https://carnegieendowment.org/research/2025/09/moldovas-election-is-a-test-for-russian-influence-in-europe?lang=en

Posetti, J., et al. (2020). *Online violence against women journalists: A global snapshot of incidence and impacts.* UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000375136/PDF/375136eng.pdf.multi

Rainsford, S. (2024, December 4). Romania hit by major election influence campaign and Russian cyber-attacks. *BBC.* https://www.bbc.com/news/articles/cgq18w507dko

ReliaQuest. (2024, September 24). 2024 US election: Top cyber threats & organizational impacts. https://www.reliaquest.com/blog/2024-us-election-top-cyber-threats-organizational-impacts/

Reuters. (2024a, October 24). Chinese influence operation targets U.S. down-ballot races, Microsoft says. https://www.reuters.com/world/us/chinese-influence-operation-targets-us-down-ballot-races-microsoft-says-2024-10-23/

Reuters. (2024b, November 5). Hoax bomb threats linked to Russia target polling places in battleground states, FBI says. https://www.reuters.com/world/us/fake-bomb-threats-linked-russia-briefly-close-georgia-polling-locations-2024-11-05/

RFE/RL Moldovan Service. (2024, October 25). Moldovan police accuse pro-Russian oligarch of $39M vote-buying scheme. https://www.rferl.org/a/moldova-police-accuse-shor-russia-oligarch-39m-vote-buying/33172951.html

Roth, A. (2024, September 4). Russia accused of trying to influence US voters through online campaign. *The Guardian.* https://www.theguardian.com/us-news/2024/sep/04/russia-us-election-online-campaign-sanctions

Saeva, E., & Tasheva, I. (2024). The 2024 EU elections and cybersecurity: A retrospective and lessons learned. *European View* (Martens Centre). https://www.martenscentre.eu/wp-content/uploads/2024/11/12.pdf

Schroeder, D. T., Cha, M., Baronchelli, A., Bostrom, N., Christakis, N. A., Garcia, D., … Kunst, J. R. (2025). How malicious AI swarms can threaten democracy. *arXiv.* https://doi.org/10.48550/arXiv.2506.06299

Stimson Center. (2024, August 8). RAI Session: AI & democracy (event). https://www.stimson.org/event/rai-session-ai-democracy/

Stockwell, S., Hughes, M., Swatton, P., Zhang, A., Hal, J., & Kieran. (2024). *AI-enabled influence operations: Safeguarding future elections.* The Alan Turing Institute (CETaS). https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections

Tanas, A. (2024, October 24). Moldovan president says bribery affected election, pledges run-off vote. *Reuters.* https://www.reuters.com/world/europe/moldova-police-say-businessman-shor-channelled-24-million-pay-off-voters-2024-10-24/

Turing Institute / CETaS. (2024). AI-enabled influence operations: *Safeguarding future elections.* https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections

Uribe Burcher, C. (2017). Assessing the threat of nexus between organized crime and democratic politics: Mapping the factors. *International Relations and Diplomacy,* 5(1). https://www.davidpublisher.com/index.php/Home/Article/index?id=30183.html

Uribe Burcher, C. (2019). *Cryptocurrencies and political finance*. International IDEA. https://www.idea.int/publications/catalogue/cryptocurrencies-and-political-finance

U.S. Cyber Command. (2024, September 12). Russian disinformation campaign Doppelgänger unmasked: A web of deception. https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception/

U.S. Department of Justice (DOJ). (2024a). Election threats. https://www.justice.gov/archives/voting/election-threats

U.S. Department of Justice (DOJ). (2024b, September 4). Justice Department disrupts covert Russian government–sponsored foreign malign influence operation. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

U.S. Office of the Director of National Intelligence (ODNI). (2024, March 11). *Annual threat assessment of the U.S. Intelligence Community*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf

U.S. Office of the Director of National Intelligence (ODNI). (2025, March 18). *Annual threat assessment of the U.S. Intelligence Community 2025*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

U.S. Treasury (OFAC). (2024a, September 4). Treasury takes action as part of a U.S. Government response to Russia's foreign malign influence operations. https://home.treasury.gov/news/press-releases/jy2559

U.S. Treasury (OFAC). (2024b, December 31). Treasury sanctions entities in Iran and Russia that attempted to interfere in the U.S. 2024 election. https://home.treasury.gov/news/press-releases/jy2766

V-Dem Institute. (2024). Democracy report 2024: *Democracy winning and losing at the ballot*. https://v-dem.net/publications/democracy-reports/

V-Dem Institute. (2025). *Autocratization turns viral: Democracy report 2025*. https://v-dem.net/publications/democracy-reports/

Vanderlee, K., & Collier, J. (2024, April 25). Poll vaulting: Cyber threats to global elections. *Google Cloud / Mandiant*. https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections

Weatherbed, J. (2024, November 14). Google says it will stop serving political ads in the EU. *The Verge*. https://www.theverge.com/2024/11/14/24296510/google-dropping-political-ads-in-the-eu-ttpa

Westminster Foundation for Democracy (WFD). (2025). *Understanding and addressing the cost of politics*. https://www.wfd.org/cost-of-politics

WHAS11. (2025, July 8). Jefferson County Clerk's Office says voting system remains safe after ransomware attack. https://www.youtube.com/watch?v=diY7hpMlY5o

Wilson, A. (2023). *Democracy under siege: Tackling Russian interference in Moldova*. ECFR. https://ecfr.eu/article/democracy-under-siege-tackling-russian-interference-in-moldova/

Wilson Center. (2025, March 19). Ukraine's presidential elections amid war: Political, legal, and security challenges. https://www.wilsoncenter.org/blog-post/ukraines-presidential-elections-amid-war-political-legal-and-security-challenges

08 Прикінцева виноска

1 Global Witness, 2025; Meaker, 2023; Rainsford, 2024; McGrath & Alexandru, 2025
2 Bay et al., 2022; Hollis & Ohlin, 2021
3 Bay, 2024; EEAS, 2025a
4 Bay et al., 2022; Bay 2024; Levin, 2020; Ohlin, 2020
5 Pamment & Tsurtsumia, 2025
6 cf. Communications Security Establishment Canada, 2025; Must, 2025; US Office of the Director of National Intelligence, 2025
7 Bay, 2024
8 Stockwell et al., 2024; Csernatoni, 2024; Schroeder et al., 2025
9 Stockwell et al., 2024; Csernatoni, 2024; Schroeder et al., 2025
10 Bay, 2024; Hybrid CoE, 2025
11 Bay, 2024
12 Bay, 2024; Alihodžić, 2023; Center for an Informed Public et al., 2021
13 International IDEA, 2024
14 Bryjka, 2024; OSCE/ODIHR, 2025b; OSCE/ODIHR, 2025c
15 Gilbert, 2024
16 Center for an Informed Public et al., 2021
17 Center for an Informed Public et al., 2021; International IDEA, 2024; DFRLab, 2023; EUvsDisinfo 2024
18 Huo, 2024; Hedling, 2025
19 Hedling, 2025
20 Hoogensen Gjørv & Jalonen, 2023
21 Hedling, 2025
22 Hedling, 2025
23 US Office of the Director of National Intelligence, 2025
24 Pamment & Tsurtsumia, 2025
25 Bay, 2024; Pamment & Isaksson, 2024; Pamment & Tsurtsumia, 2025
26 Hoffman, 2022
27 Atlantic Council 2023; Pamment & Tsurtsumia, 2025
28 Bay, 2024; European Commission, 2016; EEAS, 2024; EEAS 2025a; NATO, 2022; NATO, 2025
29 EEAS, 2025a; EEAS, 2025b
30 cf. Huo, 2024; Pamment & Tsurtsumia, 2025; Stockwell et al., 2024
31 Pamment & Tsurtsumia, 2025; Microsoft Threat Analysis Center, 2024a; Microsoft Threat Analysis Center, 2024b
32 EEAS, 2025a; U.S. Cyber Command, 2024
33 Pamment & Tsurtsumia, 2025
34 EDMO, 2024
35 Pamment & Tsurtsumia, 2025
36 EUvsDisinfo, 2024a
37 Bjola, 2025; IFES, 2024; Global Witness, 2024
38 Chan 2024; European Commission, 2024
39 Clayton, 2014; Atlantic Council, 2018
40 Nardelli, 2025
41 OSCE/ODIHR, 2024; OSCE/ODIHR, 2025b

42 Kubica, 2024; EUvsDisinfo, 2024b
43 Tanas, 2024; Balmforth & Dysa, 2024
44 Antoniuk, 2024; Antoniuk, 2025; Olari, 2024; Olari, 2025a; Olari, 2025b
45 Kubica, 2024; EUvsDisinfo, 2024a; DFRLab, 2024
46 Tanas, 2024; Balmforth & Dysa 2024; OSCE/ODIHR 2025; RFE/RL Moldovan Service, 2024
47 DFRLab, 2024; EUvsDisinfo, 2024a; Balmforth & Dysa, 2024
48 McGrath, 2025; IGP, 2025
49 McGrath, 2025; IGP, 2025
50 Moldpres, 2025; IGP, 2025
51 Antoniuk, 2023; Antoniuk, 2024; Antoniuk, 2025; Martin; 2022; OSCE/ODIHR, 2021
52 Cerulus, 2025; EEAS 2025c; European Commission 2025c
53 Pamment & Tsurtsumia, 2025
54 Euromaidan Press, 2014; EEAS, 2025a
55 Hedenskog & Hjelm, 2020; Lopatka, 2024
56 Clayton, 2014; Atlantic Council, 2018; Euromaidan Press, 2014
57 ODNI, 2024; ODNI, 2025
58 FBI, 2024; Reuters, 2024a; Roth, 2024; U.S. Treasury, 2024a, 2024b
59 DOJ, 2024b; Microsoft Threat Analysis Center, 2024b; Nakamura, Belton & Sommer, 2024
60 Atlantic Council, 2024; Microsoft Threat Analysis Center, 2024a; Reuters, 2024a
61 Bing & Vicens, 2024; DOJ, 2024a Gavin, 2025
62 DOJ, 2024a; FBI, 2024; U.S. Treasury, 2024a; 2024b
63 Kovalčíková & Spatafora, 2024; National Task Force on Election Crises, 2025a; National Task Force on Election Crises, 2025b; Turing CETaS, 2024
64 Bay, 2024
65 Ledford, 2024
66 Pamment & Tsurtsumia, 2025
67 Zuboff, 2019
68 Cf. Mutu, 2024; Newman, Fletcher, Robertson, Ross Arguedas, & Nielsen, 2024
69 European Commission, 2024
70 Weatherbed, 2024; Chan, 2025
71 Elliott, 2024
72 O'Brien & Swenson, 2024; Brennan Center for Justice, 2024
73 C2PA, 2024
74 Google DeepMind, 2025
75 Newman et al., 2024
76 Pamment & Tsurtsumia, 2025
77 Bateman & Jackson, 2024; Bay, 2025; Pamment et al. 2018; Pamment & Isaksson, 2024
78 OECD 2021; OECD 2022
79 ENISA 2023; International IDEA 2023; Bay 2025
80 Center for an Informed Public et al. 2021
81 Lewandowsky et al., 2020
82 EEAS, 2025
83 OECD, 2021
84 Center for an Informed Public et al., 2021; C2PA, 2024; ENISA, 2023
85 OECD, 2022
86 C2PA, 2024; Google DeepMind, 2025
87 Perdomo & Uribe Burcher, 2017: 128; WFD, 2025
88 Bakken, 2025; Popescu-Zamfir, 2025; OSCE/ODIHR, 2017: 12; 2021: 16
89 International IDEA, 2025
90 OSCE/ODIHR, 2025a: 1–2
91 Wilson, 2023
92 Wilson, 2023; OSCE/ODIHR, 2025b: 1
93 International IDEA, 2025
94 Perdomo & Uribe Burcher, 2017: 134
95 CoinGecko, 2025; Lores, 2025; Chainalysis, 2024a
96 Coherent Market Insights, 2025
97 Uribe Burcher, 2019: 14
98 Uribe Burcher, 2019: 13; Chainalysis, 2024b

99 International IDEA, 2025
100 Perdomo & Uribe Burcher, 2017: 139; Wolfs, 2025: 3–4
101 Wolfs, 2025: 5
102 Agrawal, Hamada & Fernández Gibaja, 2021: 12
103 Ryan, 2018; Britzky, 2018
104 DOJ, 2024a
105 IFES, 2024
106 OSCE/ODIHR, 2025a: 8–9
107 Perdomo & Uribe Burcher, 2017: 137–138
108 Council of Europe, 2025: 4
109 International IDEA, 2025
110 Wolfs, 2025: 2
111 Perdomo & Uribe Burcher, 2017: 141
112 Uribe Burcher, 2019: 7, 9–11
113 Vasani, James & Holly, 2022
114 Uribe Burcher, 2019: 15–16
115 International IDEA, 2025
116 Perdomo & Uribe Burcher, 2017: 138–139
117 Uribe Burcher, 2019: 16
118 Wolfs, 2025: 2
119 Perdomo & Uribe Burcher, 2017: 144
120 International IDEA, 2025
121 V-Dem, 2024; V-Dem, 2025; UNESCO, 2025; Posetti et al., 2020
122 Council of Europe, 2025; Liberties, 2025; Freedom House, 2024
123 CIVICUS, 2024; OSCE/ODIHR, 2023
124 OECD, 2021; OSCE/ODIHR, 2023
125 Perdomo & Uribe Burcher, 2017: 136
126 Europol, 2025a; Hoxhunt, 2025
127 Bay, 2024
128 Uribe Burcher, 2017
129 Europol, 2025a
130 Cyble, 2024
131 Deloitte, 2024
132 Europol, 2025a
133 Europol 2025a; Deloitte 2024
134 Must, 2025; ReliaQuest, 2024
135 ReliaQuest, 2024; Center for Internet Security, 2025a
136 Europol, 2025a
137 CISA, 2024
138 CISA, 2024
139 Hoxhunt, 2025
140 Forbes 2025
141 CISA 2024a; NIST 2020; FIDO Alliance 2023; ENISA 2023; MS-ISAC 2024; C2PA 2024
142 Bay, 2024; ReliaQuest, 2024
143 Bay et al., 2022
144 Bay, 2024
145 UK Electoral Commission, 2024
146 Euromaidan Press, 2014
147 Alliance for Securing Democracy, 2019
148 Council of Europe, 2024; Wilson Center, 2025
149 CNN, 2024a
150 WHAS11, 2025
151 Constella Intelligence, 2025
152 Center for Internet Security, 2025a; Center for Internet Security, 2025b; Center for Internet Security, 2025c
153 Cloudflare, 2025
154 Saeva & Tasheva, 2024
155 Bay et al., 2022; County of San Luis Obispo, 2024

156 Bay, 2024; ReliaQuest, 2024
157 Electionline, 2024
158 Ivanti, 2025
159 Cyble, 2025
160 ReversingLabs 2025; ISACA, 2025
161 ISACA, 2025
162 Cisco, 2025
163 International IDEA, 2019
164 Bay, 2024
165 Google Cloud, 2023
166 CISA, 2024
167 Molas, 2024; Cybersecurity Dive, 2024
168 Stimson Center, 2024
169 International IDEA 2019; Bay 2024; Google Cloud 2023; CISA 2024a; Stimson Center 2024
170 cf. Microsoft, 2025
171 Vanderlee & Collier, 2024; NCSC, 2025
172 Bay, 2024; International IDEA, 2023
173 Center for Internet Security 2025a; NIST, 2022; NIST, 2024
174 CrowdStrike 2025a; NIST, 2020; NIST, 2023
175 CISA, 2024b; CrowdStrike, 2025b
176 CISA & EAC, 2024a; CISA & EAC, 2024b; CISA, 2024b
177 Bay, 2024; Bay, 2025
178 Bay, 2024
179 Canada, 2025
180 Bay, 2024
181 Bay, 2024
182 European Commission, 2016; European Commission, 2025b
183 Bay, 2024; Bay, 2025
184 Bay, 2025
185 GAO, 2020
186 Columbia University, 2025
187 Elections Canada, 2025
188 Government of Canada, 2025; PCO, 2025
189 Canada, 2025, CISA 2025
190 Cf Bay, 2025
191 Hybrid CoE, 2024
192 Bay, 2025; Canada, 2025
193 European Commission, 2025b
194 Bay, 2024; Elections Canada, 2025
195 European Commission, 2025b
196 European Commission, 2025a
197 NATO, 2024; Elections Canada, 2025
198 International IDEA, 2025; The Carter Center, 2025
199 US Office of the Director of National Intelligence, 2025; Pamment & Tsurtsumia, 2025
200 Pamment & Tsurtsumia, 2025
201 Stockwell et al. 2024; CISA, 2024a
202 IFES 2024; Bay, 2024
203 Brennan Center for Justice, 2020; Elliott, 2024; European Commission, 2024; C2PA, 2024; Pamment & Tsurtsumia, 2025

Академія Фольке Бернадота (FBA) є державною установою Швеції з питань миру, безпеки та розвитку. В рамках міжнародного співробітництва Швеції з питань розвитку ми сприяємо просуванню миру в країнах, що постраждали від конфліктів. Ми пропонуємо навчання та консультації, а також проводимо дослідження з метою зміцнення миру та урядування, в контекстах миру та безпеки. Крім того, ми направляємо цивільний персонал у миротворчі операції та місії спостереження за виборами, головним чином під проводом ООН, ЄС та ОБСЄ. Установу названо на честь графа Фольке Бернадота, — першого мирного посередника ООН.

Якщо ви хочете дізнатися більше про FBA, познайомтеся з нами за посиланнями:

linkedIn.com/FolkeBernadotteAcademy

instagram.com/FolkeBernadotteAcademy

facebook com/FolkeBernadotteAcademy

fba.se/en

Folke Bernadotte Academy
Шведське агентство з питань миру, безпеки та розвитку

FBA