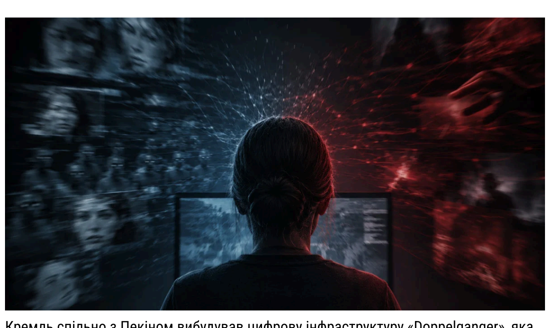
ВІЙНА З РФ

Операція Доппельгенгер та кремлівські ШІ-фабрики клонування світових медіа

PUBLISHED 19 ТРАВНЯ 2026



Кремль спільно з Пекіном вибудував цифрову інфраструктуру «Doppelganger», яка мільйонними ШІ-тиражами клонує Washington Post, Le Monde та BBC. Мета цієї спецоперації — не просто змусити західного виборця повірити в чергову брехню про Україну, а тотально отруїти сам інформаційний простір. Коли Маск і Трамп-молодший слухняно репостять ШІ-пародії на світові медіа, стає зрозуміло: головна битва розгортається не за географічні кордони, а всередині людського сприйняття, де кінцевою метою є абсолютна втрата віри у будь-яку реальність.

16 березня 2022 року, через три тижні після початку повномасштабного вторгнення Росії до України, на сайті українського телеканалу «Україна 24» з'явилося відео. На екрані президент Володимир Зеленський стояв за трибуною і звертався до нації. «Я вирішив повернути Донбас, — казала людина, схожа на нього. — Наші зусилля провалились. Моя порада — всім скласти зброю і повернутись до сімей». Насправді Зеленський ніколи цього не казав, нагадує очевидне видання ТИЖДЕНЬ. Відео було deepfake — цифровою підробкою, яку хакери розмістили на зламаному сайті телеканалу та паралельно пустили у рухомий рядок прямого ефіру. Протягом кількох хвилин відео розлетілось у телеграмі, вконтактє і твітері. Фейсбук видалив його після скарг, але до того часу воно встигло зібрати сотні тисяч переглядів.

Зеленський відреагував швидко, записавши звернення у військовій формі з вулиці у Києві. «Ми захищаємо нашу землю, наших дітей, наші сім'ї», — сказав він. Але дослідники з організації Witness, яка спеціалізується на виявленні підробленого контенту, одразу попередили про небезпеку. «Конкретна проблема полягає в так званому дивіденді брехуна, коли справжнє відео легко оголосити підробленим і перекласти тягар доведення на тих, хто стверджує, що воно автентичне», — пояснив дослідник Сем Грегорі з Witness.

> *Це був не поодинокий експеримент, а публічна демонстрація нового виду комбінованої зброї та перший публічний тест того, як далеко Росія готова зайти в інформаційній війні проти України.*

Операція Doppelganger: як Кремль клонує реальність

Поки тривала війна, паралельно розгорталася інша операція — масштабніша, витонченіша і розрахована не лише на Україну, а на весь Захід. Її назва — «Doppelganger», тобто «двійник». Суть проста: створити сайти, які виглядають точнісінько як авторитетні медіа — Fox News, Washington Post, Der Spiegel, Le Monde, BBC, — і публікувати там вигаданий контент. Читач бачить знайомий логотип, шрифт, верстку і не помічає, що адреса сайту трохи відрізняється. Замість washingtonpost.com відкривається washingtonpost.pm, замість fox-news.com — fox-news.top. Операція почалась у травні 2022 року, а вже у вересні її викрила організація EU DisinfoLab. Але, попри викриття, вона не зупинилась — лише адаптувалася.

Згідно з документами, які у 2024 році оприлюднило міністерство юстиції США, операцію проводили дві російські компанії, Social Design Agency і Structura, за прямим наказом Кремля. Заступниця генерального прокурора США Ліза Монако сформулювала це чітко: «За вказівкою Путіна, компанії SDA, Structura й ANO Dialog використовували кіберсквотинг, сфабрикованих інфлюєнсерів і фейкові профілі для прихованого просування згенерованих ШІ неправдивих наративів у соціальних мережах».

Щодо України мета операції була конкретною. Фейкові версії Fox News і Washington Post публікували матеріали про те, що американський борг зростає через допомогу Україні, що Зеленський корумпований, а США мають зосередитись на власних проблемах. Один із внутрішніх «планових документів» SDA, на який посилається американське обвинувачення, прямо вказував, що мета проєкту — «вплинути на громадську думку в США так, щоб американці вважали, буцімто їхня країна має зосередити зусилля на розв'язанні внутрішніх питань замість витрачати гроші на Україну та інші проблемні регіони».

Для різних аудиторій операція генерувала різний контент. Так, для американської ЛГБТ-спільноти публікувалися матеріали про переслідування «трансгендерної молоді» в Україні. Для німецькомовної аудиторії — дописи, що критикували уряд і підтримку України. Для франкомовної — наративи про те, що Франція є «васалом» США і що НАТО діє проти французьких інтересів.

Технічна схема була продумана до деталей. Домени реєструвались через американські реєстратори Namecheap, NameSilo і GoDaddy, платіжні операції здійснювались через підставних осіб у США, а IP-адреси серверів раніше були пов'язані з кіберзлочинною діяльністю. Для обходу алгоритмів модерації платформ використовувався спеціальний сервіс-клоакінг Kehr, який підставляв різний контент залежно від того, хто відкривав посилання — звичайний користувач чи модератор платформи.

Баварська розвідка відстежила понад 7 983 кампанії та 828 842 кліки лише за двома серверами за період з травня 2023-го по липень 2024 року. Окрема мережа фейкових профілів, так звані «Одетти», системно просувала матеріали Doppelganger у коментарях під публікаціями великих фейсбук-сторінок. Усі вони мали жіноче ім'я Одетта і нібито працювали у Netflix.

У серпні 2024 року Meta оголосила, що виявила понад 6 000 індикаторів загрози та вилучила понад 5 000 профілів та сторінок. Але операція тривала. Зрештою ФБР вилучило десятки доменів, серед них ribunalukraine.info, waronfakes.com, fox-news.top, washingtonpost.pm, spiegel.agency. Щоразу, коли платформи й уряди закривали один вузол мережі, натомість з'являлись нові.

Штучний інтелект на службі пропаганди

У попередньому десятилітті операція Doppelganger була б неможливою, принаймні в такому масштабі. Те, що мережа робила з десятками тисяч публікацій різними мовами та для різних аудиторій, вимагало б армії перекладачів, редакторів і аналітиків. Сьогодні значну частину цієї роботи виконує штучний інтелект. У 2024 році мережа «Правда», один із найбільших проросійських дезінформаційних ресурсів, опублікувала близько 3,5 мільйона статей, згенерованих ШІ. Метою було не лише поширення наративів, а й «отруєння» баз даних. Якщо в інтернет потрапляє достатньо багато фейкового контенту, наступне покоління ШІ-моделей уже навчається на спотвореній картині світу.

Операція Storm-1679 використовувала ШІ для підробки голосу відомого американського актора у фальшивому документальному фільмі від імені Netflix, спрямованому проти Міжнародного олімпійського комітету. Глядачі чули знайомий голос, бачили знайомий логотип і довіряли побаченому. У серпні 2025 року та сама мережа настільки переконливо зімітувала ABC News, BBC і POLITICO за допомогою deepfake, що її матеріали поширили Дональд Трамп-молодший та Ілон Маск.

Лютий 2026 року приніс новий задокументований приклад. Під час зимових Олімпійських ігор у Мілані та Кортіні BBC Verify задокументували масштабну операцію мережі «Матрьошка», спрямовану проти українських спортсменів та вболівальників. В одному з відео глядачі спочатку бачили справжню пресконференцію президентки Міжнародного олімпійського комітету Кірсті Ковентрі, а за кілька секунд справжній голос замінювався на ШІ-клон. «Матрьошка» змушувала Ковентрі «заявляти», буцімто українські спортсмени приїхали до Мілана «заради шаленого політичного піару» і вона «ніколи не зустрічала таких неприємних людей». Насправді ж Ковентрі не казала нічого подібного. За даними BBC Verify, до кінця лютого 2026 року було задокументовано щонайменше 35 відео, що імітували бренди медіа й урядових організацій, пов'язаних з Олімпіадою, одне з яких зібрало понад мільйон переглядів.

> *На Україну були спрямовані окремі deepfake-кампанії ще від початку повномасштабного вторгнення. Росія поширювала deepfake президента Молдови Маї Санду з фальшивими заявами про її позицію щодо Росії, а також аудіопідробку словацького політика Міхала Шімечки.*

За даними Центру протидії дезінформації України, з початку 2025 року зафіксовано 191 російську інформаційну операцію з використанням ШІ-контенту загальним охопленням щонайменше 84,5 мільйона переглядів. Дослідниця Дезіре Вінс, яка вивчала цю тему для Фонду Гайнріха Бьолля, зафіксувала важливу закономірність. «Навіть очевидні копії можуть впливати на пам'ять, переконання та ухвалення рішень, думки людей можуть змінюватись під впливом взаємодії з цифровою копією, навіть коли вони знають, що перед ними не справжня людина», — пояснила вона.

Боти, «живі» профілі та схема «відмивання» інформації

Виробництво фейкового контенту — лише перша частина операції. Другий ключовий елемент — це розповсюдження за цільовими аудиторіями. І тут Росія навчилась використовувати саму архітектуру соціальних мереж проти їхніх же користувачів. Виявляти «традиційних» ботів відносно просто. Вони публікують однотипні повідомлення, не мають особистої історії та демонструють підозріло рівномірну активність цілодобово. Але технології пішли далі: сучасні «живі» профілі, які дослідники також називають «сплячими» або «імпостерами», роками виглядають як справжні люди. Публікують фотографії з відпусток, обговорюють місцеві новини, коментують спортивні матеріали та рецепти. А потім, у визначений момент, за командою вони одночасно «прокидаються» і починають масово поширювати конкретний наратив. Платформи не встигають реагувати, бо на момент активізації профіль уже має місяці чи навіть роки «чистої» органічної історії.

Операція Doppelganger використовувала ще одну схему, яку дослідники назвали «відмиванням дезінформації». Спочатку матеріал з'являвся на маловідомому проросійському сайті. Мережа ботів і «сплячих» акаунтів підхоплювала публікацію і штучно нарощувала лайки, репости та коментарі. Алгоритм платформи фіксував активність і починав рекомендувати публікацію ширшій аудиторії. І реальні люди ділились нею далі — вже без усвідомлення, що першоджерело пов'язане з Кремлем.

Doppelganger відстежував понад 2 800 реальних американських інфлюєнсерів як потенційних партнерів. Один із внутрішніх документів SDA містив пропозицію залучити їх для розпалювання «внутрішньої напруженості» всередині союзницьких країн. Частина з цих лідерів думок не здогадувалась, що вже перебуває в прицілі кремлівського PR-відділу.

Під час виборів у Німеччині у грудні 2024-го — січні 2025 років дослідницька організація CeMAS зафіксувала понад 600 оригінальних проросійських публікацій, кожна з яких поширювалась сотні разів. Загальне охоплення склало 2,8 мільйона переглядів. Частина цього контенту потрапила до офіційних акаунтів кандидатів від різних партій, які поширювали матеріали з твердженнями, нібито «Зелені» й українські чиновники вербують мігрантів для скоєння злочинів.

Зливи документів: коли «правда» стає зброєю

Окремий інструмент інформаційних операцій, який часто залишається поза увагою широкої публіки, — цілеспрямовані зливи документів. Відповідна схема відпрацьована Росією ще у 2016 році під час президентських виборів у США і звідтоді застосовується регулярно. У травні 2017 року, за два дні до другого туру президентських виборів у Франції, хакери злили в мережу 15 гігабайтів даних зі скриньок команди кандидата Еммануеля Макрона. Операція включала три послідовні фази. Спочатку місяцями тривала дезінформаційна кампанія з чутками й фейками. Потім хакери, яких американська компанія Flashpoint з «помірною впевненістю» ідентифікувала як групу APT28, зламали акаунти штабу. Нарешті, за два дні до голосування документи були оприлюднені під гештеґом MacronLeaks, який за три з половиною години набрав 47 000 твітів, а за добу — майже пів мільйона.

Але документи самі по собі виявились нецікавими. Нічого компроматного в них не було. Тому хакери вчинили характерно: перемішали справжні листи з підробленими. Серед фальшивок знайшлися повідомлення із натяками на те, що Макрон нібито вживав наркотики. Сам Макрон схарактеризував операцію так: «Автентичні документи змішали з підробленими, щоб посіяти сумніви та дезінформацію».

> *Саме в цьому і полягає ключова хитрість за шаблонами Геббельса. Коли в зливі є частина справжніх документів, аудиторія схильна вірити всьому масиву. Оскільки людина не перевіряє кожен файл окремо, а бачить «витік» — це і формує для неї загальну картину. Навіть якщо конкретна деталь, яка справила найбільше враження, виявилась підробленою.*

Операція провалилась: французькі виборці переобрали Макрона, — але стала шаблоном. Уже в грудні 2024 року перед президентськими виборами у Румунії російські хакери здійснили понад 85 000 атак на виборчі системи країни та злили скомпрометовані облікові дані на російських хакерських форумах. Проте це не дуже допомогло проросійському кандидату.

Кіберзброя і пропаганда: як вони діють разом?

Сучасні інформаційні операції майже ніколи не існують самостійно. Кампанії у соцмережах супроводжує кіберінфраструктура:

- хакерські групи,
- зливи даних,
- атаки на системи.

Класичний приклад — описана вище операція проти телеканалу «Україна 24» у березні 2022 року. Спочатку хакери зламали сайт і прямий ефір. Потім у рухомий рядок ефіру було вмонтовано deepfake із «капітуляцією» Зеленського. Паралельно той самий матеріал почали поширювати проросійські телеграм-канали. Три компоненти — кібератака, deepfake і мережа поширення — спрацювали як єдина система. Зв'язок між операцією Doppelganger і хакерською групою APT28, відомою як Fancy Bear і пов'язаною з ГРУ, підтвердили дослідники SentinelOne і ClearSky. У коді інфраструктури Doppelganger та у фішингових атаках APT28 виявили ідентичні фрагменти HTML і текстових шаблонів. За даними Державної служби спеціального зв'язку України, у 2024 році кількість кібератак на Україну зросла майже на 70 %, до 4 315 задокументованих інцидентів, спрямованих на критичну інфраструктуру, урядові сервіси, енергетику й оборонні підприємства. Тактики включали розповсюдження шкідливого програмного забезпечення, фішинг і компрометацію облікових записів.

У Молдові Росія поєднала кібервплив із прямим підкупом. Організація Evrazia, пов'язана з олігархом Іланом Шором, виплатила приблизно 130 000 молдовським громадянам загалом 15 мільйонів доларів за голосування «ні» на референдумі про вступ до ЄС у 2024 році. Паралельно із підкупом відбувалась масована дезінформаційна кампанія в соціальних мережах. Велика Британія внесла Evrazia у санкційні списки у квітні 2025 року. Заступник помічника Генерального секретаря НАТО Джеймс Аппатурай підбив підсумок тому, що спостерігають союзники. «Ми бачимо зростання схильності Росії до ризику, і я маю на увазі не ризик для них самих, а ризик для нас, для наших економік, для безпеки наших громадян», — сказав він.

Китай і Україна: тихий фронт

Якщо Росія атакує Україну в інформаційному просторі відкрито й агресивно, то Китай діє інакше. Пекін офіційно не підтримує вторгнення, але і не засуджує його. В інформаційному просторі це виражається у конкретних задокументованих діях.

За даними Служби безпеки України, в дні, що передували повномасштабному вторгненню у лютому 2022 року, кіберпідрозділ Народно-визвольної армії Китаю здійснив атаки на сотні сайтів українського Міністерства оборони та інших державних установ. Шпигунське та шкідливе програмне забезпечення, розроблене китайськими хакерами, використовувалось Росією в Україні як у перші місяці вторгнення, так і надалі.

У інформаційному вимірі Китай системно підсилює наративи, вигідні Росії. У березні 2022 року МЗС КНР і китайські державні медіа активно поширювали твердження Москви, нібито Україна розробляє біологічну зброю у лабораторіях, пов'язаних зі США. BBC Reality Check, ООН і Бюлетень учених-ядерників спростували ці заяви, назвавши їх цілковито безпідставними. Дослідники Foreign Policy Research Institute задокументували систематичний збіг у травні 2024 року: китайські медіа синхронно підсилювали ті самі теми про Україну і НАТО, що їх просувала російська пропаганда.

Причому часові збіги між публікаціями вказували на координацію, а не на випадковий збіг. Операція «Спамофлаж» також зачіпала тему України. Китайські акаунти, що маскувались під американських виборців і військовослужбовців, серед інших тем поширювали контент, що піддавав сумніву підтримку США щодо України. Мета цієї операції були не так змінити позицію Вашингтона напряму, як поглибити внутрішні американські суперечки, щоб Конгресу було складніше ухвалювати рішення про допомогу.

Нарешті, у 2025 році в межах ширшої конвергенції китайських і російських інформаційних операцій, яку задокументував Центр європейського аналізу, Китай перейшов до активнішого використання генеративного ШІ для виробництва та поширення контенту, що підриває довіру до НАТО. Дослідники CEPA встановили, що обидві країни переслідують спільну ціль: зображувати Захід як розколотий, лицемірний і нездатний ефективно підтримувати Україну.

> *Усі описані вище операції мають одну спільну рису, яка робить їх принципово новим явищем у сучасних конфліктах. Жодна з держав, що стоять за ними, офіційно не оголошувала війни та не несе юридичної відповідальності за скоєне. Росія заперечує причетність до Doppelganger. Китай заперечує «Спамофлаж».*

Атрибуція у цифровому просторі технічно складна: оператори використовують VPN, підставних осіб у третіх країнах, платіжні системи через криптовалюту і компанії-посередники. У справі Doppelganger ключова фігура, відома лише як «Константин», стверджувала американським слідчим, що є «просто обмінником», хоча більшість транзакцій відбувалась у московський робочий час.

Саме тут формується нова реальність сучасних конфліктів — когнітивні війни. НАТО визнало її офіційно, видавши у 2025 році окремий дослідницький звіт про когнітивну війну як самостійний домен ведення конфлікту поруч із традиційними — сушею, морем, повітрям, космосом і кіберпростором. Звіт встановлює, що сучасний конфлікт є дедалі більше поведінково орієнтованим і що вирішальна «місцевість» боїв — не географічна, а когнітивна: людське сприйняття, переконання і здатність ухвалювати рішення.

Кінця цій війні не буде?

Відео із «капітуляцією» Зеленського, яке з'явилось у березні 2022 року, давно видалено з платформ. Алгоритми спрацювали, журналісти спростували, сам Зеленський вийшов на камеру і довів, що не здається. Здавалось би, система захисту спрацювала. Але навіть спростований deepfake залишає слід. Людина, яка одного разу побачила відео з «капітуляцією», вже назавжди знає, що таке відео існувало. І наступного разу, коли вона побачить справжнє звернення Зеленського, у неї промайне думка: а раптом це знову підробка?

Саме на це і розраховують держави, що вдаються до цих інструментів. Не перемогти в суперечці та не довести свою правоту — просто зробити так, щоб громадяни інших країн більше ні в чому не були певні. Підтримка України коштує мільярди, тож чи варто витрачати їх на країну, чий президент, можливо, вже давно домовився з Москвою? НАТО захищає Європу, але хто сказав, що вона сама не є агресором? Може, Росія вимушено застосовує силу, щоб захистити від геноциду російськомовних і «маленьких розп'ятих хлопчиків»? Вибори відбуваються — але чи можна їм довіряти, бо ж раптом старі еліти все купили й про все домовились?

> *Росія і Китай обрали цей інструмент не випадково. Він дешевший за армію, не залишає уламків і не вимагає оголошення війни. Він діє там, де традиційна зброя безсила і куди вона не може дістати: всередині голів виборців, парламентських дебатів та союзів. І, що важливо, він використовує проти демократій їхню ж силу: відкритість інформаційного простору, свободу слова і довіру до медіа.*

І поки демократичні уряди ухвалюють санкції та видаляють домени, когнітивні операції адаптуються і продовжуються. Це не означає, що відповідати марно, але означає, що інформаційна війна не має лінії фронту і не закінчиться підписанням капітуляції. Вона триває щодня у стрічках новин, у рекомендаціях алгоритмів і у секундному коливанні перед тим, як натиснути «поділитись». Тож питання не в тому, чи особисто ви вже стали мішенню в цій війні. Питання в тому, чи знаєте ви про це та чи готові цьому протидіяти.

Автор: Віктор Таран, керівник Центру підготовки операторів БПЛА «Крук»

Джерело: ТИЖДЕНЬ

Like
Tweet

Новини партнерів

YOU MAY ALSO LIKE...