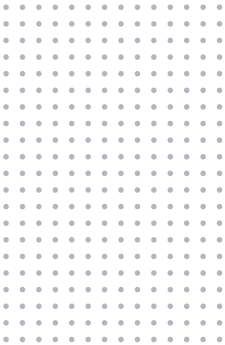
United Nations
Interregional Crime and Justice
Research Institute

Посібник з боротьби з дезінформацією на тему РХБЯ загрози



Посібник з боротьби з дезінформацією на тему РХБЯ загрози

Відмова від відповідальності

Судження, висновки та рекомендації, викладені в цьому документі, належать його авторам і не обов'язково є відображенням точки зору Міжрегіонального науково-дослідницького інституту Організації Об'єднаних Націй з питань злочинності й правосуддя (ЮНІКРІ) або будь-якої іншої залученої державної, регіональної або міжнародної організації. Вміст публікації може цитуватися або відтворюватися за умови зазначення джерела.

Ця публікація була підготована за фінансової підтримки Федерального бюро розслідування (ФБР) Сполучених Штатів Америки. Її вміст не обов'язково є відображенням точки зору ФБР.

Подяки

Цей посібник підготували пан Франческо Мареллі, керівник відділу боротьби з ризиками радіоактивної, хімічної, біологічної та ядерної небезпеки ЮНІКРІ та пані Маріана Діас Гарсіа, співробітник ЮНІКРІ. ЮНІСРІ хоче подякувати пані Кеті Керрол, пану Луці Чіслагі Ланца та пані Марті Зелоні за їхні дослідження в царині дезінформації.

Авторське право

Для отримання докладної інформації звертайтеся за адресою:

UNICRI, Viale Maestri del Lavoro, 10, 10127 Torino – Italy (Італія)
Тел.: + 39 011-6537 111 / Факс: + 39 011-6313 368.
Вебсайт: www.unicri.org
Електронна пошта: unicri.publicinfo@un.org

Вступне слово

Дезінформація на тему хімічної, біологічної, радіоактивної та ядерної (РХБЯ) загрози може бути дуже шкідливою і мати жахливі наслідки. Ця її властивість стала ще більш актуальною сьогодні, коли інформація є легкодоступною й нерозважливо поширюється без перевірки її достовірності.

Підроблена або шахрайська інформація про надзвичайні ситуації, пов'язані з РХБЯ чинниками, як-от терористичні атака або пандемії, може вводити в оману уряди та міжнародні організації, знецінювати заходи реагування, призводити до неправильного спрямування й марнування ресурсів та викликати паніку серед населення. Хибна інформація, до якої також належать теорії змови, може також підсилювати страх та тривогу серед цільових категорій населення, якщо вона, наприклад, повідомляє, що подія, пов'язана з РХБЯ загрозою, вийшла з-під контролю. Вона навіть може спричинити суспільний хаос, якщо частина населення повірить, що подія, пов'язана з РХБЯ загрозою, була навмисно й свідомо організована та є частиною зловмисного плану. Хибна інформація може також використовуватися для радикалізації й втягнення несвідомих осіб у терористичну діяльність, оскільки вона може підсилювати страх й підігрівати ненависть серед різних категорій населення.

У цьому *Посібнику з боротьби з дезінформацією на тему РХБЯ загрози* описані різні методи виявлення, аналізу та викриття інформації, яка має умисний оманливий характер. *Посібник* на конкретних прикладах знайомить читачів з інструментами, які будуть потрібні їм для того, щоб не стати жертвою дезінформації про РХБЯ загрозу.

ЮНІКРІ, відповідно до повноважень інституту, які полягають в сприянні правосуддю й законності для підтримки миру та довготривалого розвитку, різними шляхами намагається впоратися із загрозою дезінформації на тему РХБЯ небезпеки.

Починаючи з 2020 року ЮНІКРІ проводить моніторинг зловмисного використання соціальних мереж. У листопаді 2020 році ЮНІКРІ опублікував звіт *Stop the virus of disinformation* («Зупинимо вірус дезінформації»), в якому описувалось, як зловмисники під час пандемії COVID-19 скористалися нагодою, щоб піддати сумніву ефективність та підірвати довіру до заходів реагування, застосованих урядами країн. ЮНІКРІ також проаналізував наявні технічні засоби виявлення та викриття хибної інформації (*як-от* великі дані, інструменти й платформи штучного інтелекту, мобільні додатки та чатботи тощо), щоб зрозуміти переваги та недоліки кожного з них в короткостроковій і довгостроковій перспективі.

У 2021 році ЮНІКРІ разом з Всесвітньою організацією охорони здоров'я (ВООЗ) і за сприяння Федерального бюро розслідувань (ФБР) почали розробляти стратегію поліпшення поінформованості про дезінформацію на тему РХБЯ загрози і проводити навчання з представниками країн-учасників. Цей *Посібник з боротьби з дезінформацією на тему РХБЯ загрози* є результатом такого практичного підходу. *Посібник*, який призначено для фізичних осіб та організацій, що працюють над пом'якшенням ризиків РХБЯ загрози на різних рівнях, забезпечує виконавців знаннями, які допоможуть їм ефективно аналізувати, розуміти дезінформацію на тему РХБЯ загрози в засобах масової інформації та на платформах соціальних мереж та ефективно реагувати на неї.

Я сподіваюсь, що цей *Посібник* поглибить знання та поінформованість про цю складну проблему й сприятиме щоденному використанню ефективних заходів з протидії зловмисному використанню соціальних мереж та боротьбі з ним. Робота з приборкання дезінформації та невірної інформації на тему РХБЯ загрози, а також з їхніми небажаними наслідками сприяють створенню більш безпечного світу для усіх нас.

Антоніа Марі Де Мео
Директор
ЮНІКРІ

Зміст

1

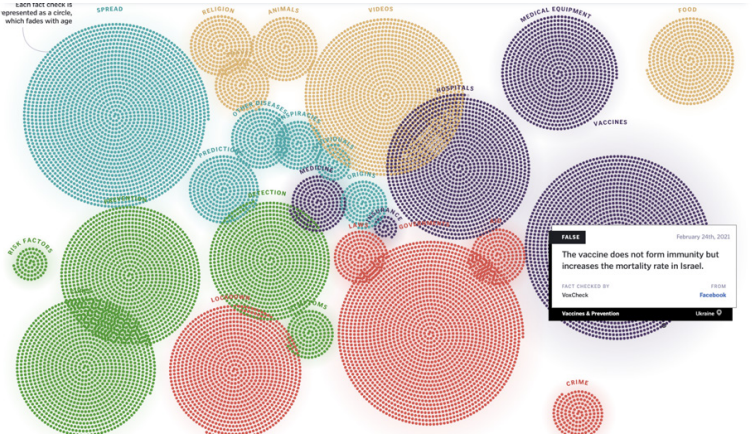
Вступ

Дезінформація на тему радіоактивної, хімічної, біологічної, та ядерної загрози (РХБЯ) — це така інформація, в яку навмисно включено оманливі або хибні відомості про РХБЯ загрозу, що потенційно може заподіяти шкоду урядам, міжнародним організаціям, науковій та академічній спільноті, промисловості й широким верствам населення.[1]

Дезінформація на тему РХБЯ загрози в соціальних мережах в останні роки перетворилась на серйозну проблему. Такому розвитку подій посприяли три основних фактори. Перший фактор — це **особлива природа РХБЯ загрози**, яка пов'язана з небезпечними і часто невидимими речовинами, що робить її дуже зручною темою для нагнітання страху та тривоги через соціальні мережі та ЗМІ. У якості прикладу можна навести хвилю дезінформації, пов'язаної пандемією коронавірусу (COVID-19), яка розповсюдилася одразу ж після того, як

1 Невірна інформація — це інформація, яка є хибною, але яка не створювалася для заподіяння шкоди. Натомість дезінформацією вважається така інформація, яка є хибною й яка навмисно створена для заподіяння шкоди особі, соціальній групі, організації або країні. Див. ЮНЕСКО (2018 р.). *Journalism, 'fake news' and disinformation. Посібник з навчання та інструктажу журналістів.* Доступно в Інтернеті. Також див. Fallis, D. (2015 р.). What Is Disinformation? *Library Trends*, 63, 401 - 426.

Муніципальна комісія з охорони здоров'я м. Ухань, КНР, повідомила про низку випадків пневмонії 31 грудня 2019 року.[2] Хвиля дезінформації почалася з безпідставних та шкідливих теорій змови щодо походження вірусу (наприклад, що COVID-19 — це біологічна зброя, яку було створено урядами та фармакологічною промисловістю, або що COVID-19 був містифікацією, метою якої було поневолення людей і встановлення диктатури) і незабаром поширилася на теми шляхів передавання вірусу, методів лікування, профілактики та терапії, існування захворювання як такого і, нарешті, ефективності та наслідків втручань та рішень, до яких вдаються влада та установи.[3]



Малюнок 1: На діаграмі показані різні тематичні галузі, у яких альянс #CoronaVirusFacts виявив хибну інформацію.
Джерело: Poynter (2022 р.). Fighting the Infodemic: #CoronaVirusFacts Alliance. Poynter. Доступно в Інтернеті

2 ВООЗ використовує термін «інфодемія», під яким мається на увазі надмірна кількість точної й неточної інформації, яка спостерігається під час епідемії, що поширюється цифровими та фізичними інформаційними системами, ускладнюючи пошук достовірних та надійних джерел. Див. ВООЗ (2020 р.). *Спеціальна технічна консультація ВООЗ Managing the COVID-19 infodemic: call for action*. Доступно в Інтернеті.

3 Для отримання докладної інформації див.: ЮНІКРІ (2020 р.). *Stop the virus of disinformation: the risk of malicious use of social media during COVID-19 and the technology options to fight it*. Доступно в Інтернеті.

Другим фактором є те, що **нові цифрові платформи** створили нові форми комунікації й посилили зв'язок між мільйонами користувачів. Всесвітній обмін контентом у соціальних мережах в реальному часі змінив звичний спосіб споживання інформації громадянами. Простий та швидкий доступ до великої кількості даних та інформації дозволив громадянам поглибити їхні знання та уможливив появу нових журналістських практик. Щоправда, як це часто трапляється з технологічними проривами, одночасно з розвитком платформ соціальних мереж також постають нові виклики. Одним з таких викликів є розповсюдження хибної інформації й теорій змови. Хоча невірна інформація й дезінформація не є новими явищами в історії людства, зараз платформи соціальних мереж використовуються зловмисниками, які навмисно фабрикують та розповсюджують хибну інформацію, щоб заподіяти шкоду фізичним особам, соціальним групам, організаціям або країнам.[4]

Третім фактором є роль агресивних **недержавних суб'єктів,** особливо у соціальних мережах. Хоча в минулому дезінформація на тему РХБЯ часто була частиною таємних операцій, що проводилися урядами країн з метою вплинути на думку й дії фізичних осіб та країн-учасників (дезінформаційні кампанії й дезінформаційна пом'якшувальна тактика), потягом останніх років терористи, крайні екстремісти й організовані злочинні групи продемонстрували здатність використовувати у злочинних цілях вразливі аспекти в екосистемі соціальних мереж, розповсюджуючи теорії змови та маніпулюючи людьми за допомогою РХБЯ загроз. Агресивні недержавні суб'єкти подекуди можуть діяти як добровільні або вимушені представники урядів, але їхнє безпосереднє залучення

4 Posetti, J., & Matthews, A. (2018 p.). A short guide to the history of 'fake news' and disinformation: A new ICFJ learning module. *Міжнародний центр для журналістів*. Доступно в Інтернеті.

стало новою змінною, яка значно підсилює поширення дезінформації.

Сьогодні дезінформація, пов'язана з РХБЯ загрозами, здатна заподіяти серйозну політичну, фінансову та фізичну шкоду урядам, міжнародним організаціям, науковій та академічній спільноті, промисловості й широким верствам населення. Зараз кількість осіб та організацій, на яких спрямована дезінформація про РХБЯ загрози, є великою як ніколи. Жертвами вірусних мережевих, а деколи й фізичних атак, стали майже всі зацікавлені особи, які працюють в галузі пом'якшення РХБЯ ризиків, у тому числі особи, які визначають політики, керівники установ, пов'язаних з РХБЯ, дослідники з університетів та дослідницьких центрів, прес-секретарі різних урядових департаментів, зокрема сектору охорони здоров'я, журналісти та представники міжнародних організацій. У цьому сенсі дезінформація на тему РХБЯ стала серйозним новим викликом.

Боротьба з дезінформацією є непростим завданням. Успішна стратегія вимагає комбінації різних заходів з боку уряду, освітніх установ, медіа-індустрії та компаній сектору інформаційних технологій. Це передбачає моніторинг дезінформації в соціальних мережах, викриття хибної інформації та теорій змови, інвестування в технічні засоби ідентифікації хибних новин, навчання на тему медійної грамотності, взяття на озброєння належних правових інструментів, не порушуючи базових прав та свобод людини, й навчання правоохоронних органів та органів прокуратури на тему розслідування та переслідування за злочини, пов'язані з дезінформацією.[5]

Були вивчені й розроблені різні методи боротьби з дезінформацією, у тому числі методи передбачення

5 Докладну інформацію про курси та посібники для покращення навичок медіаграмотності див. у: навчальних ресурсах First Draft и матеріалах, які розповсюджує Міжнародний центр для журналістів (ICFJ). Доступно в Інтернеті.

дезінформації (випереджувальне викриття), виявлення та аналізу дезінформації й ефективного реагування на дезінформацію та демонстрації хибності інформації або теорії змови (викриття).

Цей посібник здебільшого присвячено методам викриття. Його було створено для фізичних осіб та організацій, що працюють над пом'якшенням ризиків РХБЯ загрози на різних рівнях (комунікаційний, рівень прийняття рішень, управлінський, операційний, технічний тощо) які наражаються або можуть наражатися на вплив дезінформації та які є її ціллю. Посібник розглядає проблему у двох площинах: по-перше це розуміння проблеми дезінформації на тему РХБЯ загрози в соціальних мережах, а по-друге — створення багажу знань, які допоможуть ефективно попереджати й реагувати на дезінформацію у ЗМІ та на платформах соціальних мереж, звертаючи особливу увагу на методи викриття хибної інформації.[6]

Цей посібник поділено на два розділи. У першій частині, яку присвячено аналізу проблеми, подається опис стратегічних цілей дезінформації на тему РХБЯ загрози та методів, які використовуються для маніпулювання аудиторією соціальних мереж. У другій частині визначаються та описуються методи ефективної демонстрації хибності тієї чи іншої ідеї, оповіді або теорії. Також вона містить практичні поради щодо аналізу ситуацій, в якій особа або організація наражаються на вплив дезінформації, і щодо того, коли варто відповідати на хибні звинувачення, а коли краще залишити їх без уваги.

Цей посібник містить декілька практичних прикладів методів дезінформування аудиторії або викриття хибної

6 Цей документ не є посібником для професіональних журналістів та фактчекерів, чия робота полягає в забезпеченні достовірності й об'єктивності джерела новин або інформації. ООН опублікувала посібники для цих категорій осіб, як-от посібник, випущений спільними зусиллями ЮНЕСКО і Фонду «Ірондель», який називається *Журналістика, фальшиві новини та дезінформація. Посібник з навчання та інструктажу журналістів*.

інформації. Щоб створити цей документ, ЮНІКРІ здійснив моніторинг кількох платформ соціальних мереж, звертаючи особливу увагу на роль агресивних недержавних суб'єктів. ЮНІКРІ розглядає три основні типи недержавних суб'єктів. До першої належать крайні екстремісти, зокрема правоекстремістські групи (їх ще називають «крайні праві»). Ці групи не є чітко окресленим та легко ідентифікованим рухом — вони, натомість, як зазначає виконавча дирекція Антитерористичного комітету Організації Об'єднаних Націй, є «динамічним, складним та переплетеним соціальним оточенням, що складається з окремих осіб, груп та рухів (які діють онлайн та офлайн), що сповідують різні, але споріднені ідеології та яких часто об'єднують ненависть та расизм, спрямовані на меншини, ксенофобія, ісламофобія або антисемітизм».[7] Зловмисне використання соціальних мереж правими екстремістам не є новиною — деякі з цих груп намагалися використовувати Інтернет для поширення ненависті ще у 90-х роках.[8] З початком спалаху захворюваності на COVID-19 праві екстремісти поширили їхню приступність в Інтернеті й вдались до ксенофобських, ісламофобських або антисемітських наративів для поширення теорій змови про походження COVID-19 та можливі засоби його лікування.[9]

Друга група недержавних суб'єктів представлена терористичними організаціями, зокрема тими з них, які пов'язані з Ісламською державою Іраку та Леванта (ІДІЛ) та

7 Виконавча дирекція антитерористичного комітету Організації Об'єднаних Націй (CTED) (2020 р.). *Trends Alert "Member States concerned by the growing and increasingly transnational threat of extreme right-wing terrorism"*, стор. 2.

8 Conway, M., Scrivens, R. & Macnair, L. (2019 р.). Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends. *ICCT*. Доступно в Інтернеті.

9 ЮНІКРІ (2020 р.). *Stop the virus of disinformation: the risk of malicious use of social media during COVID-19 and the technology options to fight it* Доступно в Інтернеті. Також див. Diaz Garcia, M. (2021 р.). Infodemic: Right-wing extremist groups and the risk of disinformation during the COVID-19 pandemic. *Журнал Freedom from Fear (F3)*. Доступно в Інтернеті.

Аль-Каїдою.[10] Онлайн-активність цих груп проаналізована в багатьох літературних джерелах.[11] Наприклад, глобальна мережа прихильників ІДІЛ (яких вони називають *munasireen*) використовують Telegram в цілях операційної діяльності, як-от розміщення контенту, розширення аудиторії, безпечний зв'язок та фінансування.[12]

Організовані злочинні групи представляють третю групу.[13] Зловмисне використання соціальних мереж кримінальними угрупуваннями, яке, зокрема, полягає в пропаганді їхньої злочинної діяльності в регіонах їхньої активності та в залякуванні й демотивації угрупувань-конкурентів, також практикується досить давно. Щоправда після пандемії COVID-19 деякі з них проявляють велику активність, маніпулюючи їхньою аудиторією й просуваючи власний позитивний імідж надійної «організації».

10 Комітет Ради Безпеки, який називається Санкційний комітет з питань ІДІЛ та Аль-Каїди та пов'язаних з ними фізичних осіб, груп, організацій та юридичних осіб, відповідно до постанов № 1267 (1999 р.), № 1989 (2011 р.) та № 2253 (2015 р.) регулярно оновлює санкційний список фізичних та юридичних осіб, чиї активи підлягають заморожуванню, яким забороняється в'їзд у певні країни та проти яких застосовується ембарго, передбачене пунктом 1 постанови Ради Безпеки № 2368 (2017 р.), ратифіковане відповідно до глави VII Статуту Організації Об'єднаних Націй. Станом на 16 липня 2020 року доступний в Інтернеті санкційний список налічував 261 фізичних осіб та 89 юридичних особи. У цілях цього звіту список використовувався як головне джерело інформації для ідентифікації організацій, які належать до цієї другої групи агресивних недержавних суб'єктів.

11 Clifford, B., & Powell, H. (2019 р.). Encrypted Extremism Inside the English-Speaking Islamic State Ecosystem on Telegram. *Програма на тему екстремізму Університету Джорда Вашингтона*. Доступно в Інтернеті. Waters, G., & Postings, R. (2018 р.). Spiders of the Caliphate: Mapping the Islamic State's Global Support Network on Facebook. *Антиекстремістський проєкт*. Доступно в Інтернеті. Kruglova, A. (2022 р.). Terrorist Recruitment, Propaganda and Branding Selling Terror Online. *Routledge*.

12 Clifford, B., & Powell, H. (2019 р.). Encrypted Extremism Inside the English-Speaking Islamic State Ecosystem on Telegram. *Програма на тему екстремізму Університету Джорда Вашингтона*. Доступно в Інтернеті.

13 Одним з визначень організованої злочинності є «злочинна організація, яка існує постійно та вдається до раціональних дій, спрямованих на збагачення від незаконної діяльності, яка часто користується великим суспільним попитом. Безперервність її існування забезпечується шляхом підкупу державних службовців та залякуванням, погрозами або застосуванням сили для захисту її діяльності». Див. УНЗ ООН (2018 р.). Defining organized crime. *УНЗ ООН*. Доступно в Інтернеті.


2

Дезінформація на тему РХБЯ загрози

У цій главі аналізуються стратегічні цілі дезінформації на тему РХБЯ загрози та ілюструються деякі основні ефективні методи дезінформації.

2.1 Що є стратегічними цілями дезінформації на тему РХБЯ загрози?

Дезінформація на тему РХБЯ загрози може переслідувати три різних стратегічних цілі:

1. підрив репутації та довіри до організацій, які працюють у сфері пом'якшення ризиків РХБЯ;
2. спричинення страху, ненависті та жорстокості шляхом поширення радикальних наративів;
3. отримання фінансової вигоди.

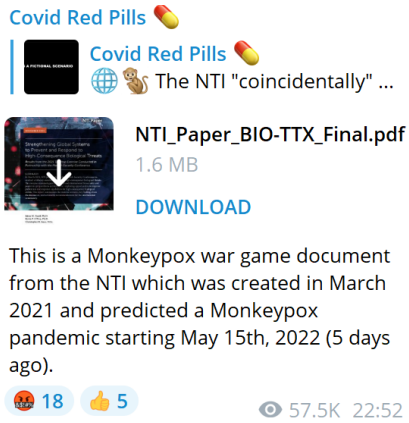
2.1.1 Підрив репутації та довіри до організацій, які працюють у сфері пом'якшення ризиків РХБЯ

Першою стратегічною метою дезінформації в соціальних мережах на тему РХБЯ загрози є підрив репутації та довіри до організацій, які працюють у сфері пом'якшення ризиків РХБЯ, до числа яких належать державні та міжурядові організації, дослідницькі центри, некомерційні організації, фармацевтичні компанії тощо. Можливим шляхом досягнення цієї мети є фабрикування й поширення неправдивих відомостей, які звинувачують ці організації в брехні щодо причини надзвичайної ситуації, пов'язаної з хімічно, біологічною, радіоактивною або ядерною небезпекою. Наприклад, у травні 2022 року у соціальних мережах було поширено документ «Ініціативи зі скорочення ядерної загрози» (NTI), у якому підбивалися підсумки проведеного в 2021 році імітаційного моделювання, який видавався за «доказ» того, що спалах віспи мавп був спланованою акцією (див. ілюстрації 2 і 3).

Імітаційне моделювання із вигаданим сценарієм широко використовується для перевірки готовності урядів та міжурядових організацій до пандемій. Цікавим є те, що імітаційне моделювання NTI насправді проводилося й розглядало можливість терористичного акту з використанням нетипового штаму вірусу віспи мавп, але це не доводить, що спалах захворювання в 2022 році був передбачуваною й спланованою акцією. Як пояснює NTI, «поточний спалах захворюваності на віспу мавп у кількох країнах є звичайним збігом обставин».[14]

14 Перевірка фактів Reuters (24 травня 2022р.). Fact Check-No evidence that 2021 Nuclear Threat Initiative exercise proves monkeypox outbreak was planned. *Reuters*. Доступно в Інтернеті.

Ілюстрація 2: Титульна сторінка доповіді NTI про імітаційне моделювання, яку було використано в якості фальшивого «доказу» спланованості спалаху віспи мавп. **Джерело**: Посилання на оригінальний документ: Yassif, J. M., O'Prey, K.P., Isaac, C. R. (November 2021), Strengthening Global Systems to Prevent and Respond to High-Consequence Biological Threats, доповідь NTI, доступно в Інтернеті.



Ілюстрація 3: Приклад допису в соціальній мережі, в якому йдеться про те, що віспу мавп було сплановано.
Джерело: Telegram, канал Covid Red Pills, допис опубліковано 20 травня 2022 р.

Онлайн-дезінформація також може намагатися **знецінити заходи, які вживають органи охорони здоров'я, та перешкодити міжнародному співробітництву** під час екстреної ситуації, пов'язаної із РХБЯ. Ілюстрація 4, опублікована на каналі соціальної мережі у вересні 2021 року, є прикладом спроби неблагонаміреного введення населення в оману щодо кампанії вакцинації від COVID-19. На зображенні лікар з пістолетом, націленим в голову пацієнтки, каже, що «вакцина є безпечною та ефективною». Зображення є інсинуацією, відповідно до якої фармацевтичні компанії (т. з. «фарма») змушують лікаря брехати пацієнту для втілення міжнародної змови, яка називається «Порядок денний на XXI століття». Порядок денний на XXI століття — це план дій, спрямований на подолання викликів довкілля та розвитку, який було ухвалено урядами 178 країн на Конференції Організації Об'єднаних Націй з питань довкілля та розвитку (ЮНСЕД), проведеній в Ріо-де-Жанейро, Бразилія, 13 червня 1992 року. Але праві екстремісти у їхніх наративах подають Порядок денний на XXI століття як секретний план, метою якого є скоротити населення Землі й зробити його меншим за 500 мільйонів, використовуючи вакцин від COVID-19 як інструмент досягнення цієї мети.

Насправді ж жодного зв'язку між Порядком денним на XXI століття та COVID-19 не існує. Порядок денний на XXI століття рекомендує розробляти нові вакцини для профілактики захворювань, і в ньому немає жодних посилань на вакцини від COVID-19, оскільки його було написано в 1992 році. Тобто цей малюнок мав зловмисну мету посіяти сумніви щодо ефективності вакцинації від COVID-19, безпідставно звинувачуючи її у зв'язку з уявним таємним планом Організації Об'єднаних Націй щодо регулювання населення світу.

Ілюстрація 4: Приклад хибних звинувачень на адресу Порядку денного на XXI століття та Організації Об'єднаних Націй.
Джерело: Telegram, канал COVID-19 Agenda, допис від 15 вересня 2021 року.

Організовані злочинні угрупування також можуть вводити населення в оману щодо надзвичайних ситуацій пов'язаних з РХБЯ чинниками, заявляючи, що вони, на відміну від уряду, «контролюють» надзвичайну ситуацію. Наприклад під час пандемії COVID-19 мексиканські наркокартелі поширювали на платформах соціальних мереж фотографії та відео, на яких озброєні члени угрупувань роздавали коробки та пакети з продуктами, медикаментами, мийними засобами та іграшками (див. ілюстрацію 5). У деяких випадках на коробки були нанесені емблеми або зображення картелю (див. ілюстрацію 6). Деякі кримінальні угрупування навіть намагалися взяти на себе роль уряду та офіційних органів

в регіонах їхньої присутності, впроваджуючи суворі заходи з охорони здоров'я, як-от локдауни, або безпосередньо забезпечуючи населення антисептичними засобами та продуктами.[15]

Наміром злочинних угрупувань було применшити роль уряду й афішувати власний позитивний імідж як структури, яка під час пандемії здатна замінити органи охорони здоров'я й відповідальних політичних діячів. У такий спосіб організованізлочинніугрупуванняможутьвикористовувати надзвичайну ситуацію, пов'язану з РХБЯ загрозою, щоб створювати хибне уявлення, що вони є «державою всередині держави», яка має владу для контролю над територіями, що ґрунтується на суспільному схваленні. На жаль, основною метою цих злочинних угрупувань є не захист місцевого населення у надзвичайній ситуації, пов'язаній з РХБЯ загрозою, а захист кримінального бізнесу й збереження соціальної бази на у відповідних регіонах. Вони побоюються, що масштабна епідемічна криза може призвести до активного залучення правоохоронних органів або збройних сил в регіонах, де діють злочинці, що наразить на небезпеку їхню незаконну діяльність.

Ілюстрація 5: Приклади відео, які поширював в TikTokКартель нового покоління Халіско (CJNG) під час роздачі пакетів з продуктами в Халіско, Мексика (Infobae, 2020 р.). **Джерело**: Infobae (10 травня 2020 р.). El narco en TikTok: el CJNG desafía al gobierno y alardea entregando despensas. *Infobae*. Доступно в Інтернеті.

15 Dudley, S. & McDermott, J. (2020 р.). GameChangers 2020: how organized crime survived the pandemic. *InSight Crime*. Доступно в Інтернеті.

Ілюстрація 6: Картель Гольфо роздає пакунки з продуктами під час пандемії COVID-19.
Джерело: Infobae (20 квітня 2020 р.). Narcos aprovechan coronavirus en México para repartir despensas y pelear territorio. *Infobae*. Доступно в Інтернеті.

Дезінформація на тему РХБЯ загроз також може мати форму розіграшу. Наприклад, в травні 2005 року уряд Нової Зеландії вимушено прореагував на лист, в якому зловмисники стверджували, що вони начебто розповсюдили на острові Уаїхеке вірус ящуру. Хоча уряд і зрозумів, що лист є розіграшем, було вжито всіх необхідних заходів для захисту інтересів Нової Зеландії та добробуту населення, у тому числі впровадження карантину на острові й 14-денного нагляду за вразливими тваринами.[16] У подібному випадку дезінформація може призводити до значних фінансових витрат, змушуючи уряд мобілізувати ресурси та впроваджувати засоби екстреного реагування на захворювання.

16 Mackereth, G. F. & Stone, M.A.B. (2006 р). Veterinary intelligence in response to a foot-and-mouth disease hoax on Waiheke Island, New Zealand.дія. *Матеріали 11-го Міжнародного симпозіуму з ветеринарної епідеміології та економіки, 2006 р.*

2.1.2 Радикалізація, рекрутинг та підбурювання до ненависті та жорстокості

Іншою стратегічною метою дезінформації на теми РХБЯ загроз є підсилення страху та тривоги серед населення й підбурювання до жорстокості, особливо під час надзвичайної ситуації, пов'язаної з РХБЯ. На ілюстраціях 7 та 8 показані зображення, опубліковані на крайніх правих каналах, метою яких було підбурювання до ненависті й агресію, спрямованої на вакцини та їхніх виробників під час пандемії COVID-19.

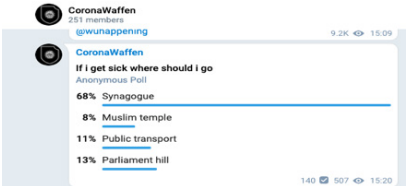
Ілюстрація 7: Приклад допису, який пропагує агресію, спрямовану проти влади та фармацевтичних компаній, що виробляють вакцини.
Джерело: Gab, канал «Nazi Society», допис від 26 листопада 2021 року.

Ілюстрація 8: Приклад допису, який пропагує агресію, спрямовану проти фармацевтичних компаній, які випускають вакцини.
Джерело: Gab, канал «Nazi Society», допис від 4 жовтня 2021 року.

У березні 2020 року Федеральне бюро розслідування (ФБР) повідомило, що члени екстремістських груп закликають один одного поширювати COVID-19, якщо вони на нього захворіють, за допомогою рідин організму та особистого контакту (див. ілюстрації 9 та 10).[17] Це повідомлення поширювалося на багатьох онлайн-каналах і його було адаптовано для різних аудиторій.[18]

17 Margolin, J. (2020 р.). White supremacists encouraging their members to spread coronavirus to cops, Jews, FBI says. *ABC News*. Доступно в Інтернеті.
18 ЮНІКРІ (2020 р.). *Stop the virus of disinformation: the risk of malicious use of social media during COVID-19 and the technology options to fight it*. Доступно в Інтернеті.

Ілюстрація 9: Приклад допису на крайньому правому каналі, який пропагує навмисне поширення COVID-19. **Джерело**: Telegram, канал CoronaWaffen, опубліковано в травні 2020 р.



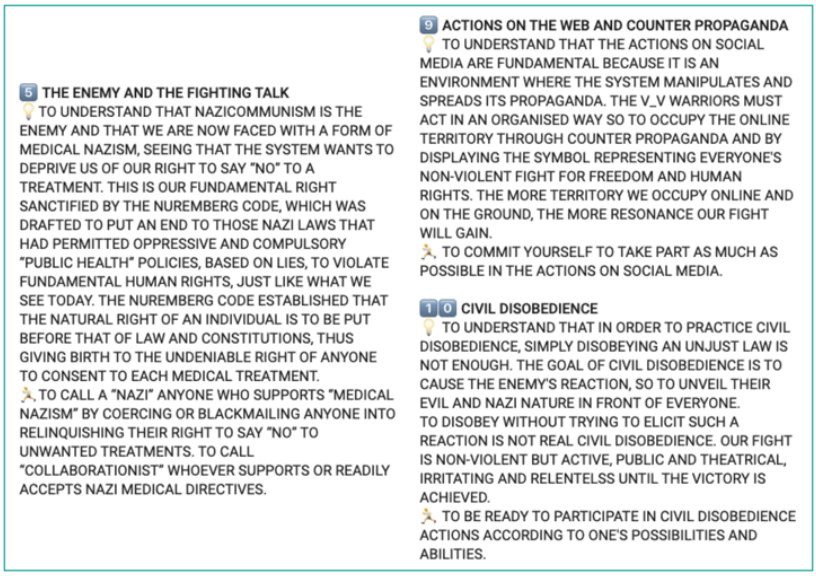
Ілюстрація 10: Приклад допису на крайньому правому каналі, який пропагує навмисне поширення COVID-19. **Джерело**: Telegram, канал «CoronaWaffen», опубліковано в травні 2020 р.

Посилення страху та ненависті під час надзвичайних ситуацій, пов'язаних із РХБЯ чинниками, також може допомогти радикалізувати й набирати нових членів. Наприклад, групи, пов'язані з ІДІЛ та Аль-Каїдою, поширювали теорії змови, які стверджували, що вірус є «солдатом Аллаха», який карає невірних та ворогів ісламу. ІДІЛ та Аль-Каїда заявляли, що вірус є проявом господнього гніву, спрямованого на Захід.[19] Аналогічно, Харакат аш-Шабаб заявив, що короновірусну хворобу було поширено «хрестоносцями, які завоювали країну, та країнами невірних, які їх підтримують».[20] Взагалі, висловлюючи думку про те, що короновірус є формою божественного втручання, ці екстремістські угрупування сподіваються радикалізувати та залучити до свої лав нових членів, які можуть сприйняти короновірус як «доказ» того, що їхні дії схвалено Аллахом.

19 Meek, J. G. (2 квітня 2020 р.). Terrorist groups spin COVID-19 as God's 'smallest soldier' attacking West. *ABCNews*. Доступно в Інтернеті.

20 BBC News (1 березня 2020 р.). Coronavirus: Fighting al-Shabab propaganda in Somalia. *BBC*. Доступно в Інтернеті.

На ілюстрації 11 показано деякі із засадничих принципів руху Viral Vendetta (V_V). Рух V_V зародився в Італії та Франції під час пандемії COVID-19. Учасники руху проявляли чималу активність, поширюючи теорії змови у соціальних мережах, заявляючи, що вакцини й інші заходи боротьби з COVID-19 є новою формою «медичного нацизму». Засадничі принципи, наведені на ілюстрації, свідчать, що цей рух намагається зацікавити, а потім і залучити до своїх лав послідовників, шляхом навіювання ідей (як правило догматичних), які не слід піддавати сумніву, та наводячи факти, які не слід піддавати критичному оцінюванню.[21]



Ілюстрація 11: Приклад трьох з 12 засадничих принципів V_V, які було перекладено різними мовами й поширено в Telegram.
Джерело: Graphika (2021 р.). *Viral Vendetta. Inside the conspiratorial movement waging a cross-platform 'psychological warfare' campaign against Covid-19 vaccine advocates*. Доступно в Інтернеті.

21 В рамках своєї онлайн-діяльності рух V_V організовував мережеві атаки на журналістів, працівників охорони здоров'я та державних службовців і спланованe голосування проти дописів в соціальних мережах на підтримку медичних заходів із боротьби з COVID-19. Докладну інформацію див. у: Graphika (2021 р.). *Viral Vendetta. Inside the conspiratorial movement waging a cross-platform 'psychological warfare' campaign against Covid-19 vaccine advocates*. Доступно в Інтернеті.

Просякнуті ненавистю промови та зображення на платформах соціальних мереж можуть бути передвісниками справжнього насильства. Під час пандемії COVID-19 було зареєстровано декілька випадків насильства, викликаних людиноненависницькою риторикою. До проявів насильства належать напади на медичні заклади, які лікують пацієнтів, центри вакцинації, ланцюги постачання лікарень, об'єкти інфраструктури, які начебто використовуються для поширення вірусу (наприклад, вежі мобільних мереж 5G) і осіб, які вважаються впливовими прихильників обмежувальних заходів, і всі вони пов'язані з пандемією COVID-19.

Наприклад, в березні 2020 року в Міссурі агенти ФБР ліквідували підозрюваного у внутрішньому тероризмі чоловіка. Як було заявлено, підозрюваний намагався здійснити терористичний акт в лікарні, в якій проходили лікування хворі на COVID-19, за допомогою саморобного вибухового пристрою. Відповідно до судових матеріалів, він був незадоволений тим, як уряд реагує на кризу COVID-19, і мотивувався расовими, релігійними та антиурядовими настроями, які підігрівалися його зв'язками з двома угрупуваннями прихильників верховенства білої раси — Націонал-соціалістичним рухом (NSM) та Vorherrschaft Division (VSD) — у додатку Telegram (див. ілюстрацію 12). Він був одним із адміністраторів Telegram чату, де заявляв, що уряд використовує пандемію COVID-19 в якості «приводу для знищення нашого народу».[22] Він також заявляв про його намір експлуатувати тему пандемії та підвищену уваги засобів масової інформації до сектору охорони здоров'я, оскільки це відкриває унікальні можливості.[23]

22 Martin, N. R. (2020 р.). Heartland terror. *The Informant*. Доступно в Інтернеті.

23 Levine, M. (2020 р.). FBI learned of coronavirus-inspired bomb plotter through radicalized US Army soldier. *ABC News*. Доступно в Інтернеті.

Werwolfe 84 07:31

If you don't think this whole thing was engineered by Jews as a power grab here is more proof of their plans

Jews have been playing the long game we are the only ones standing in their way 07:32

Ілюстрація 12: Це останнє повідомлення, яке екстреміст опублікував у Telegram на тему пандемії COVID-19.

Джерело: Martin, N. R. (2020 р.). Heartland terror. *The Informant*. Доступно в Інтернеті.

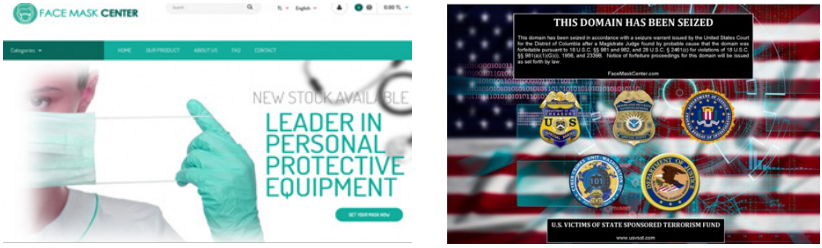
Просякнуті ненавистю промови й дезінформація також стали передвісниками спроб екстремістів інфільтруватися в лави учасників протестів проти заходів, пов'язаних з COVID-19, щоб набирати серед них нових членів та підбурювати до насильства. Наприклад, в Італії крайні праві екстремісти інфільтрувалися в лави учасників демонстрації, яка проводилася в столиці країни Римі 9 жовтня 2021 року проти вакцинації та системи «зелених перепусток», відповідно до якої громадяни повинні були пред'являти електронне посвідчення про вакцинацію від COVID-19 або наявність імунітету. У випадку, який розгадається, група демонстрантів, очолювана членами неофашистської організації Forza Nuova, відділилася від демонстрації, вступила в сутичку з поліцією й увірвалася в будівлю центрального офісу головної італійської організації профспілок, заподіявши значну шкоду.[24]

24 Аль-Джазіра (9 жовтня 2021 р.). Clashes break out in Rome amid anger over COVID 'green pass'. *Аль-Джазіра*. Доступно в Інтернеті.

2.1.3 Фінансова вигода

Дезінформація про РХБЯ загрози часто має на меті отримання прибутку. Дуже простим способом збагачення є використання Інтернету для реклами й продажу підробленої або низькоякісної продукції (наприклад, засобів індивідуального захисту (ЗІЗ), лікарських засобів і вакцин) у надзвичайній ситуації, пов'язаній із загрозою РХБЯ.

На ілюстрації 13 показано приклад вебсайту, який продавав підроблені захисні засоби під час пандемії COVID-19. Роботу цього вебсайту, яким керували члени ІДІЛ, було припинено у Сполучених Штатах в серпні 2020 року. Вебсайт продавав респіратори N95, заявляючи, що їх схвалено Управлінням з санітарного нагляду за якістю харчових продуктів та медикаментів (FDA). Також заявлялося, що запаси масок є майже необмеженими, в той час як офіціальна влада оголосила про дефіцит цих товарів.[25]



Ілюстрація 13: Знімок екрана вебсайту, який продавав підроблені засоби захисту для фінансування терористичної діяльності ІДІЛ.
Джерело: Міністерство юстиції Сполучених Штатів Америки (2020 р.). Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. Міністерство юстиції Сполучених Штатів Америки. Доступно в Інтернеті.

25 Міністерство Юстиції Сполучених Штатів Америки (2020 р.). Global Disruption of Three Terror Finance Cyber-Enabled Campaigns. *Міністерство юстиції Сполучених Штатів Америки*. Доступно в Інтернеті.

Надзвичайна ситуація, пов'язана із РХБЯ, може відкривати можливості для збагачення. Наприклад, Північний рух спротиву, радикальна неонацистська організація, звернувся з проханням про пожертви на підтримку їхньої діяльності, спрямованої проти вакцинації від COVID-19 (див. ілюстрації 14 та 15).[26] Угрупування на своєму вебсайті пропонувало різні методи оплати, у тому числі платежі в різних криптовалютах.

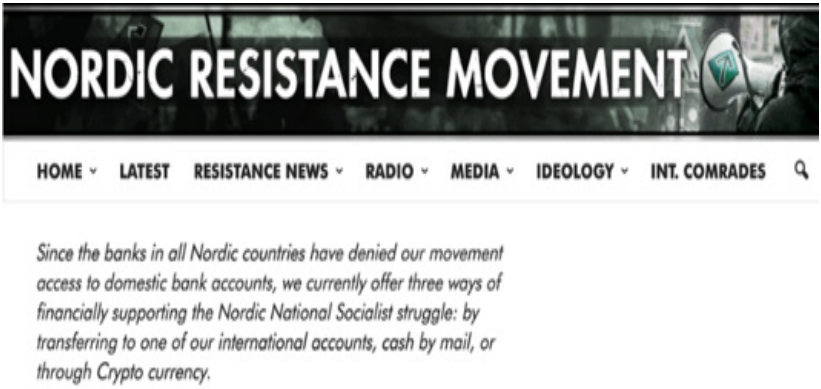
Poster action against experimental Covid-19 vaccines

BY EDITORIAL STAFF - April 2, 2021

ACTIVISM. The Norwegian branch of the Nordic Resistance Movement recently held a poster action against the experimental coronavirus vaccines.

26 Крайні праві угрупування, які базуються у Сполучених Штатах, успішно збагачувалися, використовуючи онлайн-платформи, зокрема стрімінгову платформу Dlive, криптовалюти й інші способи збору коштів, за допомогою яких їм вдавалося збирати до 1,5 мільйонів дол. США на рік. Див. Stone, P. (2021 р.). Крайні праві екстремісти у США заробляють мільйони на соціальних мережах та криптовалютах. *The Guardian*. Доступно в Інтернеті.

Ілюстрація 14: Члени крайніх правих екстремістських рухів рекламують свою діяльність в мережі.
Джерело: вебсайт, Північний рух супротиву, опубліковано в квітні 2021 р.



Ілюстрація 15: Варіанти онлайн-пожертв для фінансової підтримки крайнього правого екстремістського угрупування.
Джерело: вебсайт, Північний рух супротиву, опубліковано в квітні 2021 р.

Дезінформація може також заохочувати до участі в незаконній контрабанді РХБЯ матеріалів. Так сталося й у випадку «червоної ртуті», речовини, яка начебто використовується для створення ядерної зброї. Як показав криміналістичний аналіз зразка, захопленого поліцією, червона ртуть виявилася розіграшем. Однак деякі злочинні угрупування з початку 90-х років підігрівали міф, що червона ртуть є компонентом ядерної зброї, й намагалися продавати її як ексклюзивній товар на чорному ринку.[27]

27 Chivers, C.J. (22 листопада 2015 р.). The Doomsday Scam. *The New York Times*. Доступно в Інтернеті.

2.2 Методи та успішні практики дезінформації у соціальних мережах та додатках для обміну повідомленнями

У соціальних мережах та додатках для обміну повідомленнями для поширення дезінформації на тему РХБЯ загрози використовуються різні методи. Огляд цих методів міститься в цьому розділі.

2.2.1 Маніпуляції із вмістом

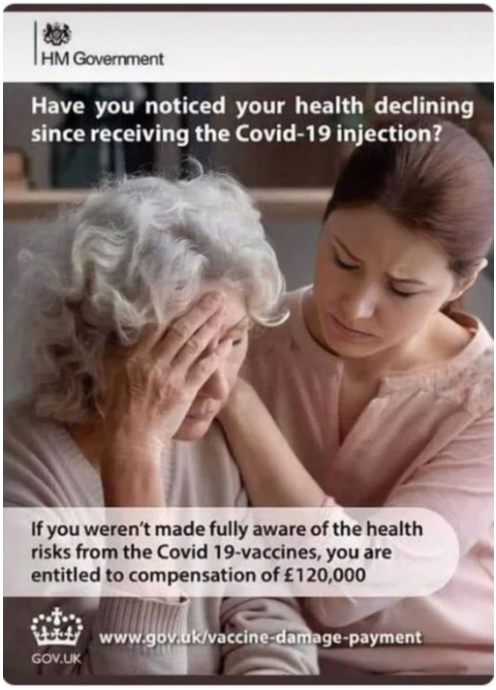
Взагалі під маніпулюванням вмістом у соціальних мережах розуміють оригінальний вміст, з яким проведено цифрові маніпуляції за допомогою програмного забезпечення для редагування фото і відео.[28] Маніпуляції із вмістом можна виконувати за допомогою відносно простого й доступного програмного забезпечення. На ілюстрації 16 показано постер, начебто опублікований урядом Об'єднаного Королівства, який закликає людей звертатися за компенсацією, якщо «до їхнього відома не були повністю доведені ризики, пов'язані з вакцинами від COVID-19». Постер виявився підробкою, яка поширювалася на платформах соціальних мереж без дозволу уряду.[29] Як можна побачити на ілюстрації 17, оригінальну фотографію, на якій зображено літню жінку, що сидить, поклавши руку на чоло, та яку втішає молода жінка, було взято із сайту зі стоковим фотографіями.[30]

28 ЮНЕСКО (2018 р.). Journalism, 'fake news' and disinformation. Посібник з навчання та інструктажу журналістів в *ЮНЕСКО*. Доступно в Інтернеті.

29 Reuters (20 травня 2022 р.). Fact Check-Poster about UK vaccine compensation scheme is not from UK. *Reuters*. Доступно в Інтернеті.

30 Ймовірніше за все, це зображення було взято з вебсторінки iStock, що знаходиться в Інтереті за адресою https://www.istockphoto.com.

Цікаво те, що в постері було певне зерно правди, оскільки уряд Об'єднаного Королівства створив механізм для одноразових виплат особам, які «отримали серйозну інвалідність внаслідок вакцинації від певних хвороб».[31] Однак цей механізм, який називався «компенсація за шкоду внаслідок вакцинації, не був створений спеціально для вакцин від COVID-19. Також на офіційному вебсайті уряду не говорилося про те, що громадяни мають право на компенсацію, якщо «до їхнього відома не були повністю доведені ризики, пов'язані з вакцинами від COVID-19» (як було написано у фальшивому постері).



Ілюстрація 16: Фальшивий постер з логотипом уряду Об'єднаного Королівства. Постер поширювався у Facebook.
Джерело: Перевірка фактів AFP (23 травня 2022р.). UK govt rejects fake Covid vaccine injury poster shared on Facebook. *Перевірка фактів AFP*. Доступно в Інтернеті.

31 Уряд Об'єднаного Королівства (б. д.). Vaccine Damage Payment in *Government of the United Kingdom*. Доступно в Інтернеті.

Ілюстрація 17: Оригінальна фотографія жінки, що сидить, охопивши голову рукою, яку втішає молода жінка. Ймовірніше за все, її було взято з iStock.

Ілюстрація 18 є зразком ще одного фальшивого постера з логотипами Центрів контролю та профілактики захворювань США (CDC) та Всесвітньої організації охорони здоров'я (ВООЗ). Це постер з виразним антисемітським, ісламофобським та расистським посланням, поширюваним через різні крайні праві онлайн канали, який закликає членів групи, що мають підтверджений діагноз COVID-19, поширювати вірус у громадах місцевих меншин.

Ілюстрація 18: Фальшивий постер CDC та ВООЗ з дезінформацією, спрямованою проти меншин, який закликає людей поширювати COVID-19.
Джерело: Telegram, канал Британського націонал-соціалістичного руху, опубліковано в березні 2020 р.

Ілюстрація 19 є черговим прикладом маніпуляції із вмістом, коли два оригінальних зображення навмисно були використані в невірному контексті з накладеним поверх них текстом, що вводить читачів в оману. Після землетрусу в Японії 24 березня 2022 року у Facebook з'явився допис з двома старими фотографіями. На першій фотографії було зображено пожежу на нафтопереробному заводі поряд з атомною електростанцією Фукусима після жахливого землетрусу 11 березня 2011 р. (ілюстрація 20). Друга фотографія — це зображення групи пожежників у захисному спорядженні, які брали участь у рятівній операції після того, як чоловік поранив ножем щонайменше 10 людей і здійснив підпал у потязі в Токіо 31 жовтня 2021 року.

Керуючись очевидним наміром ввести в оману населення, на два зображення в дописі було накладено такий текст корейською мовою: «[Останні новини] японську атомну електростанцію Фукусіма охопило червоне полум'я».

У цьому прикладі ми маємо справу із зображеннями двох реальних подій (пожежі поряд з електростанцією внаслідок землетрусу 11 березня 2011 року та групи пожежників, сфотографованої після нападу на потяг 31 жовтня 2021 року), які не підроблялися, але були умисно пов'язані з несправжніми подіями за допомогою додавання неправдивого тексту (пожежа на атомній електростанції Фукусіма 24 березня 2022 року). Заради справедливості варто зазначити, що й у цій новині було зерно правди: 16 березня 2022 року на атомній електростанції Фукусіма дійсно спрацювала пожежна сигналізація, але за інформацією японської влади, ані полум'я, ані диму виявлено не було.[32]

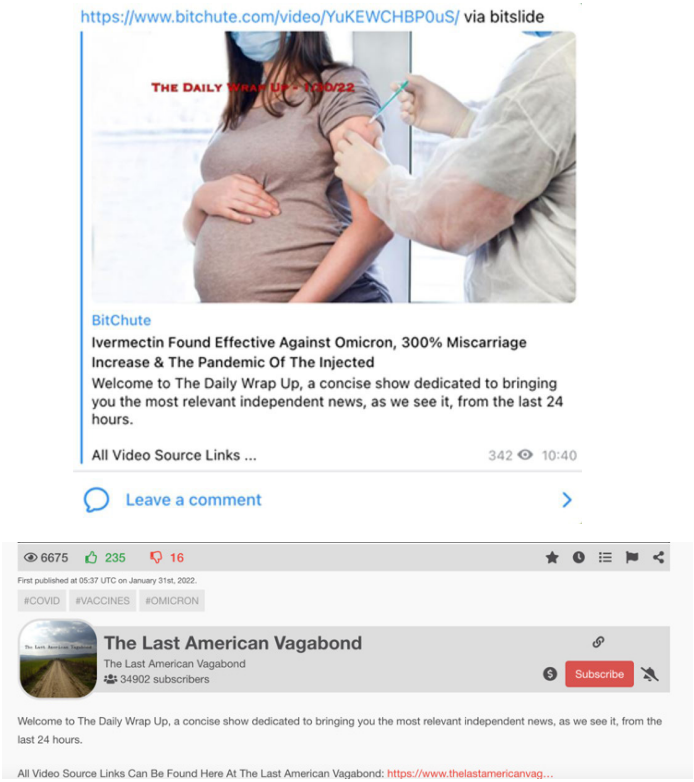
32 Shim, K. (29 березня 2022 р.). Social media users share misleading Fukushima plant claim after Japan earthquake. *Перевірка фактів AFP*. Доступно в Інтернеті.

Ілюстрація 19: Неправдивий допис, у якому стверджується начебто на атомній електростанції Фукусіма сталася велика пожежа.
Джерело: Facebook, опубліковано 24 березня 2022 року.

Ілюстрація 20: Оригінальна фотографія, на якій зображено велику пожежу на нафтопереробному заводі поряд з атомною електростанцією Фукусима після жахливого землетрусу 11 березня 2011 року.

Іншим способом маніпулювання вмістом є створення шахрайського посилання, яке переводить користувачів на вебсайт з дезінформацією. Наприклад, у дописі на ілюстрації 21 міститься хибне твердження, що вакцина від

COVID-19 підвищує ризик загибелі плоду під час вагітності. Це повідомлення посилається на джерело («All Video Source Links»), але коли користувачі натискають на гіперпосиланні, вони переадресовуються на вебсайт (The Last American Vagabond), який поширює теорії змови та екстремістський вміст.



Ілюстрація 21: У дописі міститься хибне твердження, що вакцина від COVID-19 підвищує ризик загибелі плоду під час вагітності. Це повідомлення посилається на джерело («All Video Source Links»). Але коли користувачі натискають на гіперпосиланні, вони переадресовуються на вебсайт (The Last American Vagabond), який поширює теорії змови та екстремістський вміст.
Джерело: Telegram, канал Plandemic, допис від 31 січня 2022 року та Bitchute, The Last American Vagabond, допис від 31 січня 2022 року.

Новітні технології зробили можливим використання складних методів для маніпуляції вмістом, такі як дефейс вебсайту та діпфейк відео. Дефейс вебсайту — це атака на вебсайт, яка змінює вигляд та вміст вебсайту. Хакери (яких називають «дефейсерами») зламують вебсервер і замінюють вебсайт, який на ньому розміщено, на інший, який вони створили.[33] Діпфейк-відео — це результат роботи штучного інтелекту (ШІ), який синтезує зображення людини, комбінуючи й накладаючи наявні зображення і відео на оригінальні зображення або відео. Ці відео або фотографії можуть підривати репутацію людей, адже згенеровані зображення майже неможливо відрізнити від оригіналу. У поєднанні із системами синтезу мовлення (які вчаться імітувати людські голоси) діпфейк-відео можуть подавати людей у негативному світлі, відтворюючи не лише їхні голоси, але й властивий їм темп мовлення та вирази.[34] У такий спосіб методи ШІ здатні продукувати фальшиві новини, у тому числі реалістичні відео й аудіо, з метою керування громадською думкою, впливу на політичні кампанії та підриву довіри до уряду (наприклад, в питаннях вакцинації).[35]

На ілюстрації 22 наведено приклад діпфейк-відео, виготовленого дослідниками Каліфорнійського університету, Берклі, та Південно-Каліфорнійського університету в рамках дослідження, проведеного з метою розробки нових методів визначення діпфейків, створених для компрометації політичних лідерів.

33 Ferreira, S., Antunes, M., & Correia, M. E. (2021 р.). Exposing Manipulated Photos and Videos in Digital Forensics Analysis. *Journal of Imaging*, *7*(7), 102.

34 Allen, G. & Chan, T. (2017 р.). Artificial Intelligence and National Security. *Дослідження Центру Белферів.* Доступно в Інтернеті.

35 Larson, H. J. (16 жовтня 2018 р.). The biggest pandemic risk? Viral misinformation. *Nature*. Доступно в Інтернеті. Див. також Gambetta, D. & Hertog, S. (2017 р.). *Engineers of Jihad: The Curious Connection between Violent Extremism and Education*; Д. Канеман. (2011 р.). *Мислення, швидке й повільне*.

Ілюстрація 22: Діпфейк-відео про колишнього Президента Сполучених Штатів Баррака Обаму, створене дослідниками Каліфорнійського університету, Берклі, та Південно-Каліфорнійського університету.
Джерело: Manke, K. (18 червня 2019 р.) Researchers use facial quirks to unmask 'deepfakes' in Berkeley News. Доступно в Інтернеті.

2.2.2 Імітація наукових дебатів

Ще одним методом дезінформації в соціальних мережах є імітація наукових дебатів. Під науковою достовірністю розуміють визнання науки як джерела надійної інформації, зокрема через те, що інформація вважається результатом застосування методології, яка заслуговує на довіру (науковий метод)[36], або пройшла ретельне рецензування, щоб бути визнаною науковою літературою.[37]

Зловмисники можуть маніпулювати учасникам онлайн-обговорень, посилаючись на зображення або дебати, які

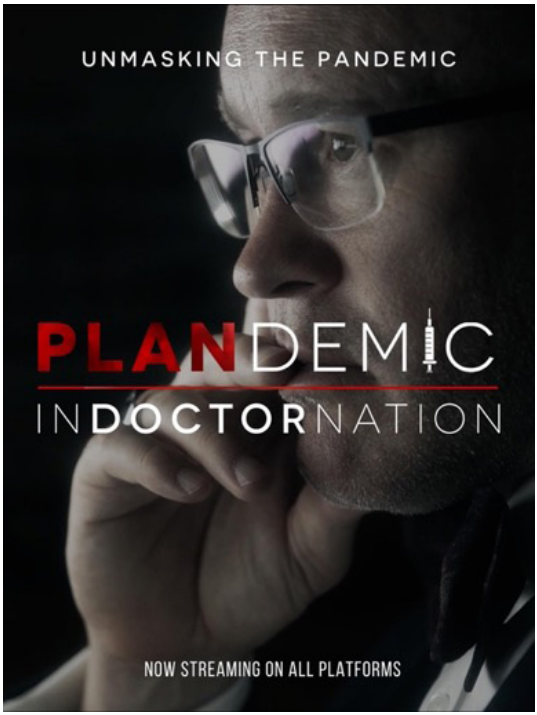
36 «Науковий метод є процесом об'єктивного встановлення фактів шляхом випробувань та експериментів. Базовий процес передбачає проведення спостереження, формулювання гіпотези, висловлення припущення, проведення експерименту та, нарешті, аналіз результатів». Докладну інформацію див. у: Wright, G. & Lavery, T (б. д.). Scientific Method. *TechTarget*. Доступно в Інтернеті.

37 Bocking, S. (2004 р.). *Nature's experts: science, politics, and the environment*. стор. 164.

оманливо асоціюються з надійним джерелом інформації. Наприклад, в псевдонаукових онлайн-дебатах можуть цитуватись особи, які іменуються «вченими», але які не мають жодного стосунку до будь-якого освітнього або наукового закладу чи не вважаються експертами в науковій спільноті. Зловмисники можуть поширювати хибні твердження в мережі, посилаючись на осіб, які видаються за лікарів або експертів попри те, що ці особи можуть не тільки не мати офіційного підтвердження їхньої кваліфікації, а й взагалі бути вигаданими людьми, які згадуються з метою створення оманливого враження про достовірність дезінформації.

Інший метод введення в оману — імітація наукового обговорення, з наведенням цитат із статей, опублікованих в Інтернеті, або посилань на них. Хитрість цього методу полягає в тому, що статті, з яких походять цитати, не були опубліковані в рецензованих журналах і тому не проходили ретельну редакторську перевірку. Той самий метод може використовуватися для виробництва документації. На ілюстрації 23 показано афішу фільму Plandemic: Indoctrination («Пандемія. Навіювання»), який вийшов в серпні 2020 року. Автори фільму стверджують, що пандемія COVID-19 є частиною секретного плану, розробленого певними організаціями, як-от Центри контролю та профілактики захворювань США та Google, для встановлення контролю над людством і отримання прибутків. Фільм претендує на звання науково-документального, але фактчекери довели бездоказовість більшості тверджень «Пандемії».[38]

38 Dunlop, W.G. (19 серпня 2020 р.). New 'Plandemic' film promotes coronavirus conspiracy theory. *Перевірка фактів AFP*. Доступно в Інтернеті.



Ілюстрація 23: Заставка конспірологічного документального фільму «Пандемія». Крайні праві екстремістські угрупування посилалися на це відео як на науковий доказ.

Викривлена інтерпретація статистики й маніпулювання даними також є тактикою розповсюдження дезінформації в соціальних мережах.[39] Так сталося з документом, опублікованим Італійською агенцією з лікарських засобів (AIFA) у травні 2020 року, у якому подається статистика смертності після першої та другої доз вакцини від COVID-19 в Італії (див. ілюстрацію 24). Допис в соціальній мережі, який належить екстремістському угрупуванню правого крила,

39 Для отримання докладної інформації про те, як визначити сфабриковану або невірну статистику, див.: Otis, C. (2020 р.). *True or False. Посібник з визначення фальшивих новин для аналітиків ЦРУ*.

закликає всіх підписників розповсюджувати статистику AIFA, хибно стверджуючи, що уряд Італії очікує 54697 смертей після першої та другої дози вакцини.

Однак в документі AIFA йдеться зовсім про інше. У ньому пояснюється, що кількість зареєстрованих смертей протягом перших 14 днів після введення першої або другої дози вакцин від COVID-19 становить 277 людей, що потрібно порівнювати із загальною очікуваною смертністю за той самий період (ця кількість, яка була розрахована на основі статистичних даних за 2019 рік, становить 52665 смертей). Як недвозначно пояснюється в документі AIFA, цей тип аналізу є важливим для розуміння можливого статистичного зв'язку між введенням вакцини й кількістю смертей, які б сталися так чи інакше, незалежно від вакцинації. Якщо кількість випадків смертності, зареєстрованих після введення вакцини є нижчою за очікувану смертність (як це сталося в Італії) зв'язок між першою й другою цифрою навряд чи є простим збігом.

Ілюстрація 24: Приклад невірного тлумачення офіційних даних, пов'язаних з COVID-19.
Джерело: Gab, канал RAM: Right-wing Alt Media, опубліковано 6 грудня 2021 р. Оригінальний документ: Італійська агенція з лікарських засобів (AIFA), *Оглядовий звіт № 5 про вакцинацію від COVID-19* за період з 27.12.2020 р. по 26.05.2021 р.

Розділ 1. Як ідентифікувати фальшиву або невірну статистику

Під час ідентифікації фальшивої або невірної статистики слід враховувати наведені нижче аспекти.

1. Статистичні дані повинні посилатися на доступне джерело.
2. Інформація повинна походити з надійного джерела (як-от наукова стаття, уряд, визнаний засіб масової інформації).
3. Правильні та/або надійні дані повинні підтверджуватися перехресним посиланням на інші надійні джерела.
4. На графіках має чітко вказуватись, який саме параметр вимірюється.
5. Надійні джерела зазвичай уточнюють, як саме збиралися або вибиралися данні для графіків або статистики. Це також може бути корисним для аналізу того, чи не було інформацію вирвано з контексту.

2.2.3 Створення й поширення теорій змови

Розвиток та поширення теорій змови у соціальних мережах може також використовуватися в якості ефективного методу дезінформації широких верств населення. Теорії змови — це пояснення складних подій або ситуацій, які не підкріплені достовірними доказами.[40] В основі цих теорії лежить таємна змова, начебто організована впливовими людьми, яким вдалося приховати їхню роль і які навмисно й свідомо спланували події, діючи за таємним планом.[41] Щоб придати теоріям змови більшої «достовірності», вони часто ґрунтуються на певних реальних подіях.

Наприклад, теорія змови була створена після жахливого вибуху в порту Бейрута 4 серпня 2020 року. Причиною вибуху була детонація великої кількості аміачної селітри, яка зберігалася на складі поблизу порту без належних заходів безпеки. Однак на різних платформах соціальних мереж з'явилося декілька дописів, у яких стверджувалося, що це був напад із застосуванням ядерної зброї. На ілюстрації 25 наведено приклад допису із соціальної мережі, у якому причиною вибуху хибно оголошується напад із застосуванням тактичної ядерної бомби. Приписка «безпосередньо на даху банка Ротшильда в Бейруті, Ліван» в кінці допису умисно натякає на те, що Ротшильди, впливова сім'я європейських банкірів, мали відношення до підозрюваного нападу із застосуванням ядерної зброї. Відповідно до фальшивого наративу, який

40 Існують різні види теорій змови, і вони часто адаптуються під світогляд цільової аудиторії,але всі вони мають подібну структуру й часто перетинаються між собою. Теорію змови можна поділити на конспірологічні теорії контролювання (відповідно до яких світ, держава, засіб масової інформації або організація перебуває під контролем унітарного органу осіб, які переслідують спільну мету) змови проти групи осіб (спроби певної групи еліт знищити іншу групу), теорії, що стосуються певної події (тлумачення подій у світлі теорії контролювання або переконання, що проти групи проводиться спланована кампанія), та складні або містичні конспірологічні теорії. Brown, M. (2020 р.). Fact check: Did Gates Foundation fund and does Pirbright Institute Own Coronavirus Patent? *Southwest Times Record*. Доступно в Інтернеті.

41 Miller, C., & Bartlett, J. (2010 р.). The Power of Unreason: Conspiracy Theories, Extremism and Counter-Terrorism. *Academia*. Доступно в Інтернеті.

є дуже популярним серед крайніх правих угрупувань, сім'я Ротшильдів володіє Центральним банком Лівану. Оскільки головне управління Центрального банку заходиться поблизу порту Бейрута, теорія змови робить висновок, що це була не випадковість, і вибух 4 серпня був нападом із застосуванням ядерної зброї, спланованим сім'єю банкірів.[42]

Ілюстрація 25: Приклад допису в соціальній мережі, в якому стверджується, що вибух в порту Бейрута 4 серпня 2020 року стався внаслідок застосування ядерної зброї. **Джерело**: Facebook, зафіксовано 5 серпня 2020 року.

42 Dunlop, W.G. (5 серпня 2020 р.). Beirut blast was not a nuclear explosion. *Перевірка фактів AFP*. Доступно в Інтернеті. Також див. McCarthy, B. (6 серпня 2020 р.). QAnon conspiracy theorists seek to link Beirut explosion to Rothschilds. *PolitiFact*. Доступно в Інтернеті.

Ще один приклад теорії змови, об'єктом якої в 2019 році став Інститут Пірбрайта. Інститут Пірбрайта — це біологічна дослідницька лабораторія, яка володіє патентом (датованим 2018 роком) на коронавірус, що в першу чергу вражає курей і може потенційно використовуватися в якості вакцини для профілактики респіраторних захворювань у птахів (IBV). Хоча цей патент неможливо було використати для розробки вакцини від COVID-19, теорія змови, яку вперше було опубліковано на вебсайті Humans Are Free в січні 2020 року, стверджує, що Інститут Пірбрайта створив та запатентував COVID-19 у 2018 році, задовго до реєстрації низки випадків захворювання в Китаї (в грудні 2019 р.). Таким чином, відповідно до цієї бездоказової теорії змови, Інститут Пірбрайта штучно створив як вірус COVID-19, так і ліки від нього. А коли захворюваність набула масштабів епідемії, інститут почав збагачуватися, продаючи вакцину (див. ілюстрацію 26).[43]

Теорія змови набула подальшого розвитку, коли Інститут Пірбрайта почали пов'язувати з Фондом Біла й Мелінди Гейтс, хибно стверджуючи, що розробка патенту на COVID-19 фінансувалася Фондом Біла й Мелінди Гейтс (див. ілюстрацію 27). Фонд насправді є одним із спонсорів інституту, проте він не фінансує дослідження, пов'язані з коронавірусом, у тому числі пов'язані з патентом на перспективну вакцину для профілактики респіраторних захворювань у птахів (IBV).[44]

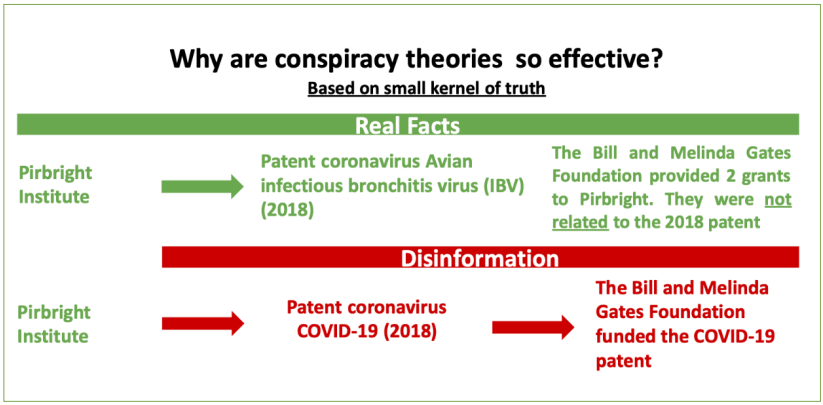
43 Наприклад, вебсайт, який спеціалізується на поширенні теорій змови й інших форм невірної інформації та дезінформації, опублікував статтю, в який стверджується, що інститут начебто запатентував COVID-19, намагаючись «створити штам вірусу, який можна буде використовувати в якості зброї й який спеціально призначено для збільшення продажів непотрібних, смертельно небезпечних вакцин, вбивши для цього декілька тисяч, а може й мільйонів, людей». Brown, M. (2020 р.). Fact check: Did Gates Foundation Fund and Does Pirbright Institute Own Coronavirus Patent? *Southwest Times Record*. Доступно в Інтернеті.

44 Фонд Біла й Мелінди Гейтс надав Інституту Пірбрайта два гранти: перший на дослідження хвороб худоби в листопаді 2013 року, а другий в червні 2016 року для проведення дослідження можливості створення універсальної вакцини від грипу.

Ілюстрація 26: Зображення, отримане із сторінки користувача у Facebook.
Джерело: Facebook, користувач, опубліковано в липні 2020.

Ілюстрація 27: Зображення, отримане на сторінці користувача у Facebook.
Джерело: Facebook, користувач, опубліковано в липні 2020.

Як видно з ілюстрації 28, ця теорія змови містить певні елементи правди (Інститут Пірбрайт є тримачем патенту на коронавірус і отримував фінансування від Фонду Біла й Мелінди Гейтс), але історія в цілому була сфальсифікована й викривлена таким чином, що Інститут виступає в ролі злого генію, який стоїть за появою COVID-19. Додавання реальних фактів робить теорію змови більш привабливою, і вона внаслідок цього швидко поширюється в соціальних мережах. Вона з'являлась на різних платформах і каналах дезінформації, у тому числі в стрічці Twitter за авторством відомого YouTube-блоггера Qanon, де стверджувалось, що патенти, які належать Інституту Пірбрайта, — це патенти на новий коронавірус.[45]



Ілюстрація 28: Діаграма, яка ілюструє поєднання фактів і дезінформації в теорії змови щодо Інституту Пірбрайта.
Джерело: ЮНІКРІ

45 ibid

Теорії змови можуть підвищувати ступінь радикалізувати, адже їхні наративи апелюють до почуття відчуженості від суспільства й налаштовують особу «проти всіх».[46] Під час пандемії COVID-19 канали соціальних мереж, переповнені радикальними екстремістами, стали родючим ґрунтом для теорій змови, які подекуди перетворилися на конспірологічні мегатеорії, у яких були поєднані зовсім не поєднувані особи та організації, у тому числі меншини, органи охорони здоров'я, Організація Об'єднаних Націй, таємні світові еліти та навіть інопланетяни. Така трансформація мала масштабні наслідки й викликала вороже ставлення та супротив у відповідь на будь-які заходи уряду в зв'язку з надзвичайними ситуаціями, пов'язаними з РХБЯ чинниками.[47]

У певних випадках теорії змови можуть видозмінюватися, адаптуючись до нової ситуації, що може виражатися у поєднані кількох конспірологічних теорій. Такі конспірологічні мегатеорії намагаються розглядати різні типи подій у світовій історії й часто посилаються на всесвітню змову. Прикладом конспірологічної мегатеорії, використаної під час пандемії COVID-19, є «новий світовий порядок». Ця теорія змови, яка має антисемітське походження, стверджує, що за лаштунками світової політики еліти займаються організацією глобальних подій і таємно впроваджують антиутопічну міжнародну структуру управління, яка дозволить їм контролювати населення Землі. Прибічники цієї теорії змови вважають, що представники еліти намагаються встановити новий світовий порядок шляхом режисерування глобальних події

46 Emberland, T. (2020 р.). Why conspiracy theories can act as radicalization multipliers of far-right ideals. *Центр вивчення екстремізму*. Доступно в Інтернеті.

47 Перевірка фактів Reuters (2021 р.). Fact check-list of claims about Bill Gates includes falsities. *Reuters*. Доступно в Інтернеті. FactCheck.org. (б. д.). Person: Bill Gates. *FactCheck.org*. Доступно в Інтернеті. FactCheck.org. (б. д.). Person: Dr. Anthony Fauci. *FactCheck.org*. Доступно в Інтернеті.

й контролю пов'язаних з ними нарративів, які провокують масові заворушення.[48]

Під час пандемії ця теорія змови розвинулася й увібрала в себе конспірологічну теорію «Великого перезавантаження». Витоки концепції Великого перезавантаження, лежать в міжнародній ініціативі, започаткованій Всесвітнім економічним форумом (ВЕФ) у червні 2020 року, головним завданням якої є підтримка більш справедливих результатів і переосмислення глобальних інвестицій та державних витрат для протидії негативним економічним наслідкам пандемії.[49] Теорія змови спотворила первинне значення Великого перезавантаження, пов'язавши цю ініціативу з конспірологічною теорією нового світового порядку. Основним припущенням конспірологічної теорії Великого перезавантаження є ідея, що світові еліти використовують пандемію COVID-19 як можливість для поширення радикальних політик, як-от примусова вакцинація, цифрові посвідчення особи й відмова від приватної власності.[50]

Ілюстрація 29 містить приклад того, як ця конспірологічна теорія поширюється у соціальних мережах. У цьому дописі користувач посилається на промову прем'єр-міністра Канади, у якій той згадує ініціативу Великого перезавантаження, впроваджену Всесвітнім економічним форумом (ВЕФ). Користувач хибно стверджує, що прем'єр-міністр говорить про теорію змови, а не про ініціативу.

48 Flores, M. (2022 р.). The New World Order: The Historical Origins of a Dangerous Modern Conspiracy Theory. *Інститут міжнародних досліджень в Монтереї при Міддлберійському коледжі*. Доступно в Інтернеті.

49 Всесвітній економічний форум (2020 р.). The Great Reset. *Всесвітній економічний форум*. The Great Reset.

50 Slobodian, Q. (2020 р.). How the 'great reset' of capitalism became an anti-lockdown conspiracy. *The Guardian*. Доступно в Інтернеті.

Ілюстрація 29: Знімки екрана, що ілюструють поширення конспірологічної теорії великого перезавантаження в мережі.
Джерело: AFP (2020 р.). Justin Trudeau's UN speech is not proof of 'great reset' conspiracy. BOOM. Доступно в Інтернеті.

Розділ 2. Як розпізнати теорію змови?

1. Предмет теорії є дуже нечітким і невизначеним (наприклад, «таємні глобальні еліти прагнуть до панування над світом»).
2. Історія є нескінченною — у теорію змови продовжують додаватися нові елементи.
3. Кількість залучених учасників є необмеженою, і по мірі розвитку теорії змови їхня кількість продовжує зростати.
4. Теорія змови пояснює все без винятку, не залишаючи можливості для альтернативного пояснення.
5. Теорія змови не обмежується певною історичною епохою, а натомість продовжує існувати в різних історичних періодах.

2.2.4 Спроба зацікавити людей фальшивими передбаченнями й очікуваннями

Метод зацікавлення користувачів теорією змови полягає в передбаченнях на майбутнє й створенні очікувань майбутньої події.

У якості прикладу використано теорію змови QAnon. Все почалося в жовтні 2017 року, коли невідомий на ім'я «Q» розмістив на вебсайті 4chan повідомлення, у якому стверджувалося, що таємна секта сатаністів-педофілів з числа лідерів Демократичної партії США, організувала міжнародну мережу торгівлі дітьми з метою сексуальної експлуатації й готує заколот проти уряду США. Хоча Q раніше робив декілька прогнозів, які не справдилися, від

повернення Джлна Ф. Кеннеді молодшого до неминучої громадянської війни, рівень підтримки цієї теорії змови не зменшився.[51]

Що відбувається, коли передбачення не здійснюються (як це часто трапляється)? Прихильники теорій змови часто пояснюють, що очікувана подія не трапилась через те, що таємні змовники відклали її. Таким чином хибність передбачень й ненастання очікуваних подій автоматично стають «доказами» вірності теорії змови.

Було проведено декілька досліджень, метою яких було зрозуміти, чому люди схильні вірити невірній інформації, коли вони стикаються із доказами, які суперечать їхнім переконанням. Одне з перших досліджень провів психолог Леон Фестнгер, якій увів термін «когнітивний дисонанс», щоб описати психологічні страждання, які відчуває людина, що намагається одночасно дотримуватися суперечливих переконань, цінностей або підходів (наприклад, коли курець бачить підтвердження того, що паління є однією з найпоширеніших причин хвороб та смерті). Щоб впоратися з такою стресовою ситуацією, людині слід або змінити її переконання (наприклад, кинути палити), або вигадати пояснення, яке усуне дисонанс. У другому випадку людина може подовжувати вірити неправдивій інформації, створюючи «альтернативні» пояснення й відповіді, які усувають конгнітивний дисонанс (наприклад: «мій сусід палить усе життя і ніколи не мав жодних проблем із здоров'ям»).[52]

51 Щоб отримати докладну інформацію про QAnon див.: Forrest B. (4 лютого 2021 року). What Is QAnon? What We Know About the Conspiracy-Theory Group. *The Wall Street Journal*. Також див. McDonald B. (31 березня 2021 р.). How QAnon Reacts to Failed Predictions. *Global Network on Extremism and Technology*.

52 Festinger, L. (1957 р.). *A Theory of Cognitive Dissonance*.

2.2.5 Апеляція до емоцій

Користувачі часто демонструють в соціальних мережах високу емоційну складову. Дезінформація стратегічно покладається на емоційно провокативний контент, за допомогою якого вона викликає сильні почуття або реакції. Надзвичайна ситуація, пов'язана з РХБЯ чинниками, може використовуватися як нагода, щоб грати на людських емоціях, особливо за відсутності достатньої інформації та вказівок з боку офіційних органів.

Прикладом є повідомлення на ілюстрації 30, яке було опубліковано тайським крайнім правим угрупуванням в жовтні 2022 році. Метою допису було стривожити читачів і спровокувати лякливу емоційну реакцію, необґрунтовано стверджуючи, що уряд Фінляндії порекомендував громадянам країни терміново купувати йод в таблетках після початку війни в Україні. Насправді ж країна, у якій працюють атомні електростанції, просто оновила настанови з використання йоду, щоб захистити своїх найбільш вразливих громадян в екстреній ситуації, яка могла статися внаслідок аварії ядерного реактора.[53]

Ілюстрація 30: Знімок екрана із дописом у Facebook, автор якого намагається налякати читачів, хибно стверджуючи, що уряд Фінляндії рекомендує громадянам країни терміново купувати таблетки йоду після того, як в Україні почалася війна. **Джерело:** Facebook, опубліковано 14 травня 2022 року.

53 Aemocha, P. (26 жовтня 2022 р.). Finland did not advise citizens to 'urgently buy iodine tablets after escalation of war in Ukraine. *Перевірка фактів AFP.* Доступно в Інтернеті.

Іншим поширеним методом, який використовується для звернення до емоцій, є пошук «ворога», наприклад звинувачення місцевих меншин в надзвичайній ситуації, пов'язаній з РХБЯ чинниками. На ілюстрація 31 зображено постер з мігрантами всередині Троянського коня, які звинувачуються в тому, що вони принесли в Європу COVID-19.

Ілюстрація 31: Мем, який поширювався неонацистським британським націонал-соціалістичним рухом.
Джерело: Telegram, канал British National Socialist Movement, опубліковано в 2020 р.

2.2.6 Крадіжка культурної власності

Інший метод дезінформації полягає у крадіжці популярних культурних символів. Деякі екстремістські угрупування використовують популярні символи, часто захищені авторським правом, як-от логотипи й значки, щоб поширювати дезінформацію без дозволу осіб, яким належить авторське право. Перевага цього методу полягає в тому, що популярний символ може приваблювати увагу онлайн-користувачів, які можуть не знати про те, що таке використання є вирваним з контексту, незаконним або шахрайським. У деяких випадках присвоювання популярних культурних символів може навіть супроводжуватися створенням (або викраденням) відчуття його приналежності шляхом повної підміни його значення.

Так, наприклад, крайні праві екстремістські угрупування, вкрали мультиплікаційний персонаж жабку Пепе. Жабку Пепе створив художник та дитячий письменник Метт Ф'юрі під час роботи над мультсеріалом Boy's Club, який вийшов на MySpace у 2005 році. Хоча персонаж жабки Пепе не мав жодного зв'язку з радикальними екстремістськими поглядами, екстремісти у 2016 році почали використовувати його для пропаганди ідей расового верховенства й альтернативного правого контенту. Під час пандемії COVID-19 персонаж жабки Пепе також було вкрадено для просування онлайн-дезінформації про політики вакцинації й інші заходи уряду. Автор започаткував кампанію «Врятуймо Пепе», закликаючи поширювати онлайн-контент з «миролюбним або приємним» описом персонажу, намагаючись запобігти його асоціюванню із символом ненависті. Щоправда, потім він вирішив «вбити» жабку Пепе в коміксі на одну сторінку, створеному з нагоди Дня безкоштовного коміксу, організованого видавництвом Fantagraphics, оскільки він не міг повернути собі цей персонаж.[54] На ілюстраціях 32-34 показано відмінності оригінального персонажу від змінених зображень, створених радикальними екстремістськими групами.

54 Hunt, E. (2017 р.) Pepe the Frog creator kills off internet meme co-opted by White Supremacists. *The Guardian*. Доступно в Інтернеті. Також див. Pettis, B. (2017 р.). *Pepe the Frog: A Case Study of the Internet Meme and its Potential Subversive Power to Challenge Cultural Hegemonies.*

Ілюстрація 32: Оригінальний персонаж жабки Пепе з фразою «feels good man».

Ілюстрація 33: Зловмисне використання крайнім правим екстремістським угрупуванням образу жабки Пепе, який в цьому конкретному випадку поєднано з нацистськими символами.
Джерело: Goodyear, S. (28 вересня 2016 р.). Pepe the Frog joins swastika and Klan hood in Anti-Defamation League's hate symbol database. *CBC News*. Доступно в Інтернеті.

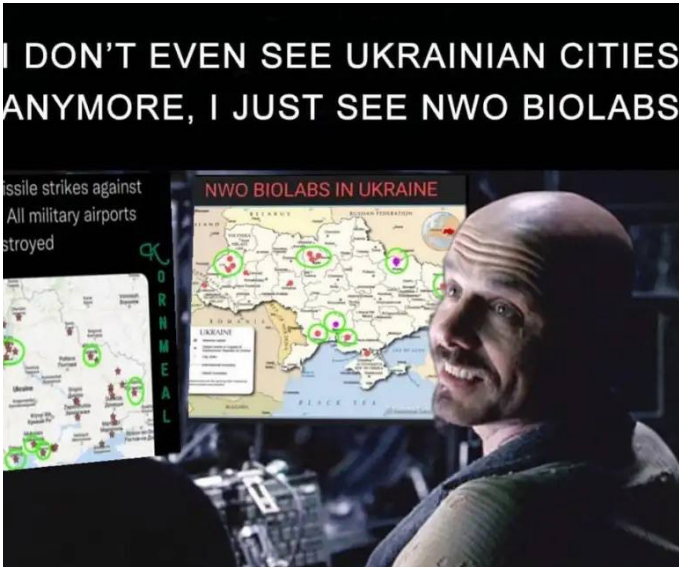
Ілюстрація 34: Мем, в якому використовується незаконно привласнене зображення жабки Пепе, поширюване в мережі на каналі крайнього правого екстремістського угрупування.
Джерело: Telegram, канал COVID-19 Agenda, опубліковано в 2022 році.

Вилучення «інтернет-мемів» з їхнього оригінального контексту є ще одним методом поширення дезінформації в Інтернеті.[55] Інтернет-мем складається з фрази, зображення або відео, яке швидко поширюється від людини людині каналами соціальних мереж і в додатках для обміну повідомленнями.[56] Меми часто вдаються до гумору, щоб посприяти їхньому поширенню і стали соціальним феноменом, який використовується для пропаганди ідей, поведінки або стилю. На жаль, радикальні екстремісти також використовують меми для поширення людиноненависницьких ідей і дезінформації.

55 Еволюційний біолог Річард Докінз впровадив термін «мем» (від грецького «*mimema*», що означає «наслідуваний») в 1976 році для позначення елементу культурної трансмісії, який розповсюджується шляхом наслідування.

56 Puche-Navarro, R. (2004 р.). Graphic Jokes and Children's Mind: An Unusual Way to Approach Children's Representational Activity. *Scandinavian Journal of Psychology*, стор. 45, 343-355.

Зокрема, деякі крайні праві екстремісти, намагаючись залучити до своїх лав молодь, починають спілкування з молодими людьми із мемів, які спочатку мають гострий гумористичний характер, але поступово набувають відвертого жорстокого та дискримінаційного характеру.[57] Ілюстрація 35 є прикладом мему, який маніпулює кадрами з популярного фільму (*«Матриця»*) для фальшивих звинувачень на адресу уряду України. Ці угрупування використовують меми, щоб здаватися актуальними й привабливими для молодої аудиторії й створювати відчуття приналежності до одної спільноти. Угрупування також у схожий спосіб пропонують «дружбу» людям, які пишуть в інтернеті про їхню самотність, пригніченість або хронічну хворобу, переслідуючи кінцеву мету зробити їх членами угрупування, користуючись їхнім прагненням до соціалізації.



Ілюстрація 35: Приклад маніпуляції популярним фільмом (*«Матриця»*).
Джерело: Telegram, канал Holocaust II, допис від 10 березня 2022 року.

57 Flores, M. (2021 р.). From memes to race war: How extremists use popular culture to lure recruits. *The Washington Post*. Доступно в Інтернеті.

2.2.7 Камери відлуння

Ефективним методом поширення дезінформації є створення онлайн камер відлуння. Камера відлуння є віртуальним середовищем, де група осіб бере участь в онлайн-обговоренні й постійно чують лише відлуння власних суджень, не стикаючись з альтернативними ідеями або думками. Камери відлуння можуть використовуватися для створення невірної інформації або для поширення дезінформації, викривлення точки зору особи й обмеження її здатності розглядати протилежну точку зору.[58]

В онлайн камері відлуння користувачі шукають, тлумачать та згадують інформацію, яка підтверджує їхні попередні переконання або ідеї. Цей феномен називається «схильність до підтвердження власної точки зору».[59] Ці канали можуть використовуватися в якості інструментів для маніпуляції думкою людей і радикалізації користувачів під час надзвичайної ситуації, пов'язаної з РХБЯ чинниками.

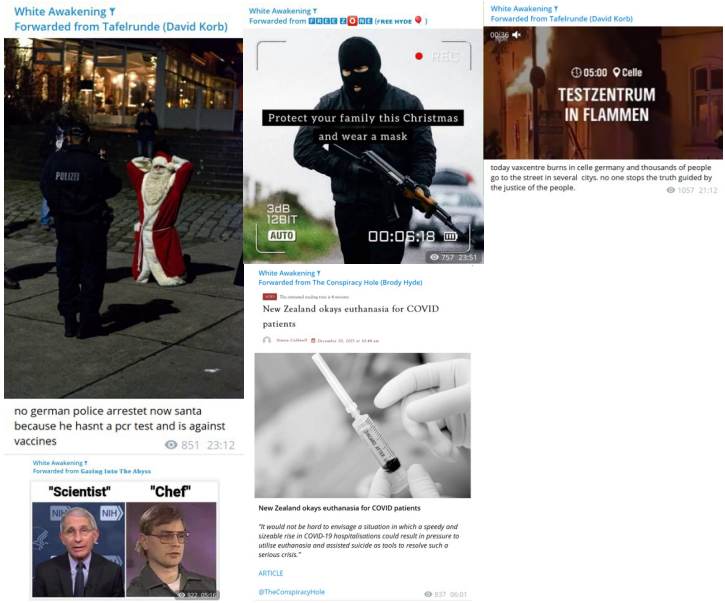
На ілюстрації 36 показано приклад крайнього правого каналу (який називається White Awakening) у соціальній мережі, де екстремістські погляди користувачів постійно відлунюються вустами інших користувачів. Вибрані повідомлення, опубліковані 25 грудня 2021 року, виражають одні й ті самі думки та, в поєднанні з іронією та хибною інформацією, критикують обмежувальні заходи, пов'язані з COVID-19, які вживають уряди різних країн в всьому світі: поліція «арештовує» Санта Клауса, тому що той не має негативного результату ПЦР тесту на COVID-19t; чоловік у балаклаві із зброєю в руках «дотримується» вимог заходів з профілактики COVID-19; д-р Ентоні Фаучі, директор Національного інституту алергічних та інфекційних захворювань (NIAID) при Національному інституті охорони здоров'я США, порівнюється з Джефрі Дамером, відомим серійним убивцею; Міністерство охорони здоров'я Нової

58 GCF Global. (б. д.). Digital Media Literacy: What is an echo chamber? *GCFGlobal.org*. Доступно в Інтернеті.

59 Casad, B. J. (2019 р.). Confirmation bias. *Британська енциклопедія*. Доступно в Інтернеті.

Зеландії прийняло закон, який прямо дозволяє лікарям приймати рішення щодо проведення евтаназії пацієнтам, хворим на COVID-19 (що є неправдою); тисячі німецьких пацієнтів спалюють центри вакцинації (що є неправдою). На каналі немає джерела альтернативної думки щодо COVID-19.

Деякі повідомлення мають посилання на інші канали (наприклад, канал «Free zone» або «Gazing into The Abyss»), але коли користувачі переходять на такі інші канали, вони знаходять там подібні екстремістські наративи. Таким чином, камера відлуння має «невидимий» механізм, який ловить користувачів, надаючи їм інформацію, що постійно повторюється й підтверджує ті самі екстремістські ідеї. Як буде показано нижче в пункті 2.2.10 («Роль алгоритмів»), алгоритми також можуть сприяти створенню камер відлуння, пропонуючи контент або зв'язки з іншими користувачами, які поділяють схожі ідеї або інтереси.



Ілюстрація 36: Приклад повідомлень, які були поширені на Різдво 2021 року на крайньому правому каналі White Awakening
Джерело: Telegram, канал White Awakening, опубліковано 25 грудня 2021 року.

2.2.8 Атаки з метою зіпсувати репутацію цілі дезінформації

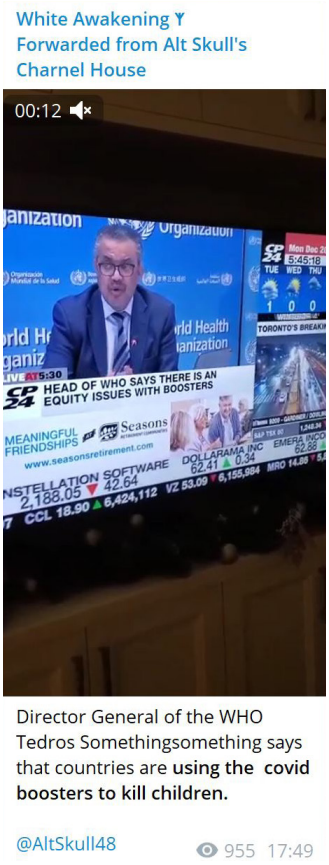
Типовим методом, який використовується в мережі, щоб дезінформація виглядала більш легітимно, є напад на репутацію об'єкту дезінформації. Головною метою такої діяльності є заподіяти шкоду іміджу жертви дезінформації, підірвати довіру до неї і, потенційно, зменшити ефективність її заходів реагування на надзвичайну ситуацію, пов'язану з РХБЯ чинниками.

Наприклад, під час пандемії Всесвітня організація охорони здоров'я (ВООЗ) та її генеральний директор Тедрос Аданом Гебреісус часто стають цілями дезінформації й теорій змови. Дезінформатори намагалися знецінити роботу організацій, наприклад, популярна теорія змови хибно стверджує, що ВООЗ планувала укладення «пандемійної угоди», яка позбавить країни-учасники суверенітету в рамках досягнення «мети Великого перезавантаження Всесвітнього економічного форуму». Ці хибні звинувачення викривалися різними фактчекерами.[60]

На ілюстрації 37 показано приклад того, як ВООЗ та її генеральний директор стали об'єктами нападу, цього разу з боку крайнього правого Telegram каналу. Фальшиве звинувачення маніпулює вмістом оригінальної промови генерального директора.

Мережева наклепницька кампанія може призвести до онлайн-переслідування, особливо коли в дезінформацію вірить достатня кількість людей. Внаслідок застосування цього методу реакція на хибні звинувачення може залишатися без уваги, оскільки репутація об'єкту дезінформації буде підірваною.

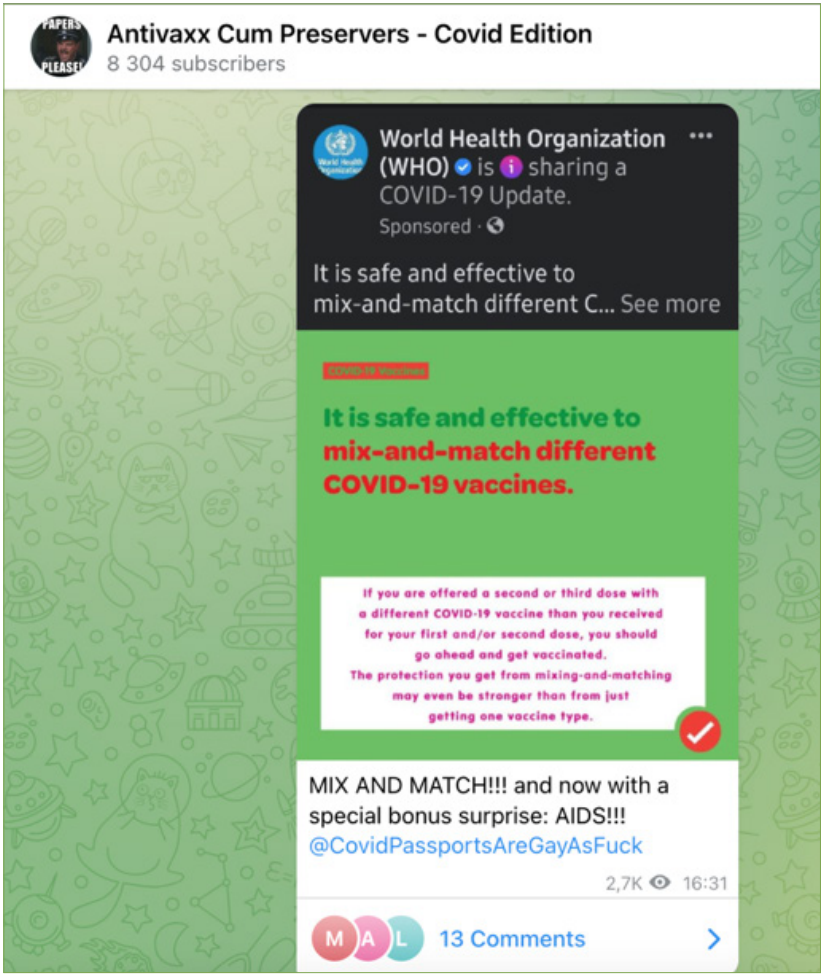
60 Перевірка фактів Reuters. (2022 р). Fact check-the WHO is not planning to implement a 'pandemic treaty' that would strip Member States of sovereignty. *Reuters*. Доступно в Інтернеті.



Ілюстрація 37: Знімок екрана, що є доказом поширення дезінформації про ВООЗ крайнім правим Telegram-каналом.
Джерело: Telegram, канал White Awakening, опубліковано в 2022 р.

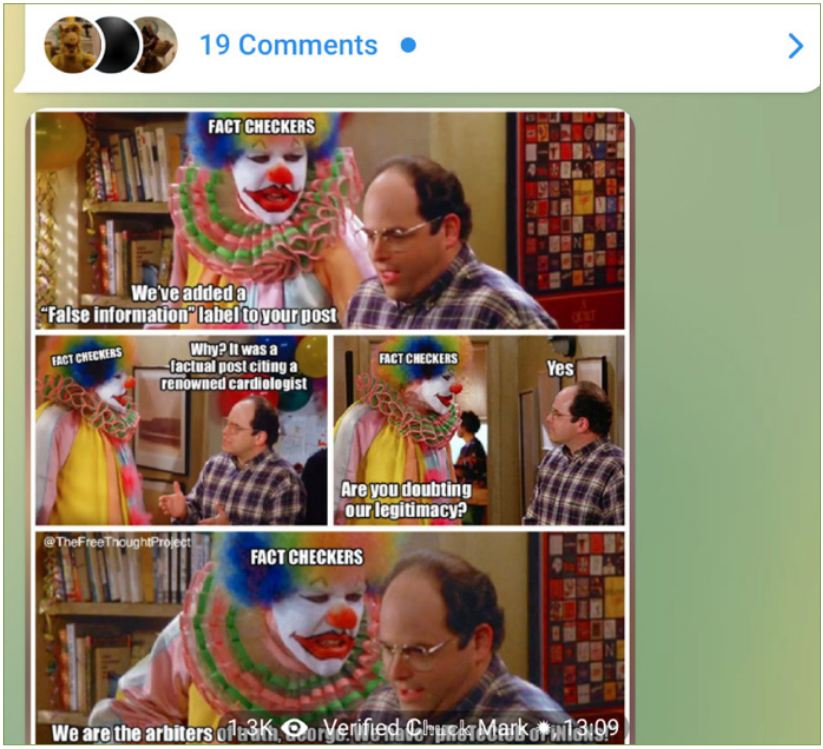
Цей метод часто застосовується проти фактчекерів і, в цілому, проти діяльності з протидії дезінформації, за допомогою невірного цитування, неправильного тлумачення або умисного вибору частини інформації, повідомленої фактчекером. Наприклад, на ілюстрації 38 показана спроба заплутати користувачів, які читають фактчекінгові дописи ВООЗ. Допис ВООЗ («про безпечність і ефективність комбінування різних типів вакцин від COVID-19») було позначено як «хибний» шляхом заміни кольору кола (із зеленого кола з білим прапорцем на червоне коло з білим

прапорцем). Таким чином, позбавляючи фактчекінговий сервіс контексту, вірна інформація використовується для поширення дезінформації.



Ілюстрація 38: На знімку екрана показано, як крайній правий Telegram-канал поширює дезінформацію, використовуючи викривний допис, який раніше опублікувала ВООЗ.
Джерело: Telegram, канал Antivaxx, опубліковано в 2022 р.

На ілюстрації 39 показано, як крайні праві угрупування у своїх дописах також атакують фактчекерів, висміюючи роботу, проведену цими особами та організаціями.



Ілюстрація 39: Знімок екрана з крайнього правого Telegram-каналу, який висміює роботу, проведену фактчекерами.
Джерело: Telegram, канал Voluntarist Memes, опубліковано в 2022 р.

2.2.9 Уникання виявлення та контролю з боку органів влади

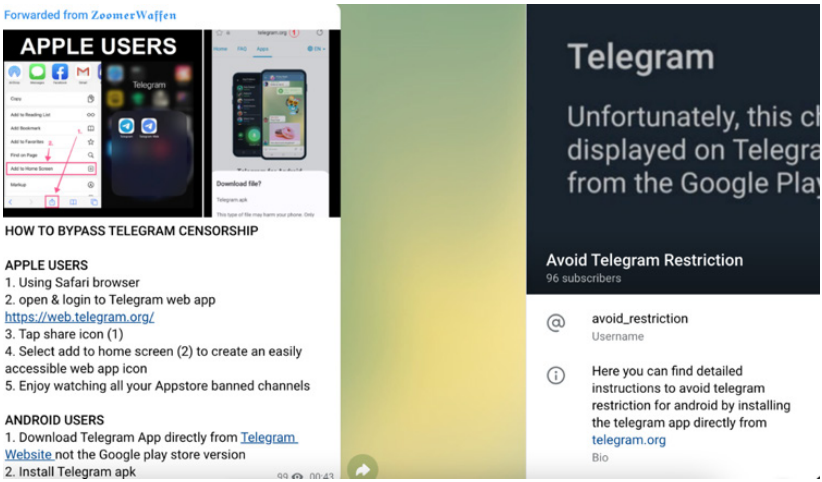
Існують різні методи, які розповсюджувачі дезінформації використовують для ухиляння від відстеження в Інтернеті правоохоронними органами й операторами соціальних мереж. Наприклад, ІДІЛ розробив різні методи, пом'якшення пропагандистських формулювань або використання *емодзі*[61] для позначення слів, які в іншому випадку були б ідентифіковані (наприклад, «зброя», «вибух» та «ракета»). Під час десятиденного бою в кінці січня 2022 року, який мав на меті звільнення терористів з в'язниці в Хасеке, Сирія, ІДІЛ використовував хештег з фальшивого засобу масової інформації для координації кампанії мережевої пропаганди, у якій послідовники з різних соціальних мереж сприяли втечі ІДІЛ з в'язниці.[62]

Інший поширений метод, який радикальні екстремісти використовують для зменшення ризику цензури, — це створення резервних облікових записів. Якщо відповідний орган виявляє й закриває основний обліковий запис, радикальні екстремісти можуть негайно перенести контент у новий обліковий запис і переспрямувати свою аудиторію. На ілюстрації 40 показано, як група крайніх правих екстремістів видала своїм послідовникам вказівки щодо отримання доступу до цензурованого контенту.

Іноді деякі радикальні екстремісти переспрямовують своїх послідовників на платформи.

61 Емодзі — це «невеликі зображення символи або значки, які використовуються в текстових полях в електронних комунікаціях (наприклад, в текстових повідомленнях, електронних листах і соціальних мережах), щоб виражати емоційне ставлення автора, повідомляти інформацію лаконічно, передавати повідомлення в грайливий спосіб без допомоги слів тощо». Словник Merriam-Webster (б. д.). Emoji. *Словник Merriam-Webster.com*. Доступно в Інтернеті.

62 Scott, M. (2022 р.). Islamic State evolves 'emoji' tactics to peddle propaganda online. *POLITICO*. Доступно в Інтернеті.



Ілюстрація 40: Знімок екрану з крайнього правого каналу, де послідовникам видаються вказівки щодо отримання доступу до цензурованого контенту.
Джерело: Telegram, канал White Awakening, опубліковано в 2022 р.

2.2.10 Роль алгоритмів

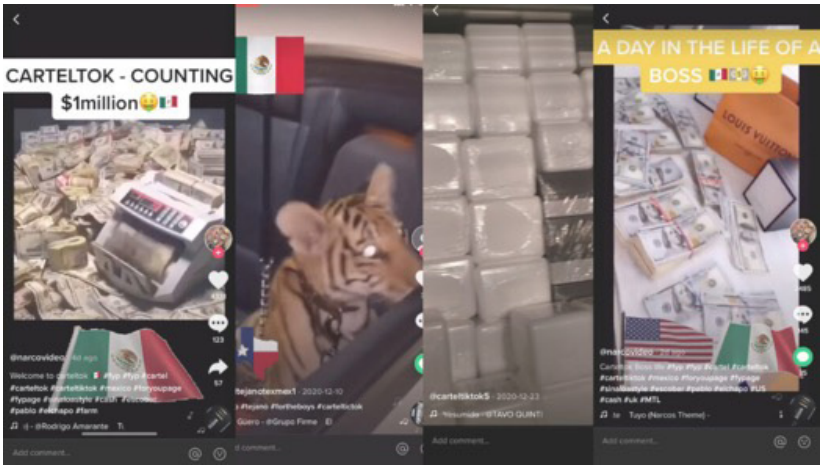
Алгоритм соціальних мережі — це набір правил, який визначає, як користувачі бачитимуть данні на платформі. Алгоритми соціальних мереж допомагають візуалізувати контент, як-от дописи або відео, відповідно до його актуальності, а не дати публікації. Іншими словами, алгоритми встановлюють черговість контенту, який користувач бачить на платформі, відповідно до ймовірності, що такий контент зацікавить користувача, незалежно від дати його публікації.[63] Наприклад, алгоритми визначають, які дописи рекомендуватимуться користувачам, коли ті гортатимуть стрічку (наприклад, у Facebook або Instagram).

63 Golino, M. A. (2021 р.). Algorithms in social media platforms. *Інститут Інтернета та справедливо суспільства*. Доступно в Інтернеті.

Таким чином, алгоритми створені для того, щоб підтримувати користувачів і визначати, що може бути для них більш цікавими, та уникати потенційно недоречного й низькоякісного контенту. Щоправда, алгоритми соціальних мереж також можуть сприяти поширенню повідомлень, які несуть фальшиву інформацію та вміст. Наприклад, відео погоні поліції за човном із злочинцями в 2020 році в США стало вірусним, після того як користувачі (здебільшого підлітки) візуалізували відео на своїй сторінці For You (ілюстрація 41). Мільйони користувачів вподобали й поширили відеоролик і внаслідок цього алгоритм почав пропонувати подібні ролики, у тому числі відео, опубліковані деякими наркокартелями в Мексиці, які рекламували «потенційні переваги» долучення до наркоторгівлі, як-от безмежна кількість грошей, дорогі автівки, гарні жінки й екзотичні тварини (ілюстрація 42).[64]

Ілюстрація 41: Знімки екрана з відеороликом TikTok про переслідування човна.
Джерело: TikTok, допис опубліковано користувачем у 2020 році.

64 Lopez, O. (2020 р.). Guns, drugs and viral content: Welcome to cartel TikTok. *The New York Times*. Доступно в Інтернеті. Також див. Proceso (2020 р.). "Narcomarketing" La Nueva Estrategia de Cárteles Mexicanos en TikTok: NYT. *Proceso*. Доступно в Інтернеті.

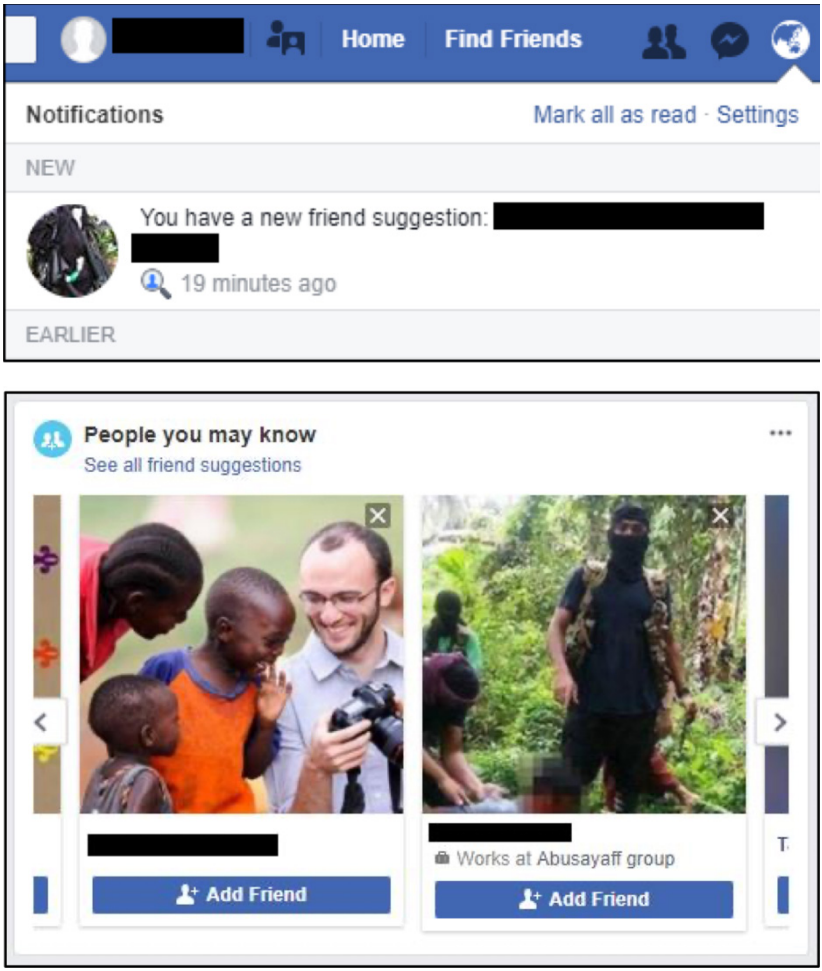


Ілюстрація 42: Екранні знімки хештега #CartelTikTok, поширюваного в TikTok.
Джерело: Morris, E. (2021 р.). Cartel TikTok: Mexican Drug Lords' newest marketing strategy? Glimpse from the Globe. Доступно в Інтернеті.

Алгоритми також можуть сприяти взаємодії між користувачами, які поділяють спільні екстремістські погляди й допомагають радикалізувати й залучати нових членів до лав терористичних або радикальних екстремістських угрупувань. Наприклад, такі функції як «люди, яких ви можете знати» або «пропоновані друзі» можуть сприяти створенню зв'язків між екстремістами.

Ілюстрація 43 демонструє приклад алгоритму пропонування друзів, який застосовує платформа, що пропонує членів ІДІЛ в якості друзів, поєднуючи профілі екстремістів і поширюючи мережу ІДІЛ.[65]

65 Waters, G., & Postings, R. (2018 р.). *Spiders of the Caliphate: Mapping the Islamic State's Global Support Network on Facebook.* Доступно в Інтернеті.



Ілюстрація 43: Знімки екрана з Facebook з пропозиціями додатися в друзі до осіб, які є членами ІДІЛ.
Джерело: Waters, G., & Postings, R. (2018 р.). Spiders of the Caliphate: Mapping the Islamic State's Global Support Network on Facebook. Доступно в Інтернеті.


3

Викриття дезінформації

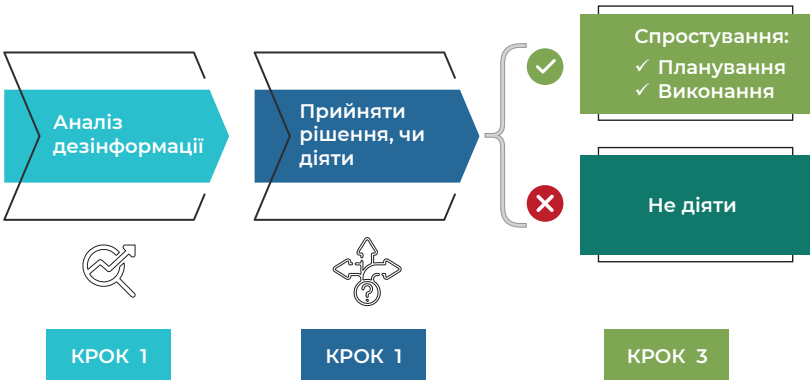
У цьому розділі описано методи ефективного викриття дезінформації на платформах соціальних мереж. Викриття — це засіб реагування, який застосовується після того, як дезінформування вже відбулося. Викриття можна визначити як процес демонстрації невірності чогось, як-от переконання або теорії, або демонстрації хибності оповіді, ідеї, заяви тощо.[66]

Викриття є не єдиною стратегією боротьби з дезінформацією. Інша стратегія, яка називається «випереджувальне викриття», полягає в реагуванні на дезінформацію до того, як хибні твердження поширяться, щоб пом'якшити їхній негативний ефект. Попереднє викриття ґрунтується на теорії щеплення, відповідно до якої невелика кількість вірусу в організмі може сприяти утворенню антитіл, які допоможуть боротися з майбутнім зараженням цим вірусом. Аналогічно, вплив дезінформації (слабкий) може допомогти виробити стійкість до майбутнього впливу дезінформації.

66 Британська енциклопедія. (б. д.). Debunk. *Британська енциклопедія*. Доступно в Інтернеті.

Незважаючи на те, що викриття й випереджувальне викриття мають багато схожого, у цьому посібнику розглядаються лише методи викриття. Перелік деяких інструментів для ефективного відстеження та виявлення дезінформації міститься в Додатку до цього посібника.

Викриття можна розглядати як трьохетапний процес: на першому етапі дезінформація аналізується, на другому приймається рішення, чи варте хибне звинувачення того, щоб витрачати на його викриття час та ресурси і, якщо таке рішення буде прийнято, настає третій етап, який полягає в плануванні й здійсненні викриття.



Ілюстрація 44: Трьохетапний процес викриття.
Джерело: ЮНІКРІ.

3.1 Перший етап: аналіз дезінформації в соціальних мережах

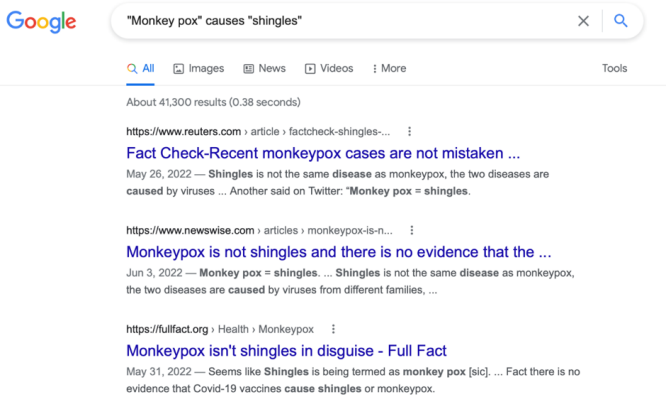
Коли особа або організація стають ціллю дезінформації, першим етапом є аналіз фальшивих звинувачень. Аналізуючи дезінформацію, можна дізнатися важливу інформацію про те, хто це зробив і з якою метою. Деякі з різних методів, які можна для цього застосувати, більш детально описані нижче (ілюстрація 45).

Ілюстрація 45: Елементи, які слід брати до уваги під час аналізу фальшивої інформації, яка поширюється в соціальних мережах.
Джерело: ЮНІКРІ.

а) Виявлення та аналіз джерел

Під час аналізу дезінформації важливо знати джерело хибної інформації (наприклад, стаття або допис) і перевірити, чи джерело містить ту саму інформацію й чи не був оригінальний контент змінений або підроблений. Цінні відомості також можна отримати, перевіряючи дату публікації хибного звинувачення і встановлюючи, хто є його автором (минуле цієї особи, опубліковані нею в Інтернеті/соціальних мережах інші дописи/статті).

Одним з методів, який можна використовувати для виявлення джерела й надійності інформації, є пошук за ключовими словами у веб-браузері, такому як Mozilla Firefox або Google Chrome, щоб перевірити, чи інформація або твердження публікувалися на інших вебсайтах. Ілюстрація 46 є прикладом застосування такого методу, коли було здійснено пошук за певною темою (віспа мавп викликає оперізуючий лишай). Терміни «віспа мавп» і «оперізуючий лишай» написано у лапках, щоб найти вебсайти із контентом, який містить точний термін. У результатах пошуку можна побачити декілька фактчекінгових вебсайтів, на яких ця дезінформація викривається. Інші корисні символи, які можуть використовуватися для отримання більш точних результатів пошуку, це мінус або дефіс (-) для виключення окремих слів з результатів пошуку Google, символ порядкового номеру або хештег (#) для пошуку терміна, який використовується в соціальних мережах та тільда (~) перед пошуковим ключовим словом, для включення в результати подібних ключових слів і синонімів.[67]



Ілюстрація 46: Екранний знімок вікна пошуку Google з використанням лапок для пошуку точних термінів «віспа мавп» та «оперізуючий лишай».
Джерело: пошук в Google, 2022 р.

67 Див. докладно: довідкова інформація із використання пошуку Google Search (б. д.). Звуження пошуку в Інтернеті. *Google*. Доступно в Інтернеті.

Інструменти інформаційних технологій, як-от розширення браузера, можуть аналізувати вебсайти й визначати, чи є джерело надійним, і якщо так, то наскільки (див. Додаток 2). Наприклад, на ілюстрації 47 показано, як працює розширення браузера під час аналізу новин і вебсайтів в мережі. Наприклад, розширення Media Bias/Fact Check відображає значок, який свідчить про точність або викривлення інформації на кожній відвіданій сторінці, і використовує систему рейтингів для оцінки надійності джерела.

Ілюстрація 47: Знімки екрана, які демонструють роботу розширень браузера Media Bias/Fact Check.
Джерело: розширення Media Bias, Fact Check, 2022 р.

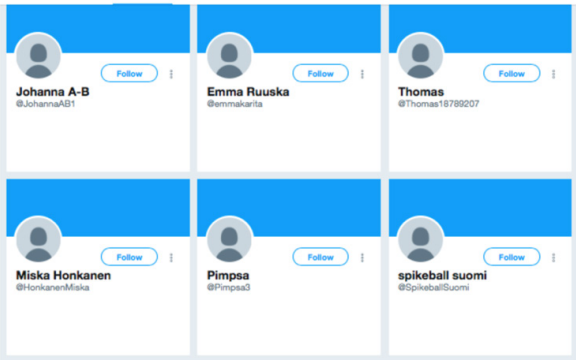
b) Виявлення та виключення фальшивих облікових записів або ботів

У певних випадках можна визначити, чи джерело хибної інформації походить з фальшивого облікового запису (створення враження присутності в соціальних мережах фізичної особи, організації або компанії, яка не існує в реальному житті) або бота.[68] Дуже простим методом є перевірка профілю особи, яка опублікувала фальшиву інформацію[69], у тому числі фото профілю, можливі зв'язки з іншими обліковими записами, року, коли було створено обліковий запис, і активності на платформі соціальної мережі або будь-яка інша інформація, яка може вказувати, що обліковий запис належить реальній особі. Якщо в обліковому записі відсутня зазначена інформація, існує висока ймовірність, що він є обліковим записом бота. Ботів також можна визначити завдяки тому, що вони не можуть ідеально імітувати людське мовлення, тому використовувані ними лексика й поведінка, можливо, здаватимуться неприродними.

Наприклад, на ілюстрації 48 показано, як виглядають облікові записи ботів, у яких немає персональних даних або зображень. На ілюстрації 49 показано приклад активності бота, де з трьох облікових записів поширюється той самий допис з тим самим заголовком.

68 Бот (скорочення від «робот») — це програмне забезпечення, яке виконує автоматичні, повторювані, попередньо визначені завдання. Зазвичай боти імітують або замінюють поведінку живого користувача. Оскільки вони є автоматизованими, вони працюють набагато швидше за справжніх користувачів. Вони виконують корисні функції, як-от обслуговування клієнтів або індексація пошукових систем, але також можуть бути одним з видів шкідливого програмного забезпечення, використовуваного для отримання повного контролю за комп'ютером». Kaspersky. (б. д.). What are bots? – definition and explanation. *Kaspersky*. Доступно в Інтернеті.

69 Соціальні профілі — це опис соціальних характеристик особи, який ідентифікує її на сайтах соціальних мереж. Соціальний профіль також відображає інформацію, яка допомагає зрозуміти тип і міцність зв'язків особи з іншими людьми, наприклад, ступень її залучення й внесок в інші ініціативи, проєкти, спільноти або обговорення, її репутація серед інших учасників тощо. Gartner. (б. д.). Definition of Social Profiles. *Gartner Information Technology Glossary*. Доступно в Інтернеті.



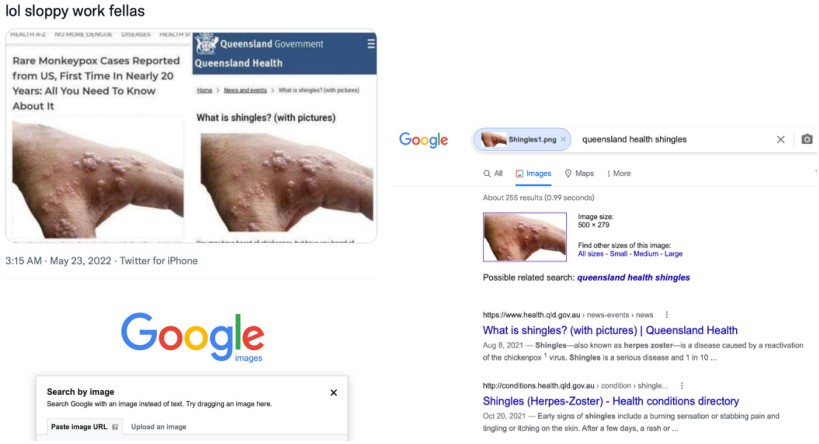
Ілюстрація 48: Знімок екрана з прикладами облікових записів ботів.
Джерело: Дослідницька цифрова кримінологічна лабораторія Атлантичної ради, 2017 р.

Ілюстрація 49: Екранний знімок з прикладом активності бота, коли з різних облікових записів ботів поширюються той самий допис з однаковим заголовком.
Джерело: Дослідницька цифрова кримінологічна лабораторія Атлантичної ради, 2017 р.

c) Підтвердження приналежності візуального контенту до оригінального джерела

Для пошуку джерела зображення можна використовувати інструменти «Пошук зображення через Google» або Tineye. Це зображення можна вивантажити у браузер безпосередньо з комп'ютера або вставивши URL-адресу зображення. Браузер повідомить вас, чи було зображення поширено на інших вебсайтах. Використовуючи цей інструмент можна визначити, чи зображення було

вилучено з контексту, і встановити, на яких вебсайтах і разом з якою інформацією зображення поширювалося раніше. Наприклад, на ілюстрації 50 демонструється, як шукати джерело зображення за допомогою функції «Пошуку зображення через Google»: спочатку потрібно вивантажити зображення або вставити його URL-адресу, а потім просто натиснути кнопку пошуку, щоб знайти вебсайти, на якій було опубліковано зображення. Приклад, в якому результати пошуку, що стосується зображення, яке було невірно підписано як віспа мавп, вказують на оригінальне джерело зображення, а також на вебсайт, який містить реакцію на хибне твердження.[70]



Ілюстрація 50: Приклад пошуку зображення за допомогою функції «Пошуку зображення через Google» з метою з'ясування походження зображення, опублікованого користувачем у Twitter в 2022 році. Користувач Twitter стверджував, що віспа мавп не існує, і співставив зображення із статті про віспу мавп й оперізуючий лишай, щоб довести, що страхування від віспи мавп є фейком. Однак аналіз зображення, опублікованого у Twitter за допомогою функції «Пошуку зображення через Google», вказує на вебсайт, на якому зображення було опубліковане вперше, на якому уточнюється, що віспа мавп існує.
Джерело: Twitter, публікація користувача від 2022 року; знімки екрана з функцією «Пошуку зображення через Google», 2022 р.

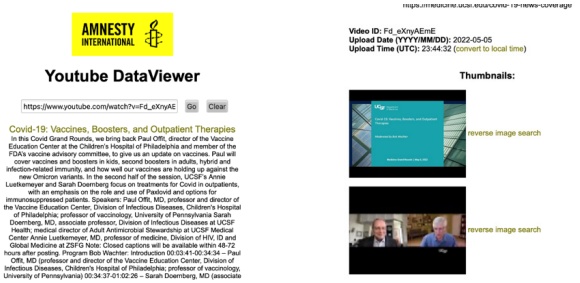
70 Schirrmacher, S. (2022 р.). Fact check: Four fakes about Monkeypox. *Deutsche Welle*. Доступно в Інтернеті.

d) Верифікація відеозаписів та часу, коли було вивантажено контент[71]

Якщо джерелом дезінформації є відео, буде корисно перевірити, коли було вивантажено відео і чи не було його підроблено. Підтвердження достовірності відео, пов'язаних з суспільними подіями, такими як протести або конференції, зазвичай є нескладним, оскільки інформацію про подію можна знайти в новинах або на інших сайтах соціальних мереж. В інших випадках, коли відео присвячено непублічній події, яку не було спланувано заздалегідь (як-от нещасний випадок, напад або природне явище), може виникнути потреба в пошуку додаткової інформації.

Наприклад, відеоролики на YouTube мають часові мітки моменту їхнього першого завантаження в форматі Північноамериканського тихоокеанського стандартного часу (PST). Для отримання додаткової інформації про відео, вивантажені на YouTube, Amnesty International пропонує інструмент, який називається YouTube Data Viewer. Цей інструмент уможливлює зворотній пошук зображення за допомогою використання зображень з відео. Для того, щоб скористатися інструментом, користувачу потрібно вставити URL-адресу відеоролика з YouTube, який потрібно верифікувати. На ілюстрації 51 показано приклад пошуку в YouTube Data Viewer відео, вперше опублікованого на YouTube, яке називається Covid-19: Vaccines, Boosters and Outpatient Therapies («Covid-19: вакцини, бустерні дози та амбулаторне лікування»). Інструмент відображає інформацію про відео, у тому числі час і дату завантаження.

71 Silverman, C. (ред.) (2016 р). *Verification handbook*. Доступно в Інтернеті.



Ілюстрація 51: Знімки екрана, зроблені під час пошуку відео, виконаного в 2022 році в YouTube Data Viewer.
Джерело: YouTube Data Viewer, 2022 р.

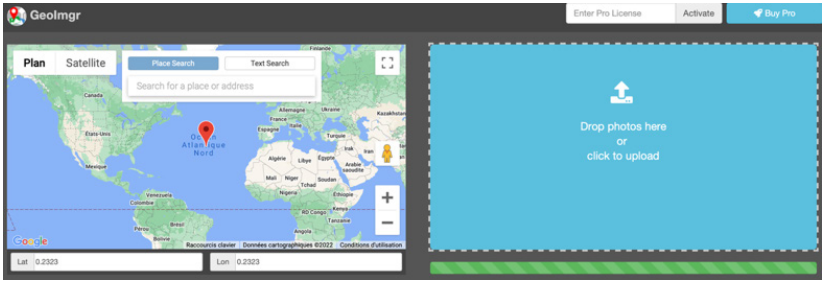
е) Геолокація фото й відео[72]

У більшості випадків зображення або відео містить корисну інформацію. До неї належать виразні елементи вуличного пейзажу, будівля, церква, ряд дерев, гірське пасмо, мінарет або міст — усі вони можуть порівнюватися із супутниковим знімком та фотографіями з відомою геолокацією. Зображення або відео також можуть надати інші корисні дані: назва компанії може вказуватися в мережевій рубрикованій рекламі (мережева реклама, яка містить переліки товарів, продуктів або послуг на інтернет-сайтах) або локальних каталогах, а діалоги й акценти у відео можуть використовуватися для визначення конкретного регіону, вуличні знаки можуть вказати на точне місцезнаходження, автомобільні номери або рекламні білборди можуть містити інформацію про розташування, сонячне світло або тінь можуть допомогти визначити приблизний час доби, коли сталась подія.

Деякі інструменти дозволяють автоматично визначати геолокацію, навіть якщо не всі зображення мають тег з даними геолокації. Наприклад, геолокацію можна перевірити онлайн за допомогою Карт Google (у тому числі з використанням «Перегляду вулиць» для отримання

72 Silverman, C. (ред.). (2016 р). *Verification handbook*. Доступно в Інтернеті.

зображення більшого масштабу або опції «Показати фотографії», щоб перевірити, чи фотографій з відомою геолокацією відповідають місцю, де знято відео), Wikimapia або Google Планета Земля. На ілюстрації 52 показано GeoImgr, який може використовуватися для автоматичного визначення геолокації завантаженого зображення. Користувачу потрібно нажати на синьому екрані (праворуч) й вибрати файл для завантаження.



Ілюстрація 52: Знімки екрану головної сторінки вебсайту GeoImgr.
Джерело: GeoImgr, 2022 р.

f) Виявлення фальшивої статистики або даних, які вводять в оману

Невірне тлумачення статистики й маніпуляція даними також є тактикою розповсюдження дезінформації в соціальних мережах. Для створення враження правдивості хибного твердження точні дані також можуть вилучатися з контексту. Так сталося й у випадку з документом, опублікованим Італійською агенцією з лікарських засобів травні 2021 року, в якому повідомлялась статистика смертності після першої та другої дози вакцини від COVID-19 в Італії (див. п. 2.2.2, «Імітація наукових дебатів») або в ситуації з патентом Інституту Пірбрайта, який було помилково оголошено патентом на COVID-19 (див. ілюстрації 53 та 54).

У наведених нижче прикладах показаний твіт, в якому безпідставно стверджується про існування патентів на COVID-19 у 2006 та 2014 роках. У цьому конкретному

випадку можна дуже просто продемонструвати, що цей твіт є неправдивим, переглянувши базу даних Відомства з патентів і товарних знаків США.[73] Зазначені у твіті номери патенті США просто не існують. Пошук в Google за номером патенту веде на сторінку відкритої бази даних хімічних сполук і сумішей PubChem Національного інституту здоров'я США. Щоправда, інформація на сторінці PubChem свідчить, що із застосуванням для людини пов'язано інший опублікований в 2006 році патент, схожий на патент, про який йдеться в дописі. Він має майже той самий номер, що й патент, згаданих в дописах соціальних мереж, але відрізняється від нього одним зайвим нулем. Цей патент із зайвим нулем у номері стосується нуклеїнових кислот і білків вірусу тяжкого гострого респіраторного синдрому (SARS), які можуть використовуватися для приготування й виготовлення складних вакцин для лікування або профілактики SARS.[74] Згаданий в твіті європейський патент є зареєстрованим в 2018 році патентом Інституту Пірбрайта на коронавірус, який переважно вражає курей і потенційно може використовуватися в якості вакцини для профілактики респіраторних захворювань птахів (IBV), як вже пояснювалось вище у пункті 2.2.3.

Ілюстрація 53: Знімки екрана з твітами, в яких хибно стверджується про існування патентів на COVID-19: одного в Європі, а іншого в США (з посиланням на номер патенту Інституту Пібрайта). Жоден з цих патентів не має стосунку до COVID-19. **Джерело:** перевірка фактів AFP.

73 Онлайн-база даних Відомства з патентів і товарних знаків США доступна в Інтернеті.
74 Dunlop, W. G. (2020 р.). False claims on patents fuel novel coronavirus conspiracy theories online. *Перевірка фактів AFP.* Доступно в Інтернеті.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 172 319 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
20.11.2019 Bulletin 2019/47

(21) Application number: **15750093.5**

(22) Date of filing: **23.07.2015**

(51) Int Cl.:
C12N 7/04 *(2006.01)* ***C07K 14/165*** *(2006.01)*
A61K 39/00 *(2006.01)* ***A61K 39/215*** *(2006.01)*

(86) International application number:
PCT/GB2015/052124

(87) International publication number:
WO 2016/012793 (28.01.2016 Gazette 2016/04)

(54) **CORONAVIRUS**
CORONAVIRUS
CORONAVIRUS

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **23.07.2014 GB 201413020**

(43) Date of publication of application:
31.05.2017 Bulletin 2017/22

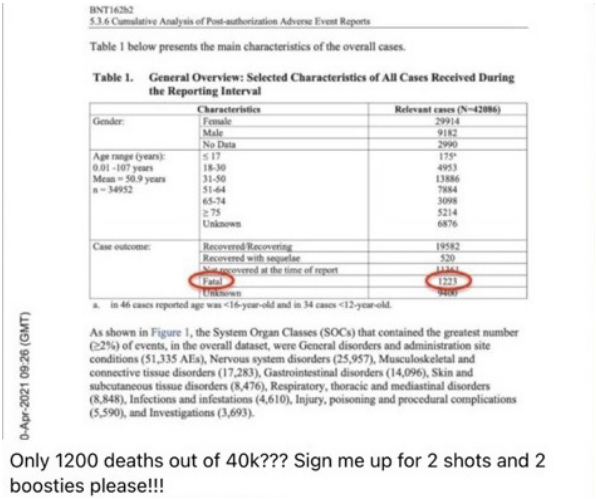
(73) Proprietor: **The Pirbright Institute**
Pirbright
Woking
Surrey GU24 0NF (GB)

(72) Inventors:
- **BICKERTON, Erica**
Woking
Surrey GU24 0NF (GB)
- **KEEP, Sarah**
Woking

- **V. D. MENACHERY ET AL: "Attenuation and Restoration of Severe Acute Respiratory Syndrome Coronavirus Mutant Lacking 2'-O-Methyltransferase Activity", JOURNAL OF VIROLOGY, vol. 88, no. 8, 29 January 2014 (2014-01-29), pages 4251-4264, XP055215583, ISSN: 0022-538X, DOI: 10.1128/JVI.03571-13**
- **Anonymous: "EM_STD:KF377577", , 30 October 2013 (2013-10-30), XP55216202, Retrieved from the Internet: URL:http://ibis/exam/dbfetch.jsp?id=EM_STD :KF377577 [retrieved on 2015-09-25]**
- **PAUL BRITTON ET AL: "Modification of the avian coronavirus infectious bronchitis virus for vaccine development", BIOENGINEERED, vol. 3, no. 2, 1 March 2012 (2012-03-01), pages 114-119, XP055215793, ISSN: 2165-5979, DOI: 10.4161/bbug.18983**
- **MARIA ARMESTO ET AL: "A Recombinant Avian Infectious Bronchitis Virus Expressing a Heterologous Spike Gene Belonging to the 4/91**

Джерело 54: Знімки екрана зареєстрованого в 2018 році патенту Інституту Пірбрайта, в якому описується новий підхід для розробки вакцини для створення покращених вакцин від вірусу інфекційного бронхіту свійських птахів. Цей патент жодним чином не пов'язаний з COVID-19.
Джерело: Європейське патентне відомство.

На ілюстрації 55 зображено допис на крайньому правому каналі в Telegram, який намагається ввести читачів в оману, демонструючи їм таблицю з кількістю пацієнтів, які померли від COVID-19. Однак якщо уважно вивчити таблицю, ви не знайдете в ній жодної згадки про COVID-19.



BNT162b2
5.3.6 Cumulative Analysis of Post-authorization Adverse Event Reports

Table 1 below presents the main characteristics of the overall cases.

Table 1. General Overview: Selected Characteristics of All Cases Received During the Reporting Interval

Characteristics		Relevant cases (N=42086)
Gender:	Female	29914
	Male	9182
	No Data	2990
Age range (years):	≤ 17	175[a]
0.01 -107 years	18-30	4953
Mean = 50.9 years	31-50	13886
n = 34952	51-64	7884
	65-74	3098
	≥ 75	5214
	Unknown	6876
Case outcome:	Recovered/Recovering	19582
	Recovered with sequelae	520
	Not recovered at the time of report	13361
	Fatal	1223
	Unknown	9400

a. in 46 cases reported age was <16-year-old and in 34 cases <12-year-old.

As shown in Figure 1, the System Organ Classes (SOCs) that contained the greatest number (≥2%) of events, in the overall dataset, were General disorders and administration site conditions (51,335 AEs), Nervous system disorders (25,957), Musculoskeletal and connective tissue disorders (17,283), Gastrointestinal disorders (14,096), Skin and subcutaneous tissue disorders (8,476), Respiratory, thoracic and mediastinal disorders (8,848), Infections and infestations (4,610), Injury, poisoning and procedural complications (5,590), and Investigations (3,693).

0-Apr-2021 09:26 (GMT)

Only 1200 deaths out of 40k??? Sign me up for 2 shots and 2 boosties please!!!

Ілюстрація 55: Оманлива статистика на крайньому правому каналі, яка не пов'язана з випадками захворювання на COVID-19.
Джерело: Telegram, канал White Awakening, опубліковано в 2022 р.

Як пояснюється в цьому розділі, в процесі аналізу інформації деякі елементи можуть виявитися «червоними прапорцями» або попередженнями про те, що щось може бути фальсифікацією або походити з ненадійного джерела. На ілюстрації показані деякі елементи, які слід брати до уваги під час оцінки правдивості інформації.

Приклади можливих "червоних прапорців"

Ілюстрація 56: Приклади можливих «червоних прапорців», з якими можна стикнутися під час спроби підтвердити інформацію, отриману з Інтернету.
Джерело: ЮНІКРІ.

Аналіз дезінформації може забезпечити нас важливою інформацією й допомогти перейти до наступних двох етапів.

Короткий зміст: Аналіз дезінформації

- Визначайте джерела та оцінюйте їхню надійність.
- Виявляйте та вилучайте фейкові акаунти та ботів.
- Переконайтеся, що зображення та відео мають посилання на першоджерело.
- Перевіряйте дані про розміщення відео.
- Визначайте геолокацію зображення або відео.
- Виявляйте неправдиву статистику або дані, що вводять в оману.
- Оцініть надійність веб-сайту, перевіривши джерела, URL-адресу, формулювання та пунктуацію тексту, а також загальний зміст.

Ілюстрація 57: Зведений перелік аспектів, на які слід вважати під час аналізу дезінформації.
Джерело: ЮНІКРІ.

3.2 Другий етап: прийняття рішення

На другому етапі приймається рішення щодо доцільності реагування на хибне твердження. Рішення має ґрунтуватися на інформації, зібраній на попередньому етапі й на додаткових факторах, які слід враховувати, перш ніж витрачати час та ресурси на викриття дезінформації.

Допомогти з прийняттям рішення можуть наведені нижче запитання.

Наскільки поширилось хибне твердження?

Викриття може виявитися непотрібним, якщо масштаби поширення хибного твердження або теорії змови є незначними або якщо вони не здатні заподіяти шкоду в поточний момент або в майбутньому.[75] Викриття може знадобитися, якщо фальшиве або хибне твердження сильно поширилося. Наприклад, фальшива інформація про шляхи передавання вірусу або його походження чи дезінформаційний допис, які привертають значну увагу, можуть потребувати певної реакції, адже хибне твердження, яке швидко поширюється мережею, може змусити велику частку населення змінити їхню думку щодо участі в програмі вакцинації або профілактичних заходах. Увагу можна виміряти в кількості вподобань або подібних реакцій у соціальних мережах, кількості коментарів під дописом або кількості випадків поширення або повторних публікацій допису. Інша можлива ситуація, в якій може знадобитися викриття, це коли один і той самий графічний контент широко розповсюджується в численних дописах різними користувачами. Це може статися, коли популярна фальшива статистика або зображення, які пройшли обробку, стають вірусними й перетворюються на загальну тему для обговорення серед користувачів платформ соціальних мереж.[76]

75 Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, M. A., Kendeou, P., Lombardi, D., Newman, E. J., Pennycook, G., Porter, E. Rand, D. G., Rapp, D. N., Reifler, J., Roozenbeek, J., Schmid, P., Seifert, C. M., Sinatra, G. M., Swire-Thompson, B., van der Linden, S., Vraga, E. K., Wood, T. J., Zaragoza, M. S. (2020 p.). *The Debunking Handbook 2020*. Доступно в Інтернеті.

76 Якщо відео, зображення або оповідь стають вірусними, вони швидко й широко поширюються в Інтернеті на платформах соціальних мереж і електронною поштою.

Наскільки хибне твердження пов'язане з вашою сферою діяльності або досвідом?

Викриття дезінформації може не знадобитися, якщо хибне твердження не стосується спеціалізації, посад запланованих жертв дезінформації або організацій, у яких вони працюють. Наприклад, уявімо, що у фальшивому твердженні просто згадується загальна теорія змови без конкретного посилання на місце роботи або посаду жертви, як-от «ти, мабуть, належиш до еліти рептилоїдів». У такому разі, можливо, не варто витрачати ресурси на її розвінчування.

Хто за цим стоїть? Це лише поодинокий епізод чи частина спланованого переслідування в Інтернеті?

Важливо зрозуміти, чи інформація є поодиноким випадком або ж це результат спланованого переслідування в Інтернеті. Онлайн-переслідування може проявлятися у формі тролінгу в Інтернеті (умисні образливі або провокативні дописи в мережі, які мають на меті прикро вразити когось або отримати дратівливу відповідь), кібербулінгу (який включає отримання образливих або зловмисних повідомлень або навіть створення вебсайтів, які спеціально відкриваються для того, щоб заподіяти шкоду особам або окремим групам населення)[77] або риторики ненависті (яка охоплює всі форми виразів, які поширюють, підбурюють, пропагують або виправдовують расову ненависть, ксенофобію, антисемітизм або інші форми ненависті, які ґрунтуються на нетерпимості).[78]

У випадку спланованого переслідування в Інтернеті жертва може розглянути певні альтернативні заходи, перш ніж відповісти кривднику, як-от проігнорувати коментарі, заблокувати користувача або повідомити про зловмисний

77 Рада Європи (2017 р.). Internet – Addressing the challenge. *Посібник з інтернет-грамотності*. Доступно в Інтернеті.

78 Рада Європи (б. д.). Hate speech in *Council of Europe Freedom of Expression*. Доступно в Інтернеті.

контент.[79] Якщо особа бажає доповісти про переслідування, важливо зробити екранні знімки образливого контенту в якості доказу. Також важливо пам'ятати, що відповідь може призвести до подальшого залучення агресора або інших інтернет-тролів чи хуліганів. З цієї причини, зіткнувшись із дезінформацією, важливо контролювати емоції, перш ніж писати відповідь. У більшості випадків найкращою тактикою буде трохи почекати й заспокоїтися та вирішити, який варіант подальших дій є оптимальним. Жертва переслідування в інтернеті може звернутися на онлайн-ресурси та довідкові лінії, які спеціалізуються на наданні необхідної допомоги.[80]

Пам'ятайте про ефект зворотнього вогню

Варто наголосити, що спроба виправлення може мати небажані наслідки, у тому числі підсилення хибних тверджень. Це називається «ефект зворотного вогню», який можна визначити як ситуацію, в якій «спроба виправлення ненавмисно підсилює віру у вихідну або невиправлену невірну інформацію, або покладання на неї».[81] Це може трапитися через властивість повторення викликати відчуття чогось знайомого, а знайома інформація часто сприймається як більш правдива, ніж нова інформація. Повторювання дезінформації може ускладнити її усунення з пам'яті людини, і читачі деколи пригадують її як реальний факт. Однак це не означає, що хибне твердження не слід згадувати під час викриття, оскільки в багатьох випадках його повторювання не становить жодної небезпеки, — деколи це навіть покращує ефективність виправлення.[82]

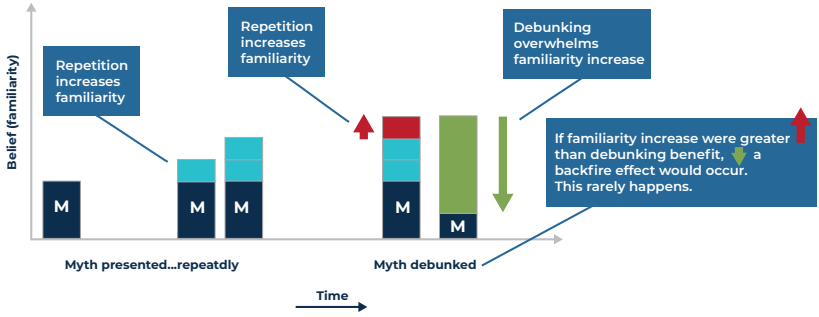
79 Endsleigh (б. д.). Що таке інтернет-тролінг? *Endsleigh*. Доступно в Інтернеті.

80 Прикладами організацій, які можуть надавати підтримку цього типу, є Access Now та The Cyber Helpline. Доступно в Інтернеті.

81 Ecker, U.K.H., Lewandowsky, S. & Chadwick, M. (2020 р.). Can corrections spread misinformation to new audiences? Testing for the elusive familiarity backfire effect. *Cognitive Research: Principles and Implications*, 5, 41.

82 Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, M. A., Kendeou, P., Lombardi, D., Newman, E. J., Pennycook, G., Porter, E. Rand, D. G., Rapp, D. N., Reifler, J., Roozenbeek, J., Schmid, P., Seifert, C. M., Sinatra, G. M., Swire-Thompson, B., van der Linden, S., Vraga, E. K., Wood, T. J., Zaragoza, M. S. (2020 р.). *The Debunking Handbook 2020*. Доступно в Інтернеті.

У певних випадках буде краще приділити більше уваги фактам, аніж міфу. Наприклад, створення допису в Інтернеті, який вказує на переваги й безпечність вакцини, може мати більший корисний ефект, ніж безпосереднє викриття пов'язаного з вакцинацією хибного твердження. У першому випадку ви створите перспективний набір тем для обговорення, а в другому можете ненавмисно перевести обговорення на хибне твердження, підсилюючи відчуття його «знайомості» у суспільній свідомості.[83] Тобто під час прийняття рішення щодо ужиття заходу або утримання від дій, слід вважати на можливість підсилення ефекту зворотного вогню.



Ілюстрація 58: Знайомість та ефект зворотнього вогню.
Джерело: Посібник з викриття.

Одним з найбільш ефективних підходів для уникнення ефекту зворотнього вогню є зосередження під час спілкування на фактах, а не на міфі, — це можна зробити використовуючи факти в якості заголовка або найбільш помітної частини викривного допису.[84]

83 ibid
84 Cook, J., Lewandowsky, S. (2011 p.). *The Debunking Handbook*.

Тим не менше, недавні свідчення не дають достатніх підстав для уникнення викриття через побоювання ефекту зворотного вогню.[85]

Чи достатньо у вас інформації для викриття хибного твердження?

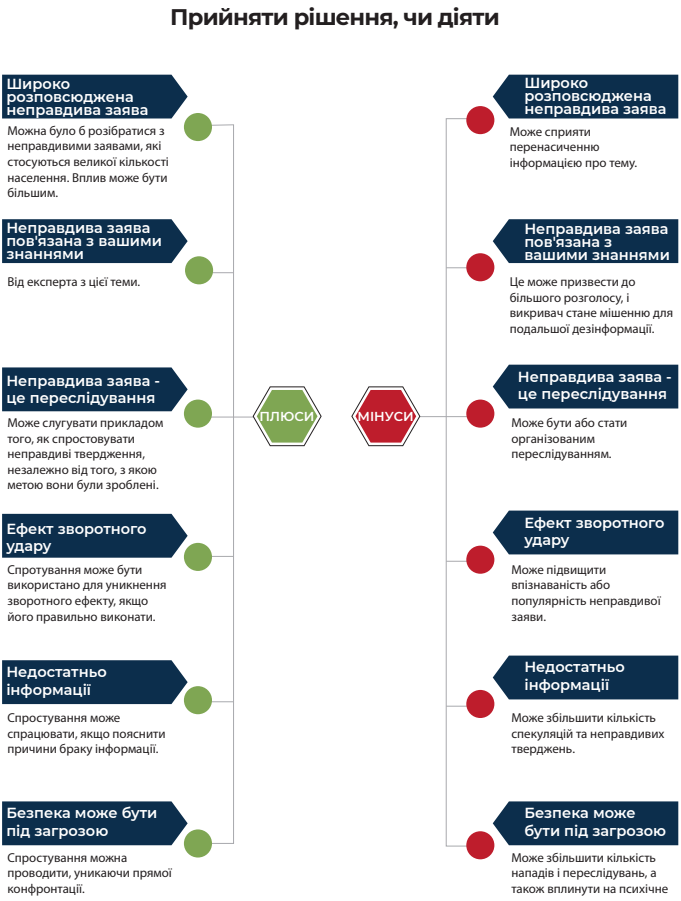
У деяких випадках жертви дезінформації можуть не володіти достатньою інформацією для викриття хибного твердження через те, що воно знаходиться за межами їхньої сфери компетенції або через брак достатньої інформації чи доказів на підтримки контраргументів. У цьому випадку можна повідомити аудиторію, що інформація є обмеженою або що оновлена інформація з'явиться пізніше по мірі розвитку ситуації. Наприклад, дезінформація може стосуватися нового вірусу, оцінка механізму передавання якого потребує додаткових досліджень. По мірі розвитку ситуації інформація з часом може змінюватися. За таких обставин уряд може уточнити, що наразі нові віруси є недостатньо вивченими й що результати оцінки ризику можуть змінитися по мірі розвитку ситуації. Таким чином до відома аудиторії доводиться, що інформація, надана урядом, може оновитися, якщо під час дослідження будуть виявлені нові аспекти.

85 Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, M. A., Kendeou, P., Lombardi, D., Newman, E. J., Pennycook, G., Porter, E. Rand, D. G., Rapp, D. N., Reifler, J., Roozenbeek, J., Schmid, P., Seifert, C. M., Sinatra, G. M., Swire-Thompson, B., van der Linden, S., Vraga, E. K., Wood, T. J., Zaragoza, M. S. (2020 p.). *The Debunking Handbook 2020.* Доступно в Інтернеті.

Пам'ятайте про безпеку!

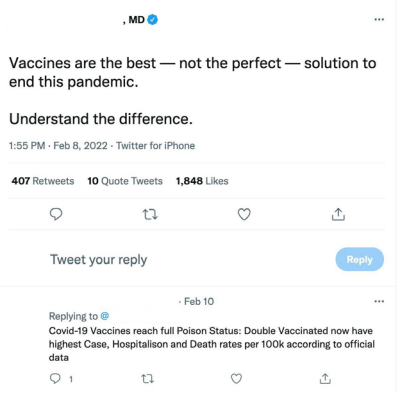
Дезінформація може надходити від екстремістських угрупувань. Важливо добре зважити, чи безперечно брати участь у бесіді з особами, які можуть бути схильними до проявів жорстокості. Наприклад, уявімо, що члени неонацистської організації вибрали об'єктом нападу особу або організацію. У такому разі жертва нападу повинна подумати, чи її відповідь не буде пов'язана з небезпекою для неї, оскільки неонацисти можуть організовувати інші типи нападів, як-от злам електронної пошти або переслідування в мережі. У таких ситуаціях викриття можна здійснити, реагуючи на хибні твердження цих угрупувань, не вдаючись до безпосередніх відповідей на коментарі й не згадуючи їхні назви (наприклад, крайні праві групи можуть безпідставно заявляти, що інститут займається створенням ядерної зброї; інститут може спростувати хибне звинувачення й пояснити, якою діяльністю він займається, не відповідаючи крайній правій групі безпосередньо).

На ілюстрації 59 підсумовано основні аспекти, на які слід вважати вирішуючи, чи варто відповідати на хибне твердження. На зображенні ліворуч перелічені деякі аргументи на користь викриття, в той час як праворуч наведені контраргументи.



Ілюстрація 59: Аспекти, на які слід вважати під час прийняття рішення.
Джерело: ЮНІКРІ.

Приклад прийняття рішення з приводу того, чи варто реагувати на дезінформацію, з якою ви зіткнулись, наведено нижче. На ілюстрації 60 показано відповідь користувача Twitter на повідомлення, розміщене лікарем. У випадку, який ми розглядаємо, лікар вирішив не викривати хибне твердження, оскільки користувач не послався на жодні джерела, а інші користувачі ніяк не прореагували на коментар.



На ілюстрації 61 наведено приклад викриття широко поширеного хибного твердження про засіб, який нібито виліковує COVID-19, замість спростування хибного твердження в поодинокому дописі або коментарі.

Ілюстрація 61: Приклад викриття широко поширеного хибного твердження про засоби, які нібито виліковують COVID-19.
Джерело: Twitter, ЮНЕСКО, опубліковано в 2022 р.

3.3 Етап 3: викриття дезінформації

Якщо особа або організація вирішує відповісти, настає третій етап, тобто викриття хибного твердження. Викриття можна розділити на дві фази: планування викривальних заходів та власне викриття.

Фаза планування

Перш ніж відповідати на хибне твердження, слід чітко визначити три аспекти: цільова аудиторія повідомлення, тема хибного твердження, яке планується спростувати, а також засоби або платформи, на яких буде передаватися повідомлення.

Ілюстрація 62: Аспекти, які слід розглядати під час планування стратегії викриття.
Джерело: ЮНІКРІ.

Визначення цільової аудиторії

Викриття має бути адаптоване під конкретну аудиторію. Найімовірніше, цільовою аудиторією буде конкретна група(-и), серед якої була поширена дезінформація. Якщо вибір цільової аудиторії не є очевидним, платформа або засоби поширення дезінформації або визначення характеристик групи можуть допомогти отримати додаткову інформацію (наприклад, якщо інформація поширюється в TikTok, готуючи відповідь, мабуть, потрібно орієнтуватися на підліткову цільову аудиторію).

Визначення цільової аудиторії

- Хто найбільше постраждав від дезінформації?
- Які групи більш схильні повірити неправдивій заяві? Враховуйте відповідні характеристики цільової групи (груп) залежно від теми (вік, стать, освіта, релігія, цінності, переконання, інтереси тощо)

Ілюстрація 63: Навідні запитання для визначення цільової аудиторії під час викриття дезінформації.
Джерело: ЮНІКРІ.

Визначення теми

Важливо вибрати, які саме хибні твердження будуть викриватися. Під час вибору дезінформації, яку планується викрити, важливо розглянути тип поширюваного хибного твердження, щоб заходи із викриття можна було зосередити на темах, як мають найбільший влив. Наприклад, деякі хибні твердження й міфи є більш поширеними, ніж інші. Деякі хибні твердження можуть мати сильніший вплив на суспільство, якщо їх не спростувати, що підвищує їхню пріоритетність з точки зору викриття. Крім того зосередити викривні заходи на правильній темі можуть допомогти деякі загальні запитання, наведені нижче. Які хибні твердження можуть мати найсильніші негативні наслідки? Яка інформація потрібна людям? (Визначити часті запитання або проблеми, пов'язані з дезінформацією). Які основні теми обговорюються під час поширення дезінформації? Чи існують запитання або теми, пов'язані з поширюваною дезінформацією, які ви можете передбачити й викрити?

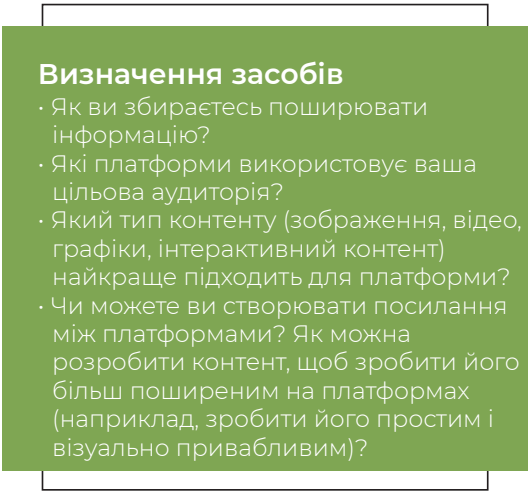
Приклади в період пандемії COVID-19

Як передбачити/попередити дезінформацію про...
- Звідки походить вірус?
- Способи передачі?
- Можливі заходи щодо стримування?
- Політика щодо імунізації?

Ілюстрація 64: Приклад навідних запитань для визначення хибних тверджень, які потрібно спростувати.
Джерело: ЮНІКРІ.

Визначення засобів

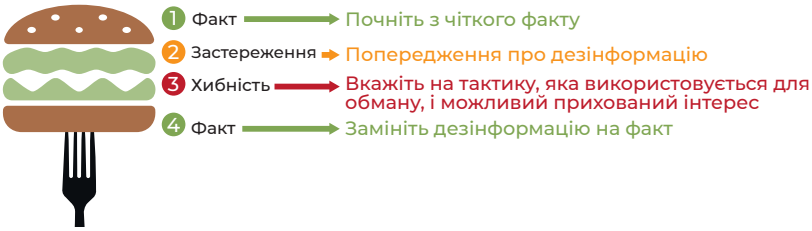
Залежно від того, хто є цільовою аудиторією, можуть застосовуватися різні засоби поширення. Тип контенту та стратегія залежить від вибраної платформи. Наприклад, якщо робота з викриття ведеться у TikTok, тоді найкращим варіантом буде створити коротке відео з інформацією. Якщо викривач збирається використовувати Facebook, тоді варто розглянути публікацію дописів із графікою, які доповнюватимуть відео.



Ілюстрація 65: Навідні запитання для визначення засобів викриття хибної інформації.
Джерело: ЮНІКРІ.

Фаза виконання

Існують різні готові моделі викриття дезінформації.[86] Однією з найефективніших технік є розроблений лінгвістом Джорджем Лакоффом так званий «сендвіч правди». Метод сендвіча правди складається з чотирьох елементів.



Ілюстрація 66: Приклад використання стратегії «сендвіча правди» для попереднього й основного викриття. Ідею запропонував лінгвіст Джордж Лакофф. **Джерело:** ЮНІКРІ.

1 Факт → Почніть з чіткого факту

Розпочніть з фактів, які підкріплюють верифіковану інформацію: викриття слід починати з **верифікованої фактичної інформації**, викладеної у простий спосіб. Інформація не повинна бути складною й повинна мати роз'яснювальний характер. Помітність фактичної інформації також можна покращити за допомогою відповідного заголовку або назви. Факт не слід викладати у формі

86 Garcia, L., & Shane, T. (2021 p.). A guide to prebunking: a promising way to inoculate against misinformation in *First Draft*. Доступно в Інтернеті. Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, M. A., Kendeou, P., Lombardi, D., Newman, E. J., Pennycook, G., Porter, E. Rand, D. G., Rapp, D. N., Reifler, J., Roozenbeek, J., Schmid, P., Seifert, C. M., Sinatra, G. M., Swire-Thompson, B., van der Linden, S., Vraga, E. K., Wood, T. J., Zaragoza, M. S. (2020 p.). *The Debunking Handbook 2020*. The Debunking Handbook 2020. Cook, J., Lewandowsky, S. (2011 p.). *The Debunking Handbook*. Доступно в Інтернеті.

запереченння або покладатися на те, що дезінформатор зречеться своїх слів (наприклад, «це твердження є неправдивим»).[87]

2 Застереження → Попередження про дезінформацію

Попередження й реагування на хибне твердження: другим елементом сендвіча правди є виразне попередження про те що інформація, візуальний або аудіоконтент, який незабаром буде опубліковано, є хибним.[88] Важливо, щоб під час реагування на дезінформацію хибна інформація повторювалась лише один раз, безпосередньо перед виправленням. Слід уникати непотрібних повторювань, щоб мінімізувати ризик «зворотного вогню» або створення ефекту знайомості хибного твердження. Крім того, викриття може бути більш ефективним за наявності пояснення того, чому джерелу дезінформації не варто вірити й що є справжньою метою дезінформації (наприклад, підрив довіри до уряду або збагачення).

3 Хибність → Вкажіть на тактику, яка використовується для обману, і можливий прихований інтерес

Пояснення помилковості: пояснення хибного твердження й чому воно є невірним — це третій елемент сендвіча правди. Виправлення слід презентувати в такий спосіб, щоб вони контрастували з помилковою інформацією, для забезпечення чіткого спростування. Слід повністю виключити ситуацію, коли аудиторія зможе проігнорувати виправлення або пропустити його, навіть під час

87 Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, M. A., Kendeou, P., Lombardi, D., Newman, E. J., Pennycook, G., Porter, E. Rand, D. G., Rapp, D. N., Reifler, J., Roozenbeek, J., Schmid, P., Seifert, C. M., Sinatra, G. M., Swire-Thompson, B., van der Linden, S., Vraga, E. K., Wood, T. J., Zaragoza, M. S. (2020 p.). *The Debunking Handbook 2020.* Доступно в Інтернеті.

88 Cook, J., Lewandowsky, S. (2011 p.). *The Debunking Handbook*. Доступно в Інтернеті.

поверхневого вивчення інформації. Цього можна досягти, якщо використовувати для пояснення просту й лаконічну мову, а також графічні елементи для підкреслення фактів, як-от більший шрифт або різні кольори. Також потрібно докладно пояснити, чому важливо виправити хибне твердження, чому після викриття стає очевидним, що твердження було хибним і чому альтернативне пояснення є вірним. Демонстрація невідповідностей у дезінформації може запобігти поверненню аудиторії до переконань, які у неї були до ознайомлення з виправленням. Надійність і репутація особи або організації, які здійснюють викриття, є ще одним важливим елементом, на якому слід наголосити, щоб спростування твердження було успішним. Використання надійних джерел допомагає створювати більш переконливі відповіді. Щоб читач звернув увагу на джерела, повідомлення слід адаптувати до конкретних цільових груп.[89]

4 Факт ➡ Замініть дезінформацію на факт

Повторно сформулюйте факт: наприкінці процесу замініть дезінформацію фактами, переконавшись, що в доповіді немає прогалин.[90] В більшості випадків викладення факту, який заповнює «прогалину» в поясненні, викриття значно полегшується, тому що факт може замінити неточну інформацію в первинному уявленні, яке склалося в особи, новою версією того, що сталося.[91]

Під час розробки стратегії викриття слід вважати на наведені нижче аспекти.[92]

89 ibid
90 ibid
91 Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, M. A., Kendeou, P., Lombardi, D., Newman, E. J., Pennycook, G., Porter, E. Rand, D. G., Rapp, D. N., Reifler, J., Roozenbeek, J., Schmid, P., Seifert, C. M., Sinatra, G. M., Swire-Thompson, B., van der Linden, S., Vraga, E. K., Wood, T. J., Zaragoza, M. S. (2020 p.). T*he Debunking Handbook 2020.* Доступно в Інтернеті.
92 ibid

- **Почніть із заголовка**: заголовок повинен бути чітким і лаконічним викладенням факту. Однак в якості заголовка не слід використовувати заперечне речення.

- **Додайте подробиць, але без зайвої детальності**: поясніть, чому твердження є хибним, але не перевантажуйте аудиторію інформацією. Завдання полягає в тому, щоб збільшити віру людей та забезпечити їх контраргументами, які дозволять їм викрити твердження, коли вони з ним зіткнуться.

- **Коротко описати використовувані методи й тактику**: під час викриття хибного твердження нагадайте аудиторії, що ця тактика не є унікальною й використовується не лише в цьому випадку.

- **Поясніть, звідки у викривачів інформація, яку вони поширюють, і що вам досі невідомо**: поясніть, як були отримані відомості, щоб побудувати довірчі відносини. Цей процес може забезпечити аудиторію більш чітким розумінням під час аналізу протиріччя між фактом і міфом та озброює її інструментами, які дозволять легше відкидати хибні твердження в майбутньому. Крім того, пояснивши аудиторії, що деяка інформація залишається невідомою, ви попередите її про те, що по мірі розвитку ситуації деякі факти можуть змінитися. В такому разі під час надання інформації може бути корисно зосередитися на консенсусі на поточний момент часу, нагадуючи, на чому зійшлися експерти й чому.

- **Не залишайте прогалин у вашій оповіді:** інформація, якої бракує в пояснені, може бути замінена дезінформацією. Це може призвести до витрачання ресурсів на неодноразове спростування того ж самого хибного твердження, на подальше

уточнення інформації, що може призвести до плутанини, оскільки ви реагуватимете на хибне твердження багато разів і щоразу наводитиме різні факти під час спроб його викриття.

- **Нехай ваша інформація буде стислою й простою (так званий принцип KISS від англ. «Keep it short and simple»)**: під час викриття слід звертати першочергову увагу на чіткість, лаконічність і послідовність. Це зменшить ймовірність ефекту зворотного вогню або спантеличування цільової аудиторії.[93]

- **Використовуйте малюнки та інші візуальні елементи**: може бути корисним застосувати графіку для відображення ключових фактів, оскільки інформація виглядатиме більш привабливо як з точки зору її прочитання, так і з точки зору поширення на платформах соціальних мереж. Це також полегшить її розуміння, адже в такому разі буде забезпечена її стислість і простота.

Ілюстрація 67: Аспекти, які слід брати до уваги під час випереджувального й основного викриття.
Джерело: ЮНІКРІ.

93 Changing Minds. (б. д.). Keep it short and simple (принцип KISS). *Changing Minds Organisation*. Доступно в Інтернеті.

На ілюстраціях 68 і 69 показано два приклади того, як застосовувати сендвіч правди під час викриття дезінформації. У наведених прикладах викриття розпочинається з викладення факту, а не повторення міфу, після чого робиться попередження, що інформація, яку буде спростовано, є хибною, і, нарешті, згадується неправдива інформація й пояснюється, чому вона є невірною. Наприкінці ще раз викладається факт, як ми це бачимо на прикладі. Після кожного прикладу структури сендвічу правди наводяться приклади можливих дописів, в яких показано, як спростування можна подати у графічній формі.

1 Факт

Американський Червоний Хрест приймає донорську кров від людей, вакцинованих проти COVID-19.

Почніть з фактів, які підтверджують перевірену інформацію

2 Застереження

Неправдива заява була поширена в кількох повідомленнях у соціальних мережах.

Додайте чіткі застереження про те, що контент, який буде представлений, є неправдивим

3 Хибність

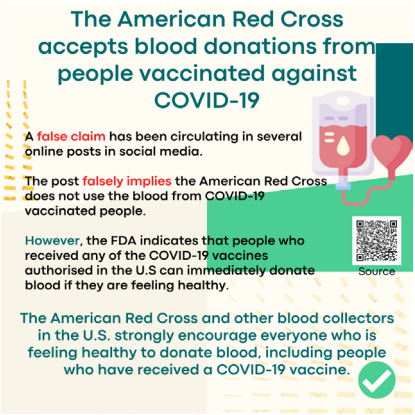
У **дописі помилково стверджується**, що Американський Червоний Хрест не використовує кров вакцинованих від COVID-19 людей. **Однак** FDA вказує, що люди, які отримали будь-яку з дозволених у США вакцин проти COVID-19, можуть одразу ж здати кров, якщо вони почуваються здоровими.

Поясніть, в чому полягає неправдиве твердження і чому воно не відповідає дійсності

4 Факт

Американський Червоний Хрест та інші організації зі збору крові в США наполегливо закликають усіх, хто почувається здоровим, здавати кров, включно з людьми, які отримали вакцину проти COVID-19.

Замініть дезінформацію фактами в кінці процесу



Ілюстрація 68: Приклади викриття хибного твердження, пов'язаного з роллю організації (Американського Червоного хреста) під час пандемії COVID-19. Приклад ґрунтується на хибному твердженні, спростованому фактчекерами.[94]
Джерело: ЮНІКРІ.

94 Jaramillo, C. (2022 р.). Red Cross accepts blood donations from people vaccinated against COVID-19. *FactCheck.org*. Доступно в Інтернеті.

1 Факт

Віспа мавп - це захворювання, що передається від тварини до людини (зооноз).

Почніть з фактів, які підтверджують перевірену інформацію

2 Застереження

Неправдива заява поширюється у відеоролику, який розповсюджується на різних платформах соціальних мереж.

Додайте чіткі застереження про те, що контент, який буде представлений, є неправдивим

3 Хибність

У **допису помилково стверджується**, що мавпяча віспа - це біологічна війна, яку ВООЗ, МВФ та Білл Гейтс розв'язали проти громадськості. **Спалах** мавпячої віспи не був спричинений біологічною війною.

Поясніть, в чому полягає неправдиве твердження і чому воно не відповідає дійсності

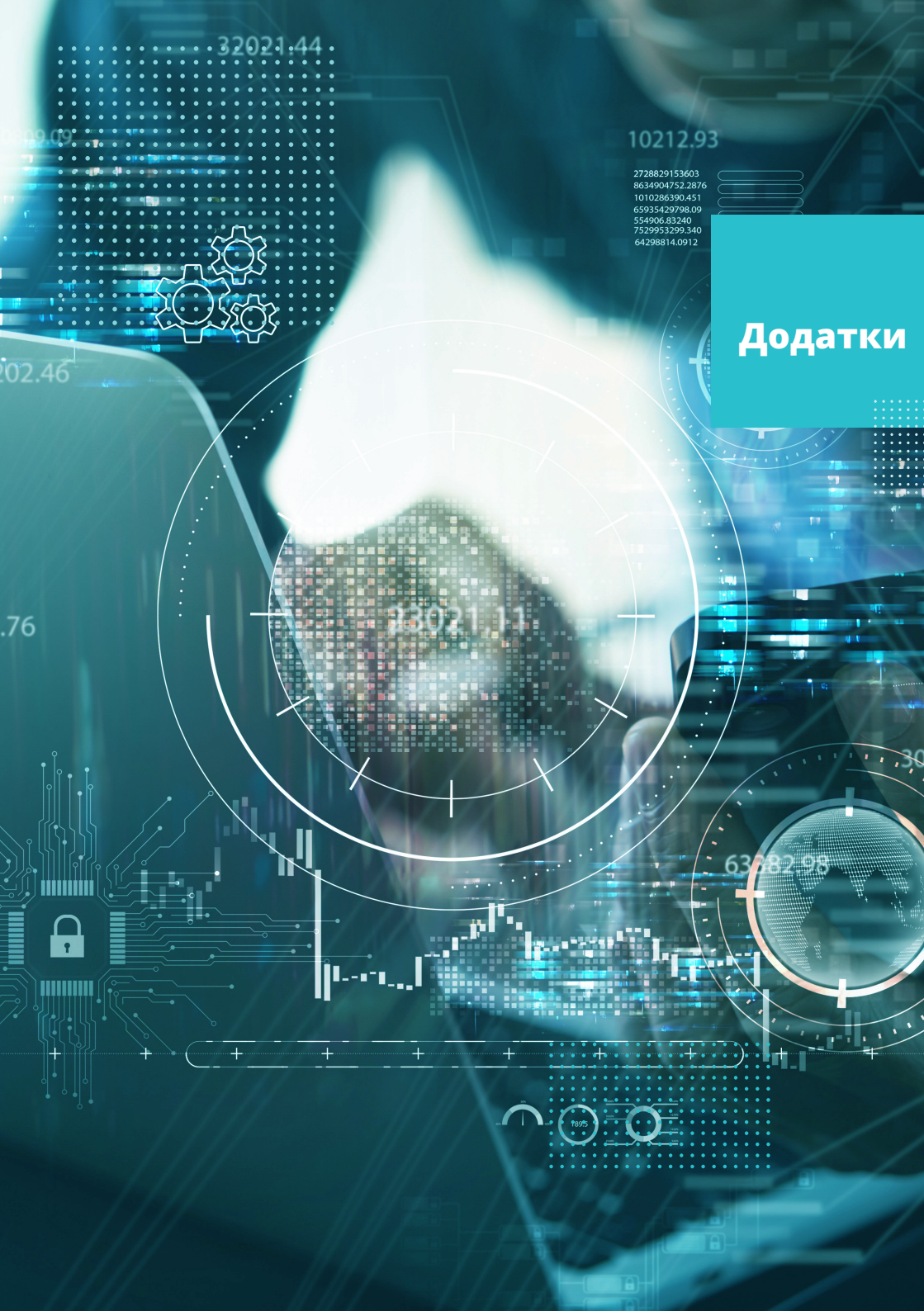
4 Факт

Захворювання було виявлено у 1958 році у мавп, а перший випадок захворювання у людини був зафіксований у 1970 році. Було кілька спалахів серед людей, але жоден з них не був пов'язаний з біологічною війною.

Замініть дезінформацію фактами в кінці процесу

Ілюстрація 69: Приклади викриття хибного твердження, пов'язаного з роллю різних акторів під час спалаху віспи мавп в 2022 році. Приклад ґрунтується на хибному твердженні, спростованому фактчекерами.[95]
Джерело: ЮНІКРІ.

95 Rahman, G. (2022 p.). No evidence monkeypox is an agent of biological warfare. *Full Fact*. Доступно в Інтернеті.


32021.44
10212.93
2728829153603
8634904752.2876
1010286390.451
65935429798.09
554906.83240
7529953299.340
64298814.0912
Додатки

Була створена низка технічних засобів для сприяння роботі з випереджувального й основного викриття. Ці засоби ґрунтуються на різних підходах, як-от гейміфікація або покращення навичок медіаграмотності. Наведений перелік засобів не є вичерпним. Тим не менше, в ньому містяться огляди деяких наявних технічних засобів, які можуть допомогти викрити або зрозуміти явища дезінформації.

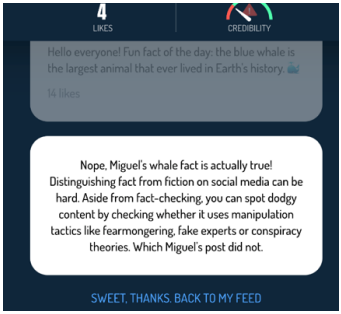
Додаток 1: Технічні засоби випереджувального викриття

Різні технічні засоби допомагають розвивати навички медіаграмотності, у тому числі обізнаність з випереджувальним та основним викриттям. Оскільки випереджувальне викриття здійснюється до поширення дезінформації, ці технічні засоби зосереджуються на покращені навичок осіб, зокрема навичок виявленні методів дезінформації й стратегій суб'єктів, які користуються цими методами.

У деяких технічних засобах для заохочення людей до активного тренування[96] їхніх навичок випереджувального викриття використовується гейміфікація.

Bad News: Це онлайн-гра, метою якої є зробити гравцям, що є представниками різних культур, «щеплення» від фальшивих новин. Основна увага у цій грі приділяється випереджувальному викриттю методів невірної інформації та дезінформації. У користувачів з являється розуміння методів, за допомогою яких поширюється дезінформація. У грі до гравців застосовується типова тактика фальшивих новин, роблячи їх «сьогунам» фальшивих новин. Виграє той гравець, який публікуючи заголовки привабив найбільше підписників.[97]

Go Viral: Це гра, яка ґрунтується на Bad News, що спеціалізується на невірній інформації про COVID-19.[98]

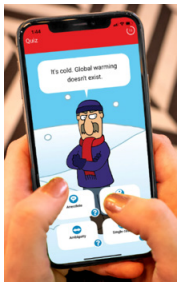


96 «Процес додавання до чогось (наприклад, завдання) ігор або ігрових елементів для заохочення до участі». Визначення отримано з: Merriam-Webster. (б. д.). Gamification definition & meaning. *Merriam-Webster*. Доступно в Інтернеті.

97 https://www.getbadnews.com/#intro

98 https://www.goviralgame.com/en/play

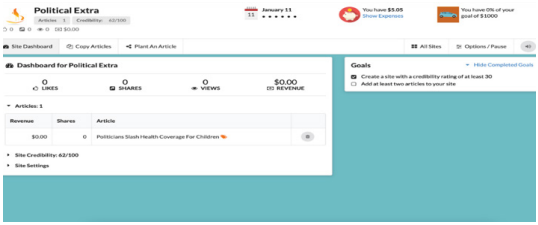
Cranky Uncle: У цій гру використовується гумор і критичне мислення для викриття методів введення в оману, а саме заперечення наукових фактів, а також побудова здатності опиратися невірній інформації. У цій грі гравці мають наставника-мультиплікаційного персонажа, який є персоніфікацією заперечувача науки про клімат, який пояснює 14 методів заперечення наукових фактів (включно з фальшивими експертами, вибірковим підходом і різними логічними помилками).[99]



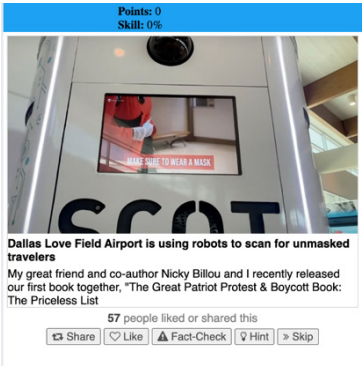
Factitious-Pandemic Edition: це гра, створена для відточування навичок виявлення фальшивих новин. В грі також є посилання на джерело новин, що допомагає користувачам тренувати навички визначення надійного джерела.[100]

99 https://crankyuncle.com/game/
100 http://factitious-pandemic.augamestudio.com/#/

Fake It to Make It: користувачу потрібно створити персонажа, мету та вебсайт, а щоб досягти поставленої мети, особа повинна створити фальшиві новини. Гра побудована на припущенні, що підвищуючи поінформованість гравців щодо процесу створення й розповсюдження фальшивих новин, можна виховати в них більш скептичне ставлення до інформації, з якою вони зіткнуться в майбутньому.[101]

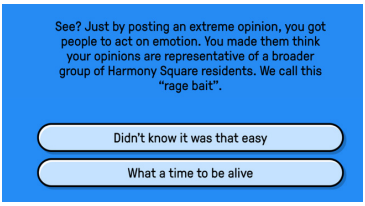


Fakey: це імітація стрічки новин, у якій користувачу потрібно аналізувати різні історії, а кінцевою ціллю гри є навчання медіаграмотності й вивчення взаємодії людей з невірною інформацією.[102]



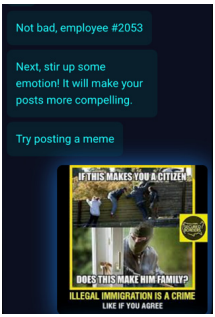
101 https://www.fakeittomakeitgame.com/
102 https://fakey.osome.iu.edu

Harmony Square: ця гра створена для демонстрації різних тактик і методів маніпуляції, які використовуються для введення людей в оману, залучення послідовників або недобросовісного використання соціальної напруги в політичних цілях. Гра була задумана як «психологічна» вакцина від дезінформації, яка створюється шляхом виховання когнітивного опору. Місцем дії гри є житловий район, мешканці якого одержимі демократією; один з гравців призначається на роль головного спеціаліста з дезінформації, чиїм завданням є провокування внутрішніх чвар і нацьковування мешканців одне на одного.[103]



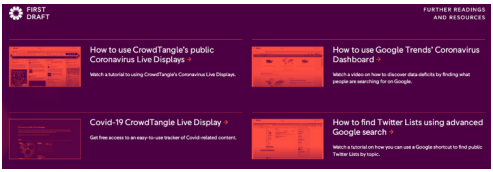
Troll Factory: ця гра демонструє, як працюють інформаційні операції у соціальних мережах, показуючи на реальних прикладах контенту із соціальних мереж, як фальшиві новини, емоційний контент і армії ботів використовуються для впливу на настрої й прийняття рішень.[104]

Інші підходи передбачають використання курсів, настанов, інфографіки та інших матеріалів для забезпечення осіб інструментами для випереджувального викриття хибних тверджень.



103 https://harmonysquare.game/en
104 https://trollfactory.yle.fi/

First Draft — Дізнайтеся, як виявляти невірну інформацію та міфи про вакцини: Цей курс складається з 20-хвилинних сесій, які зосереджені на навичках дослідження, моніторингу, верифікації тощо.[105] Відео включають посібники із самостійного вивчення. Організація пропонує інші інструменти, як-от онлайн-завдання з верифікації контенту,[106] численні посібники з покращеної онлайн-журналістики,[107] і віртуальна дошка з інструментами для верифікації й відповідальної звітності.[108]



Міжнародний центр для журналістів (ICFJ) Ресурси для журналістів: ресурс «Освітлення новин під час пандемії COVID-19: ресурси для журналістів», метою якого є забезпечення інструментами для навчання у спеціалістів з охорони здоров'я та інших експертів. Він надає доступ до вебінарів, присвячені різним темам, включно з дезінформацією про охорону здоров'я, керування студіями новин та останні дослідження COVID-19. Цей інструмент також включає нові ресурси з освітлення новин про COVID-19, поради для журналістів, тенденції та можливості журналістики й надає можливість співпраці з іншими особами.[109]

105 https://firstdraftnews.org/vaccine-insights-flexible-learning-course/
106 https://ftp.firstdraftnews.org/articulate/2020/en/OVC/story_html5.html
107 https://firstdraftnews.org/long-form-article/first-drafts-essential-guide-to/
108 https://start.me/p/vjv80b/first-draft-basic-toolkit
109 https://www.icfj.org/resources

Додаток 2: Технічні засоби викриття

Як зазначалося у випадку із випереджувальним викриттям, технічні засоби можуть виявитися корисними інструментами для підвищення ефективності викриття. Ці інструменти можуть використовуватися на трьох етапах викриття, описаних раніше (аналіз дезінформації, прийняття рішення й реалізація стратегії). Ось деякі з цих інструментів:

Аналіз дезінформації

Виявлення ботів: у більшості випадків інструменти можуть автоматично виявляти, чи обліковий запис є акаунтом бота. Наприклад, Bot Sentinel[110] використовує штучний інтелект для перевірки облікових записів Twitter і класифікує їх як достовірні або недостовірні, допомагаючи користувачам виявляти ботів. Виявлені облікові записи ботів зберігаються в базі даних для відстеження їхньої щоденної активності. Зібрані дані можуть використовуватися для дослідження впливу пропаганди з використанням ботів на дискурс і пошуку шляхів протидії поширенню розповсюджуваної ними дезінформації.

Іншим подібним інструментом є Botometer,[111] який використовує машинне навчання, щоб визначати, наскільки активність облікового запису Twitter є подібною до діяльності, характерної для ботів. Він аналізує особливості профілю, як-от друзі, структура взаємовідносин із соціальними мережами, тимчасова активність, мова та настрій дописів. Після цього він присвоює обліковому запису загальний бал, який вказує на ступінь ймовірності того, що акаунт належить боту.

Hoaxy[112] — це інструмент, який шукає твердження, відстежуючи поширення посилань на повідомлення з

110 https://botsentinel.com/info/about
111 https://botometer.osome.iu.edu
112 https://hoaxy.osome.iu.edu

джерел з поганою репутацією та незалежні фактчекінгові організації. Програма також підраховує бал бота, який вказує на ймовірний ступінь автоматизації.

Інтерфейс Hoaxy

Фактчекінгові вебсайти й інструменти: ClaimBuster[113] — це мережевий інструмент для моментального фактчекінгу, який використовує штучний інтелект (обробка природної мови та інші методи навчання з вчителем) для визначення фактичної й фальшивої інформації. Іншим інструментом є SciCheck,[114], доступний на FactCheck.org, який спеціалізується на фальшивих та оманливих псевдонаукових твердженнях.

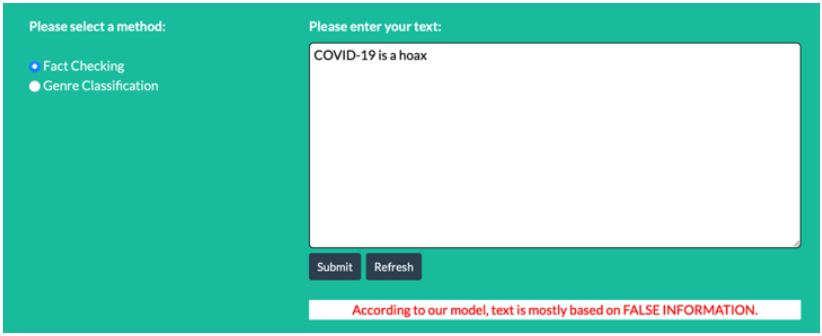
У якості інших прикладів можна навести Lead Stories,[115], мережеву фактчекінгову платформу, яка виявляє фальшиві або оманливі повідомлення, плітки та теорії змови. Движок цього сайту Trendolizer™ індексує посилання з різних інтернет-джерел, а потім вимірює ступінь зацікавленості, який вони викликають, щоб визначати трендовий контент. Потім цей котент піддається фактчекінгу силами власної команди журналістів.

Fake News Detection[116] — це інструмент, якій збирає новинні статті, достовірність яких буде перевірена фактчекінговими вебсайтами, і використовує їх для навчання систем класифікації текстів. Ви можете вставити текст й перевірити

113 https://idir.uta.edu/claimbuster/
114 https://www.factcheck.org/scicheck/
115 https://leadstories.com/how-we-work.html
116 http://fakenews.research.sfu.ca/#footer

його подібність до текстів, які містяться в бібліотеці справжніх та фальшивих новинних статей цієї платформи.

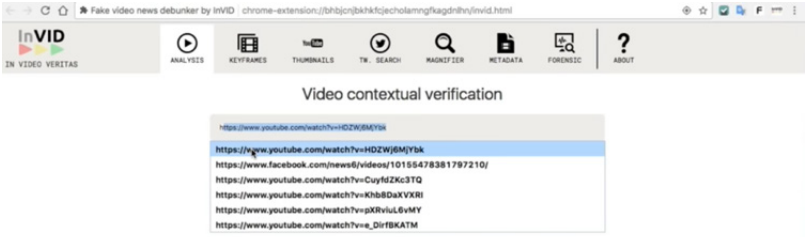
До інших прикладів можна віднести The Vaccines Insights Hub[117] з віртуальною дошкою із свіжими інсайтами, аналітикою й настановами із звітування щодо нової невірної інформації про охорону здоров'я та вакцинацію, а також інструменти фактчекінгу Google[118] (Fact Check Explorer та Fact Check Markup Tool), призначенням яких є полегшення праці фактчекерів, журналістів і дослідників.



Інтерфейс Fake News Detection

Рейтинги вебсайтів та джерел інформації: до інших інструментів належать розширення браузера, які оцінюють достовірність контенту, коли користувач переглядає інформацію в Інтернеті, сервіс HealthGuard від NewsGuard[119] або Our.News,[120] які використовують спеціальні ярлики, щоб повідомляти по надійність джерела. Ще існують такі варіанти як Media Bias/Fact Check, FakerFact, TrustServista, Check та TrustedNews.[121] Ще одним прикладом є плагін Video Verification Plugin (InVid)[122], який отримує контекстуальну інформацію й верефікує контент в соціальних мережах.

117 https://firstdraftnews.org/vaccineinsights/
118 https://toolbox.google.com/factcheck/explorer
119 https://www.newsguardtech.com/solutions/healthguard/
120 https://our.news/how-it-works/?main
121 https://thetrustedweb.org/browser-extensions-to-detect-and-avoid-fake-news/
122 https://www.invid-project.eu/tools-and-services/invid-verification-plugin/



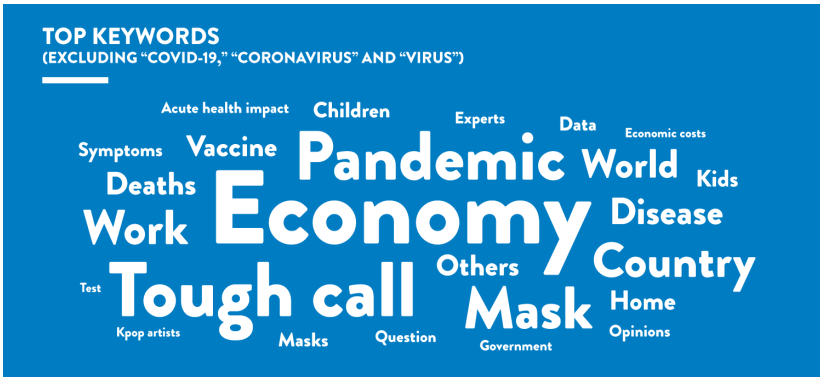
Інтерфейс InVid

Вибір теми

Соціальне прослуховування за допомогою штучного інтелекту: під час вибору теми, яку належить викрити у фазі виконання, можна використовувати соціальне прослуховування для визначення тем, які наразі обговорюються більшістю. Це може допомогти зосередити зусилля на популярних темах та часто отримувати свіжу інформацію про актуальні теми.

ВООЗ вже використовує технічні засоби для впровадження стратегії прослуховування соціальних мереж, яка дозволить визначати основні теми, пов'язані з охороною здоров'я, що обговорюються в мережі. Це робиться з використанням машинного навчання для аналізу інформаційних повідомлень на різних платформах соціальних мереж. Після цього здійснюється пошук на основі таксономії, щоб цю інформацію можна було віднести до відповідних тем.[123] Машинне навчання також може допомогти зрозуміти, які емоції відчувають користувачі. Засоби мовної аналітики не просто поділяють данні за типом ставлення (позитивне, нейтральне, негативне) — вони можуть розпізнавати тривогу, смуток, заперечення, прийняття та інші емоції, виражені у дописах соціальних мереж. Ця інформація може використовуватися для побудови ефективної стратегії захисту та заспокоєння суспільства до того, як невірна інформація набере оберти.

123 ВООЗ (2020 р.). Immunizing the public against misinformation. *Всесвітня організація охорони здоров'я*. Доступно в Інтернеті.



Основні теми, що стосуються охорони здоров'я, визначені ВООЗ станом на 9-15 липня.
Джерело: ВООЗ.

Опанування та тренування навичок

Ігровий підхід: як і у випадку з випереджувальним викриттям, основне викриття теж може мати інтерактивний характер. Captain Fact[124] є вебсайтом, робота якого побудована за принципом колективної модерації. На сайті використовується ігровий підхід, реалізований шляхом накладання текстової інформації на відео (для цього потрібне розширення браузера) — до відео, які переглядаються в інтернеті, додаються джерела та контекст. Накладання тексту на відео означає, що вебсайт може використовуватися як платформа для дебатів, оскільки користувачі можуть послідовно ставити під сумнів усе, про що говориться у відео. У Myth Busters Quiz від ВООЗ (вікторина «Руйнівники міфів»)[125] також використовується ігровий підхід: користувачам надається можливість перевірити їхні знання популярних міфів і фактів про COVID-19.

124 https://captainfact.io/
125 https://www.facebook.com/watch/ref=saved&v=433416304464216

Інтерфейс Myth Busters Quiz від ВООЗ

Інші ініціативи: проводилася й інша діяльність з покращення викривальної роботи: наприклад, були укладені принципи Міжнародної мережі фактчекінгу[126] для організацій, які звітують про точність заяв або інших поширених тверджень, пов'язаних з важливими суспільними питаннями. Механізм ВООЗ для протидії інфодемії[127] — це механізм, який ґрунтується на наборі навичок, метою якого є визначення пріоритетності й вирішення проблем надмірності й неточності інформації про інфодемію COVID-19.

126 https://www.poynter.org/ifcn-fact-checkers-code-of-principles/
127 https://www.who.int/publications/i/item/9789240010314