

# ІНФОРМАЦІЙНА ВІЙНА: АНАЛІЗ ФЕНОМЕНА

Олександр Тягло

**Анотація.** Інформаційна війна ґрунтується на різного роду матеріальних явищах і ставить за мету в певний спосіб вплинути на матеріальний світ. Однак вона включає й не менш необхідну та важливу — ідеальну — складову, що вкорінена у психіці окремих людей, людських спільнот і зазвичай відображується назовні, сприймається, викликається до життя та організовується через застосування мови, візуалізацію тощо. Моя розвідка присвячена логіко-філософському аналізу саме цієї складової інформаційної війни.

Соціальні мережі й електронні ЗМІ, ширше — Internet, сьогодні виявляються чи не найважливішим полем ведення ідеальної складової інформаційної війни. Велику інформаційну небезпеку в Internet становлять професійні тролі та боти, організовані у «фабрики тролів», «ботоферми». Їх головний продукт — масове поширення замовної (дез)інформації. Для цього продукуються множина вигаданих «істот» — «військо інформаційних ляльок-солдатів» із певними іменами та профілями в соціальних мережах. Традиційно публікація під псевдонімом є виправданим чи навіть законним засобом забезпечення життя, інших прав автора. Ситуація набуває нового загрозливого характеру, коли людська активність масово переміщується в кіберпростір, і ще й за умов інформаційної війни. Тут використання псевдонімів забезпечує не тільки анонімність, а й масове продукування троями та ботами «інформаційних ляльок-солдатів».

У розвідці виявлені деякі елементарні способи ідентифікації тролів. Разом із фактчекінгом вони корисні в забезпеченні від зловиякісних інформаційних впливів, але не завжди достатні. Це стосується випадків, коли, зокрема, рознощик дезінформації, намагаючись уникнути явного обману, вдається до логічних хитрощів. Тут не обійтися без знання хоч би основ логіки та вміння критичного мислення. Це вимагає посилення й оновлення масового викладання цих дисциплін у школах і вишах.

Підкреслено, що дієва національна система ведення ідеальної складової інформаційної війни має поєднувати відповідні групи фахівців із компетентних державних структур, спеціалізований персонал медіа, профільні громадські організації, інформаційних волонтерів. Та в ідеалі кожен має бути навчений надавати собі сам бодай первинну допомогу проти дезінформації.

**Ключові слова:** інформаційна війна, ідеальна складова інформаційної війни, інтернет, троль, ідентифікація троя, «інформаційна лялька-солдат», логіка, критичне мислення.

## I

Усе більша частина людства долучається до способу життя, у якому інформація набула статусу базової цінності. Аби переконатися в цьому навіть без глибокодумних студій, достатньо подивитися на список 10 найбагатших сьогодні людей світу [1]. Б. Гейтс і С. Балмер (Microsoft), Л. Пейдж і С. Брін (Google), а також Л. Елісон (Oracle) безпосередньо пов'язані з забезпеченням сучасного оперування чи споживання інформації. І. Маск (Tesla, SpaceX), Дж. Безос (Amazon) чи В. Бафет (Berkshire Hathaway) уособлюють не видобування нафти та газу чи виробництво чавуну та сталі, а новітню знаннєву економіку, суттєво ґрунтовану на продукуванні, розповсюдженні, використанні чи споживанні інформації і знань.

Тривалий час в осмисленні наявної ситуації наголос робився на, так би мовити, «світлому боці сили» інформації, інформаційних технологій. Майже всі практично беззастережно раділи, що їм випало жити у зростаючому на очах майже необмеженими темпами всесвітньому інформаційному середовищі. Правда, ще у 2005 році у Всесвітній доповіді ЮНЕСКО «До спільнот знань» було наголошено, що розвиток глобального інформаційного суспільства в напрямку спільнот знань не тільки дозволяє значно збільшити обсяги доступної інформації та швидкість оперування нею, а й примушує *кожну людину вміти вільно орієнтуватися у здатному поглинути її потоці інформації, розвивати когнітивні вміння та вміння критичного мислення з тим, аби відрізнити «корисну» інформацію від «позбавленої користі»* [2, с. 19]. Але тоді «темний бік сили» інформації і пов'язаних з нею технологій був тільки м'яко означений відповідно, вочевидь, їх ще не зовсім дозрілий потузі й достатньо усвідомлений небезпеці. Сьогодні ж м'якого нагадування про необхідність «триматися на плаву» у всепоглинаючому океані інформації, лагідного застереження щодо марнотратного споживання його «позбавленою користі» вмісту вже абсолютно недостатньо. Часто-густо вміст цього океану виявляється не лише «позбавленим користі», а й отруйним, смертельно небезпечним. Тому не можна обійтись без жорстко реалістичного — найширшого та систематичного — вивчення та роз'яснення загрози маси фатальних «бермудських трикутників» — хитро прихованої хиби, майстерно організованої брехні, місінформації та дезінформації, що доставляється всесвітній аудиторії загалом, практично кожній локальній спільноті та нормальній людині як традиційними мас-медіа, так і новітніми соціальними мережами, телеграм-каналами тощо. Однією з актуальних

конкретизації цієї загрози є феномен інформаційної воєнної активності, або, скорочено, інформаційної війни (information warfare) — як самостійної активності за переважно «мирних часів», так і невід’ємної складової «гарячої» гібридної війни.

У російсько-українських відносинах інформаційна війна жевріла практично з часу розпаду СРСР та утворення незалежної і суверенної України, суттєво підсилюючись із розгортанням відкритої гібридної агресії російської держави на початку 2014 року. Створювані тут загрози та реальну шкоду цілком підтверджує, наприклад, фрагмент звернення Президента України 16 липня 2022 року, в якому згаданий фейк про нібито масований російський ракетний удар по Україні. В. Зеленський підкреслив, що *таким чином ворог намагається доповнити ракетний та артилерійський терор проти України це й інформаційним терором*. Зрештою він узагальнив ситуацію так.

Іноді інформаційна зброя може зробити більше, ніж зброя звичайна. Очевидно, що будь-якими ракетами й артилерією Росії не вдасться зламати нашу єдність і збити нас зі своєї дороги. І так само очевидним має бути й те, що українську єдність не зламати брехнею чи залякуванням, фейками чи теоріями змови [3]<sup>1</sup>.

Як же забезпечити ефективну реалізацію цього імперативу?

## II

Розгляну далі стислі, але достатні для цієї розвідки, роз’яснення феномену інформаційної війни, розміщені на офіційному сайті НАТО [4].

Інформаційна війна — це діяльність, здійснювана задля досягнення інформаційної переваги над ворогом. Вона полягає, з одного боку, у контролі власного інформаційного простору, у захисті доступу до власної інформації, а з іншого — в одержанні та використанні інформації супротивника, у знищенні його інформаційних систем і порушенні інформаційних потоків.

У цьому фрагменті ясно виділені два боки інформаційної війни: як будь-яка типова війна задля досягнення переваги, зрештою перемоги, вона передбачає захист, убезпечення свого та порушення, руйнування чи захоплення ворожого.

---

<sup>1</sup> Фактчекінг виявляє, що 16 липня росіяни справді завдали ракетного удару по Україні з району Каспійського моря, здійнявши стратегічні бомбардувальники Ту-95МС. Але було випущено лише 6 ракет, а не 40. Українська ППО збила 4 з 6 ракет, дві ракети влучили в сільськогосподарське підприємство на Черкащині.

Важливим полем інформаційної війни сьогодні є кіберпростір і пов'язана з ним сфера нових технологій. Кібервійна (cyberwar activities) може полягати в кібератаках, руйнуванні інформаційних систем супротивника, але також і у так званих соціальних кібератаках, створюючи у свідомості людей певну картину світу, що відповідає тим цілям інформаційної війни, яку веде певна країна.

Інформаційна війна, як і будь-яка значуща людська активність, здійснюється на перетині двох фундаментальних реальностей — матеріальної й ідеальної. У матеріальному світі вона пов'язана із захистом чи нападом на інформацію, точніше — на її матеріальні носії чи процеси накопичення, збереження, передавання і т. ін. Та хоча повноцінна інформаційна війна не може існувати, не ґрунтуючись на різного роду матеріальних явищах і не ставлячи за мету в певний спосіб вплинути на матеріальний світ, вона включає й не менш необхідну та важливу ідеальну складову, що вкорінена у психіці окремих людей, людських спільнот і зазвичай відображується назовні, сприймається, викликається до життя й організовується через застосування мови, візуалізацію тощо. Без потрібного результативного впливу на людські цінності, світогляд, усталені методи мислення чи алгоритми спілкування навіть досягнення якихось матеріальних воєнних цілей не буде, у загальному випадку, ані ефективним, ані остаточним<sup>2</sup>.

Моя розвідка за мету має аналіз саме цієї — ідеальної — складової інформаційної війни, що піддається вираженню в термінах логіки та критичного мислення. Водночас важливість особливих суто психологічних чи інших аспектів аналізованого феномена визнається, але вони залишені поза розглядом.

Інтернет посилює та розширює можливості одержання даних, захисту чи знищення інформації, а також полегшує вплив як на громадян певної країни, так і на міжнародні спільноти. З огляду на швидкість комунікації, широке охоплення та низьку вартість заходів (дез)інформації, вирішальну роль тут відіграють соціальні мережі. Сайти соціальних мереж є також цінним джерелом відомостей про цільові групи, на які

---

<sup>2</sup> У такому зв'язку варто звернути увагу на міркування знаного російського теоретика гібридної війни О. О. Бартоша, опубліковане в центральному журналі російського міністерства оборони: «В гибридной войне на роль ключевых факторов, определяющих революционные изменения в формах и методах конфликта и формирование его нового качества, выдвинулись глобализация и развитие информационно-коммуникационных технологий... Война смыслов составляет сердцевину стратегии гибридной войны, главная цель которой заключается в обеспечении последовательного планомерного установления контроля над всеми сторонами жизни государства — объекта гибридной агрессии, и прежде всего над менталитетом его населения» [5, с. 13].

спрямовують (дез)інформаційну діяльність. Типові засоби інформаційної війни через Internet наступні:

- Фабрики тролів — угруповання, члени яких, тобто тролі, зі вказаною замовником метою розміщують коментарі в Internet, використовуючи за цих обставин несправжні, оманливі профілі в соціальних мережах.
- Боти — програми, які автоматично надсилають повідомлення, наприклад, у відповідь на появу ключового слова.
- Фейкові новини, фейки — повідомлення, спрямовані на введення в оману користувачів різного роду медіа [4].

Зі сказаного зрозуміло, чому саме соціальні мережі й електронні ЗМІ, ширше — інтернет, а загалом — кіберпростір останнім часом виявляється чи не найважливішим полем ведення ідеальної складової інформаційної війни, реально конкуруючи з іще недавно всемогутнім «телевізором» (див., напр., дані соціологічного дослідження, виконаного Центром Разумкова в 2020 році [6]).

Стосовно наведеного переліку типових «інформаційних бойових одиниць» зауважу наступне. Хоча вдосконалення штучного інтелекту вже дозволяє замінити ним у нескладних ситуаціях людські істоти, однак у вітчизняній традиції ботами інколи називають не тільки спеціальні програми, але і людей, за функціями схожих на тролів: із цього погляду показовим є відомий в Україні фільм-розслідування «Я — бот» [7] (див. також: [8]). Власне тролі тут відрізняються скоріше однозначно негативною спрямованістю своєї активності; це, так би мовити, явно «погані хлопці» — свідомі брехуни, провокатори і т. ін. Трапляються тролі-одинаки, тролі-любители, але регулярнішу та набагато більш концентровану інформаційну небезпеку створюють професійні тролі та боти. Вони є кінцевими виконавцями в чисельних добре організованих угрупованнях — «фабриках тролів», «ботофермах» — зі значним фінансуванням з боку різноманітних замовників, зокрема політичних чи державних структур<sup>3</sup>. Їх головний продукт — масове поширення замовної інформації чи дезінформації, фейків і

<sup>3</sup> «Facebook заявляє, що з 2017 року він виявив кампанії з дезінформації в більш ніж 50 країнах. Звіт підсумовує 150 операцій з дезінформації. В цілому, згідно з аналізом, Росія була найбільшим постачальником дезінформації: за чотири роки там виявили 27 операцій з впливу. З них 15 були пов'язані з розташованим в Санкт-Петербурзі Агентством інтернет-досліджень (IRA) або іншими організаціями, пов'язаними з Євгеном Пригожиним, російським олігархом, що тісно пов'язаний з президентом Росії Володимиром Путіним. Ще чотири російські мережі були пов'язані з кремлівськими спецслужбами, а ще дві — з сайтами російських ЗМІ» [9]. Протягом останніх років розглядувана

маніпулятивних меседжів, для чого створюється множина вигаданих «істот» — «військо інформаційних ляльок-солдатів» із певними іменами та профілями в соціальних мережах.

Частка та вплив тролів і ботів у спілкуванні в Internet зростає<sup>4</sup>. Інколи це спілкування чи не буквально перетворюється на «війну ботів і тролів», де щирі людські істоти опиняються в меншості. Розгляну та прокоментую в такому зв'язку показовий приклад.

Так, 27 червня 2022 року «Українська правда» опублікувала новину щодо загибелі внаслідок російського обстрілу мешканців Лисичанська [13]. Із 16 коментарів і коментарів до коментарів 8 одразу викликають сумнів, оскільки реальні автори чи їх «інформаційні ляльки-солдати» мають чисті аватарки, тобто прагнуть анонімності.

Крім того, «істоти» з іменами «Станіслав Укр», «Аманян Акапян» і ще дві мають й абсолютно чисті профілі у Facebook. Поєднання вже двох вказаних обставин дозволяє, згадуючи наведену раніше нагівську характеристику, із достовірністю ідентифікувати їх як «інформаційних ляльок» якихось анонімних тролів.

Ті, хто іменуються «Oleksiy Shepotko», «Микола Ветров» і ще двоє, теж мають чисті аватарки. Хоча в їх профілях у Facebook наявні якісь мінімальні відомості, однак замало, а їх правдивість важко або

---

ситуація набула характеру, так би мовити, масової і регулярної повсякденності. Так, вже без будь-якого натяку на сюрприз, знаходимо у повідомленні від 28 серпня 2021 року, що СБУ у Києві викрили потужну ботоферму, ворожа інтернет-агентура використовувала її для дискредитації України перед міжнародною спільнотою. І далі: *«Як зазначили у прес-службі відомства, за завданням своїх “кураторів” зловмисники поширювали через соцмережі антиукраїнські гасла та дезінформацію щодо результатів проведення “Кримської платформи”. Основна діяльність зловмисників була сфокусована на мережах Facebook, Instagram та TikTok. Для розповсюдження викривлених фактів та відвертої дезінформації вони адміністрували понад 15 тисяч анонімних акаунтів, а свої дописи публікували від імені “пересічних громадян”* [10]. А 5 серпня 2022 року «Українська правда» повідомила: *«Meta видалила 45 акаунтів “тролів” у соціальній мережі Facebook і 1037 — в Instagram і продовжує блокувати їхні спроби повернутися [...] У звіті компанії зазначається, що ці “тролі” працювали щодня “з невеликою перервою на обід”, а деякі публікували і проросійські, і проукраїнські коментарі з різницею в кілька хвилин. Meta розпочала розслідування після публікації, яка викриває “фабрику тролів”, робота якої публічно координувалася через телеграм-канал “Кібер фронт Z”. У ході розслідування Meta виявила спроби “заспамити” пости в Instagram, Facebook, TikTok, Twitter, YouTube, LinkedIn, “ВКонтакте” та “Однокласники”* [11].

<sup>4</sup> Це глобальне явище. Останнім часом набула розголосу скандальна відмова І. Маска купувати Twitter. Десь за 44 мільярди доларів, оскільки ця популярна у всьому світі соцмережа, як підозрюють, має не менше 5% фальшивих, або спам-користувачів щодня [12].

**Станислав Укр**

Вже не має чому дивуватися, тварюки до мозгу кісток .

Позначка «Подобається» · 👍 29 · 5 тиж.

**Oleksiy Shepotko**

Та не просити треба евакуюватись. А примусово евакуювати дітей. До людей не дійде поки власна хата не почне горіти. Позбавляти батьків батьківських прав, якщо вони можуть але не хочуть евакуювати власних дітей. Це безвідповідальне і суспільно небезпечно ставлення батьків. Своєю бездією вони наражають дітей на небезпеку. Держава має втрутитись. Передавати таких дітей органам опіки і евакуювати негайно. Взагалі з питання примусової евакуації дітей з прикордонних і прифронтових зон Верховна Рада має зміни до законодавства прийняти, а Зеленський ці зміни ініціювати. У воєнний час потрібно дозволити примусову евакуацію дітей з лінії фронту держаними органами без усякої бюрократії і рішень суду.

Позначка «Подобається» · 👍 43 · 5 тиж. · Відредаговано

**Микола Ветров**

і куди їм краще їхати? Порадьте, якщо можете.

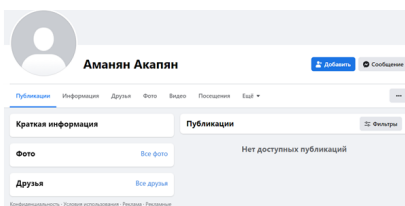
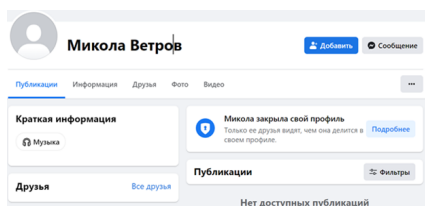
Позначка «Подобається» · 👍 5 · 5 тиж.

**Аманян Акапян**

Да, да, може розстріл хто нехоче евакуйовуватись?

Позначка «Подобається» · 👍 2 · 5 тиж.

взагалі неможливо перевірити щонайменше без спеціальних знань і витрат часу, на що типовий читач новин навряд чи налаштований. Тож, із високим ступенем ймовірності, який здається достатнім з огляду на рівень коментарів у популярному електронному ЗМІ, можна стверджувати, що це теж або тролі, або їх «ляльки».



Не можна не побачити, що в розглянутій ситуації тролі обстоюють суттєво відмінні, навіть несумісні за смыслом позиції: у принципі, феномен троля, тролінга не має якоїсь державної, партійної чи сталої військової прив'язки. Це новітнє відтворення явища колишніх ландскнехтів, продажних найманців, що воюють виключно за гроші, тут-і-зараз на боці того, хто їх тут-і-зараз утримує.

Використання псевдонімів у літературі чи медіа — далеко не нове явище. Наприклад, небагато хто чув про Ф. М. Аруе, хоча Вольтер широко відомий усьому світові. Використовувати псевдоніми, публі-

куватися без реальної самоідентифікації — це давній засіб приховати своє походження чи соціальне становище, уникнути утисків Святої інквізиції чи світської влади... Тож, в історичній ретроспективі публікація під псевдонімом — часто-густо зовсім не підступна маніпуляція чи брехня. І сьогодні цей спосіб захисту життя, інших прав автора визнається законним, не пов'язаним необхідно з прагненням увести в оману. Зокрема, у п. 5 ст. 25 чинного Закону України «Про інформацію» вказано: *«Журналіст має право поширювати підготовлені ним матеріали за власним підписом або під умовним ім'ям»*.

Ситуація набуває нового загрозливого характеру, коли людська активність масово переміщується у створюваний електронними ЗМІ чи соціальними мережами кіберпростір і ще й за умов інформаційної війни. Тут використання псевдонімів, що забезпечує не тільки анонімність тролів і людей-ботів, а й масове продукування ними «інформаційних ляльок-солдатів», досить часто є ознакою зл�якісних впливів. Анонім під псевдонімами, троль чи людина-бот виступає практично безвідповідальним джерелом чи рознощиком замовної дезінформації, брехливої пропаганди, виконавцем різного роду воєнних інформаційних операцій супротивника. А залучення штучного інтелекту здатне усунути фактично всі суттєві обмеження чисельності «війська інформаційних ляльок-солдатів».

Тому, зіткнувшись із повідомленням, коментарем «істоти» з чистою або сумнівною аватаркою, із чистим або таким, що вимагає часу та спеціальних знань для перевірки вмісту профілю в соціальній мережі, підозрілим — надто простим, штучним тощо — ім'ям, слід бути дуже уважним, аби не опинитися під впливом ворожого троля, бота. Це, звичайно, не убезпечить від пасток дезінформації абсолютно, але зменшить можливість уведення в оману, зрештою — заподіянущою шкоду.

Простодушню ж сприймати описаного аноніма під псевдонімами за добродесного співучасника спілкування, поспіхом відповідати на меседжі його «інформаційних ляльок-солдатів» навряд чи розумно. Натомість найпершою реакцією тут має бути ясна публічна ідентифікація цих — за вихідним припущенням, презумптивно — небезпечних «істот» кіберпростору.

### III

Сумлінний фактчекінг, вказані вище елементарні заходи убезпечення від недоброякісних чи навіть ворожих інформаційних впливів тролів і ботів є корисними, але не завжди достатніми. Це стосується



множини випадків, коли, зокрема, рознощик дезінформації, брехливої пропаганди, намагаючись уникнути занадто відвертого обману, вдається до логічних хитрощів, замаскованих пасток.

У матеріалі Громадської мережі «Опора» від 18 липня 2022 року проаналізовані деякі приклади сьогоденної російської пропаганди та вказано, серед іншого, таке.

[Вона] не вигадує нічого нового та використовує ті самі прийоми пропаганди, що й Радянський Союз. Зокрема, йдеться про тактику під назвою “whataboutism”, спрямовану на дискредитацію опонента твердженням, що той сам не діє відповідно до своєї позиції. При цьому первісні аргументи опонента не спростовують, а їх хибність не доводять. Цю тактику використовують для того, щоб зірвати обговорення одного питання, змусивши замість нього обговорювати інше [14].

Далі наведений конкретний випадок із брифінгу одіозної речниці російського МЗС.

Описане зовсім не асоціюється з активністю анонімного троля, до того ж вміло підібрані факти можуть і не бути самі собою брехливими. Хитрість тут інша, її особливий варіант відомий навіть не з радянських часів, а ще з історії Давнього світу — це аргумент до людини (*argumentum ad hominem*), або атака особи. Загалом ця хитрість полягає в порушенні загальнологічного закону тотожності, у повній підміні тези, коли оцінка змісту певного твердження підмінюється оцінкою якостей суб'єкта (особи, спільноти, держави і т. ін.), який його артикулював чи підтримує. Для аудиторії, що обмежена використанням тільки природного здорового глузду, до того ж у насиченій емоціями атмосфері за умови браку часу тощо такого роду хитрощі досить часто спрацьовують. Тому, прагнучи не потрапити до хитро розставлених інформаційних пасток ворога, не опинитися під його шкідливим впливом, не можна обійтися без засвоєння хоч би основ науки логіки та вміння критичного мислення. Це вимагає посилення та якісного оновлення викладання відповідних дисциплін у школах і вишах [15, 16].

Ворога в інформаційній війні, як і у «гарячій» гібридній війні загалом, не можна недооцінювати: він досить часто виявляється не тільки численним і підступним, а й розумним і підготовленим. Тому й наш арсенал належної зброї мусить бути потужним, різноманітним і готовим до бою, ще більшою мірою це стосується і, так би мовити, особового складу. Його неприпустимо обмежити тільки групами фахівців із різноманітних державних структур, зокрема з Державної

служби спеціального зв'язку і захисту інформації України [17], Центру протидії дезінформації при РНБО України тощо. Тут не обійтися без роботи спеціалізованого персоналу самих медіа, що вже виконує, наприклад, адміністрація Facebook, відстежуючи та блокуючи активність тролів і ботів. Але і цього замало: доцільною є участь громадських організацій на кшталт «Центру Медіареформи» з флагманським проектом «StopFake», а також уже підготовлених за своєю освітою чи самоосвітою і внутрішньо вмотивованих інформаційних волонтерів. Нарешті, нагальною залишається задача медіа-освіти найширшої аудиторії споживачів інформації. На неформальному міжнародному рівні цим активно займається ЮНЕСКО, на загальноукраїнському, наприклад, «Академія української преси», а на місцевому, серед інших, одеська «Школа місцевого самоврядування». В ідеалі — завдяки синергії формальної та неформальної освіти — кожен телеглядач, радіослухач, читач новин у друкованих ЗМІ чи відвідувач соціальної мережі має бути навчений надати собі сам бодай первинну допомогу проти дезінформації, типових хитрощів і маніпуляцій.

#### IV

Основні висновки цієї короткої розвідки полягають у наступному.

Сила інформації, інформаційних технологій має не тільки «світлий», а і вкрай небезпечний «темний бік». Він зростає та набуває істотної ваги завдяки інформаційній военній активності, або, скорочено, інформаційній війні — як самостійної активності за переважно «мирних часів», так і невід'ємної складової «гарячої» гібридної війни.

Хоча повноцінна інформаційна війна не може існувати, не ґрунтуючись на різного роду матеріальних явищах і не ставлячи за мету в певний спосіб вплинути на матеріальний світ, однак вона має й не менш необхідну та важливу ідеальну складову. Ця складова піддається дослідженню засобами насамперед логіки та критичного мислення.

Соціальні мережі й електронні ЗМІ, ширше — інтернет, сьогодні виявляється чи не найважливішим полем ведення ідеальної складової інформаційної війни, реально конкуруючи зі ще недавно всемогутнім «телевізором».

Хоча розвиток штучного інтелекту вже дозволяє замінити ним у нескладних ситуаціях людські істоти, однак у вітчизняній традиції ботами інколи називають не тільки спеціальні програми, але і людей, за функціями схожих на тролів. Власне тролі тоді відрізняються скоріше однозначно негативною спрямованістю своєї активності.

Регулярну та концентровану інформаційну небезпеку створюють професійні тролі та боти, організовані у «фабрики тролів», «ботоферми» зі значним фінансуванням із боку різноманітних замовників, зокрема політичних чи державних структур. Їх головний продукт — масове поширення замовної інформації чи дезінформації, фейків і маніпулятивних меседжів, для чого створюється множина вигаданих «істот» — «військо інформаційних ляльок-солдатів» із певними іменами та профілями в соціальних мережах.

В історичній ретроспективі публікація під псевдонімом часто-густо зовсім не є підступною маніпуляцією чи брехнею. Та й сьогодні цей спосіб захисту життя, інших прав особи визнається законним, не пов'язаним необхідно з намаганням увести в оману. Ситуація набуває нового загрозливого характеру, коли людська активність масово переміщується в кіберпростір та ще й за умов інформаційної війни. Тут використання псевдонімів, що забезпечує не тільки анонімність тролів і людей-ботів, а й можливість масового продукування ними «інформаційних ляльок-солдатів», досить часто є ознакою зляканих впливів.

Зіткнувшись із повідомленням, коментарем «істоти» з чистою або сумнівною аватаркою, із чистим або таким, що вимагає часу та спеціальних знань для перевірки профілем у соціальній мережі, підозрілим — надто простим, штучним тощо — ім'ям, слід бути дуже уважним, аби не опинитися під впливом ворожого троля, бота.

Сумлінний фактчекінг та інші елементарні заходи убезпечення від недоброякісних чи навіть ворожих інформаційних впливів тролів і ботів є корисними, але не завжди достатніми. Це стосується множини випадків, коли, зокрема, рознощик дезінформації, брехливої пропаганди, намагаючись уникнути занадто відвертого обману, вдається до логічних хитрощів, замаскованих пасток для природного здорового глузду. Тому, прагнучи не опинитися під шкідливим впливом ворога, не можна обійтися без знання хоч би основ науки логіки, без вміння критичного мислення. А це вимагає посилення й оновлення масового викладання відповідних дисциплін у школах і вишах.

Дієва національна система ведення ідеальної складової інформаційної війни мусить поєднувати відповідні групи фахівців компетентних державних структур, спеціалізований персонал медіа, профільні громадські організації, інформаційних волонтерів. Нагальною залишається задача медіа-освіти найширшої аудиторії споживачів інформації. В ідеалі кожен телеглядач, радіослухач, читач новин у друкованих ЗМІ чи відвідувач соціальної мережі має бути навчений надавати собі

сам бодай первинну допомогу проти дезінформації, типових хитроців і маніпуляцій.

## Література

1. *The richest people in the world. Forbes world's billionaires list.* 2022. URL: <https://www.forbes.com/billionaires/>
2. *Towards knowledge societies: UNESCO world report.* Paris: UNESCO Publ., 2005. URL: <https://unesdoc.unesco.org/ark:/48223/pt0000141843>
3. *Ракетами та артилерією Росії не вдасться зламати нашу єдність і збити нас зі свого шляху — звернення Президента України. Президент України Володимир Зеленський. Офіційний веб-сайт.* 16 липня 2022. URL: <https://www.president.gov.ua/news/raketami-ta-artileriyeyu-rosiyi-ne-vdastsya-zlamati-nashu-ye-76521>
4. *Information warfare. Media – (Dis)Information – Security.* 2020. URL: [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf)
5. *Бартош А.А. Стратегия и контрстратегия гибридной войны. Военная мысль.* 2018. № 10. С. 5-16. URL: <https://cyberleninka.ru/article/n/strategiya-i-kontrstrategiya-gibridnoy-voyny>
6. *Як змінилися уподобання та інтереси українців до засобів масової інформації після виборів 2019 р. та початку пандемії COVID-19 (серпень 2020 р.).* URL: <https://razumkov.org.ua/napiamky/sotsiologichni-doslidzhennia/yak-zminylys-upodobannia-ta-interesy-ukraintsiv-do-zasobiv-masovoi-informatsii-pislia-vyboriv-2019r-ta-pochatku-randemii-covid19-serpen-2020r>
7. *Фільм-розслідування «Я — бот». Спільний проект «Нromadske.ua» і «Слідство. Інфо».* 2019. URL: <https://www.youtube.com/watch?v=s5O-j0gXtno>
8. *Кишак В. Війни ботів. Як працюють українські армії медіа-кілерів у Facebook. Українська правда.* 3 лютого 2020. URL: <https://www.pravda.com.ua/articles/2020/02/3/7239192/>

9. *Facebook*: Україна стала одним з найбільших постачальників дезінформації. *Українська правда*. 27 травня 2021. URL: <https://www.pravda.com.ua/news/2021/05/27/7295015/>
10. СБУ викрила потужну ботоферму, що працювала на РФ проти «Кримської платформи». *Українська правда*. 28 серпня 2021. URL: <https://www.pravda.com.ua/news/2021/08/28/7305299/>
11. Мазуренко А. Мета видалила більше 1000 фальшивих акаунтів, які підтримали вторгнення РФ в Україну. *Українська правда*. 5 серпня 2022. URL: <https://www.pravda.com.ua/news/2022/08/5/7362051/>
12. Павлич О. Маск викликав главу Twitter на публічні дебати щодо ботів соцмережі. *Економічна правда*. 7 серпня 2022. URL: <https://www.epravda.com.ua/news/2022/08/7/690115/>
13. Карловський Д. Росіяни обстріляли натовп у Лисичанську: 8 загиблих, 21 поранених. *Українська правда*. 27 червня 2022. URL: <https://www.pravda.com.ua/news/2022/06/27/7355043/>
14. War speeches. Казки про «нацизм» та «русофобію» від російської пропаганди. *Українська правда*. 18 липня 2022. URL: <https://www.pravda.com.ua/columns/2022/07/18/7358751/>
15. Тягло О.В. Досвід засвоєння критичного мислення в українській вищій школі. *Філософія освіти. Philosophy of Education*. 2017. №2(21). С. 240-257. URL: [https://www.researchgate.net/publication/324840890\\_Dosvid\\_zasvoenna\\_kriticnogo\\_mislenna\\_v\\_ukrainskij\\_visij\\_skoli](https://www.researchgate.net/publication/324840890_Dosvid_zasvoenna_kriticnogo_mislenna_v_ukrainskij_visij_skoli)
16. Тягло О.В. Чи просто «увімкнути критичне мислення»? *Зміст освіти та освітні практики нової української школи: матеріали всеукраїнського освітнього форуму «Зміст освіти та освітні практики Нової української школи» (Полтава, 28 квітня 2021 р.)*. Полтава: ПОШПО, 2021. С. 66-74. URL: [https://www.researchgate.net/publication/341740957\\_Taglo\\_OV\\_Ubezpecenna\\_spozivanna\\_informacii\\_-\\_viklik\\_sucasnomu\\_gromadanskomu\\_suspilstvu](https://www.researchgate.net/publication/341740957_Taglo_OV_Ubezpecenna_spozivanna_informacii_-_viklik_sucasnomu_gromadanskomu_suspilstvu)
17. Шиголь Ю. Інформаційна безпека: ще один фронт боротьби за Україну, за який має нести відповідальність держава. *Українська правда*. 12 червня 2021. URL: <https://www.pravda.com.ua/columns/2021/06/12/7296926/>

## References

1. *The richest people in the world. Forbes world's billionaires list.* 2022. URL: <https://www.forbes.com/billionaires/>
2. *Towards knowledge societies: UNESCO world report.* Paris: UNESCO Publ., 2005. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000141843>
3. *Russia's missiles, artillery not to be able to break our unity, to throw us off our path—address of President of Ukraine. President of Ukraine Volodymyr Zelenskyy. Official website.* 16 July 2022. URL: <https://www.president.gov.ua/news/raketami-ta-artileriyeyu-rosiyi-ne-vdastsya-zlamati-nashu-ye-76521>
4. *Information warfare. Media – (Dis)Information – Security.* 2020. URL: [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf)
5. *Bartosh A.A. Strategy and counterstrategy of hybrid war. Military thought.* 2018. # 10. P. 5-16. URL: <https://cyberleninka.ru/article/n/strategiya-i-kontrstrategiya-gibridnoy-voyny>
6. *How Ukrainians' preferences and interests in mass media changed after the 2019 elections and the start of the COVID-19 pandemic (August 2020). Razumkov center.* URL: <https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/yak-zminylys-upodobannia-ta-interesy-ukraintsiv-do-zasobiv-masovoi-informatsii-pislia-vyboriv-2019r-ta-pochatku-pandemii-covid19-serpen-2020r>
7. *Investigative film “I am a bot”. Joint project “Hromadske.ua” and “Investigation. Info”.* 2019. URL: <https://www.youtube.com/watch?v=s5O-j0gXtno>
8. *Kishchak V. Bot wars. How Ukrainian armies of media killers work on Facebook. Ukrainska pravda.* 3 February 2020 p. URL: <https://www.pravda.com.ua/articles/2020/02/3/7239192/>
9. *Facebook: Ukraine has become one of the biggest suppliers of disinformation. Ukrainska pravda.* 27 May 2021. URL: <https://www.pravda.com.ua/news/2021/05/27/7295015/>

10. *The SBU* exposed a powerful bot farm operating for the Russian Federation against the Crimean Platform. *Ukrainska pravda*. 28 August 2021. URL: <https://www.pravda.com.ua/news/2021/08/28/7305299/>
11. *Mazurenko A.* Meta deleted more than 1,000 fake accounts that supported the invasion of the Russian Federation in Ukraine. *Ukrainska pravda*. 5 August 2022. URL: <https://www.pravda.com.ua/news/2022/08/5/7362051/>
12. *Pavlysh O.* Musk called the head of Twitter to a public debate about the bots of the social network. *Ekonomichna pravda*. 7 August 2022. URL: <https://www.epravda.com.ua/news/2022/08/7/690115/>
13. *Karlovskiy D.* Russians fired at the crowd in Lysychansk: 8 killed, 21 wounded. *Ukrainska pravda*. 27 June 2022. URL: <https://www.pravda.com.ua/news/2022/06/27/7355043/>
14. *War* speeches. Tales of “Nazism” and “Russophobia” from Russian propaganda. *Ukrainska pravda*. 18 July 2022. URL: <https://www.pravda.com.ua/columns/2022/07/18/7358751/>
15. *Tiaglo O.* Experience of mastering of critical thinking in the Ukrainian higher education. *Філософія освіти. Philosophy of Education*. 2017. # 2(21). P. 240-257. URL: [https://www.researchgate.net/publication/324840890\\_Dosvid\\_zasvoenna\\_kritichnogo\\_mislenna\\_v\\_ukrainskij\\_visij\\_skoli](https://www.researchgate.net/publication/324840890_Dosvid_zasvoenna_kritichnogo_mislenna_v_ukrainskij_visij_skoli)
16. *Tiaglo O.* Is it simple to “turn on critical thinking”? *Content of education and educational practices of the New Ukrainian school: materials of the all-Ukrainian educational foresight “Content of education and educational practices of the New Ukrainian school” (Poltava, April 28, 2021)*. Poltava: POIPPO. 2021. P. 66-74. URL: [https://www.researchgate.net/publication/341740957\\_Taglo\\_OV\\_Ubezpecenna\\_spozivanna\\_informacii\\_-\\_viklik\\_sucasnomu\\_gromadanskomu\\_suspilstvu](https://www.researchgate.net/publication/341740957_Taglo_OV_Ubezpecenna_spozivanna_informacii_-_viklik_sucasnomu_gromadanskomu_suspilstvu)
17. *Shyhol Yu.* Information security: one more front of the struggle for Ukraine, for which the state should bear responsibility. *Ukrainska pravda*. 12 June 2021. URL: <https://www.pravda.com.ua/columns/2021/06/12/7296926/>

**INFORMATION WARFARE:  
AN ANALYSIS OF THE PHENOMENON**

**Oleksandr Tiaglo**

**Abstract.** Information warfare is based on different material phenomena and aims to influence the material world in a certain way. However, it also includes an equally necessary and important — ideal — constituent, which is rooted in psyche of individuals, human communities and is usually reflected outward, perceived, introduced into life and organized through relevant use of language, through visualization, etc. My research is devoted to the logical and philosophical analysis of this particular constituent of information warfare.

Social networks and electronic media, more widely — the Internet is almost the most important field for conducting the ideal component of information warfare today. Professional trolls and bots organized into “troll factories” and “bot farms” pose a great informational danger in the Internet. Their main product is the mass delivering of made-to-order (dis)information. For this, a set of fictitious “creatures” is produced — an “army of informational puppet-soldiers” with certain names and profiles in social networks.

Traditionally, publishing under a pseudonym is an acceptable or even legal way to protect the life and other rights of an author. The situation acquires new dangerous character when human activity moves into cyberspace massively, especially under condition of information warfare. Here, the use of pseudonyms provides not only anonymity, but also mass production of the “information puppet-soldiers” by trolls and bots.

In this research, some elementary ways to identify trolls were found. Together with fact checking, they are useful to protect against malicious informational influences, but are not always sufficient. This is so in the cases where, in particular, a deliverer of disinformation, trying to avoid clear deception, employs different logical tricks. Here one cannot do without of at least the basics knowledge of logic and some skill in critical thinking. This requires strengthening and renovating the mass teaching of these disciplines in schools and universities.

It is emphasized that an effective national system of conducting the ideal component of information warfare should combine groups of special officers of the competent state structures, specialized media workers, as well as relevant public organizations and individual information volunteers. But ideally, everyone should be educated to give himself or herself at least first aid against disinformation.

**Keywords:** information warfare, ideal constituent of information warfare, Internet, troll, troll identification, “information puppet-soldiers”, logic, critical thinking.

*Надійшла до редакції 11 серпня 2022 р.*



---

**Тягло Олександр Володимирович**

Кафедра соціально-гуманітарних дисциплін

Харківський національний університет внутрішніх справ

просп. Льва Ландау, 27

м. Харків

61080

**Tiaglo Oleksandr**

Department of Social and Humanitarian Disciplines

Kharkiv National University of Internal Affairs

Lva Landau ave., 27

Kharkiv

61080



<http://orcid.org/0000-0003-0721-1153>



[olexti@gmail.com](mailto:olexti@gmail.com)



<https://doi.org/10.31812/apm.7628>