УДК 327.8:355.4:37
DOI: https://doi.org/10.17721/1728-2292.2025/2-61/97-101

Аліна ЮРІЙ, асп.
ORCID ID: 0000-0003-2363-2409
e-mail: alinayuriy15@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

РОЛЬ МЕДІАГРАМОТНОСТІ У ФУНКЦІОНУВАННІ ЕСТОНСЬКОЇ СИСТЕМИ ПРОТИДІЇ ЗОВНІШНЬОПОЛІТИЧНІЙ ДЕЗІНФОРМАЦІЇ

Вступ. ***Сучасне інформаційне середовище, змінене під впливом стрімкого розвитку штучного інтелекту та цифрових комунікаційних платформ, зумовило перетворення дезінформації на системну загрозу глобального масштабу, особливо для демократичних держав. У цьому контексті Естонія, з огляду на власний геополітичний досвід, сформувала одну з найпослідовніших та інституціоналізованих моделей протидії зовнішньополітичній дезінформації. Метою статті є розгляд механізмів функціонування естонської системи інформаційної безпеки, з особливою увагою до ролі медіаграмотності як інструменту підвищення суспільної стійкості до інформаційних впливів.***

Методи. ***Методологічну основу дослідження становить поєднання історичного аналізу для реконструкції формування національної політики у сфері інформаційної безпеки, контент-аналізу стратегічних документів, законодавчих актів і публічних комунікацій, а також інституційного аналізу діяльності ключових державних і громадських структур.***

Результати. ***Естонія розробила багаторівневу систему протидії дезінформації, що базується на принципі "цілісного суспільства". Законодавчі інструменти надають повноваження для обмеження діяльності ворожих інформаційних ресурсів. Медіаграмотність системно інтегрована в освітній процес, що сприяє стабільно високим результатам у міжнародних індексах. Активна участь неурядових організацій, особливо у роботі з російськомовними громадами, посилює ефективність системи. Естонія демонструє здатність до оперативного реагування на зовнішньополітичні інформаційні впливи. Міжнародна співпраця, зокрема в межах Центру передового досвіду НАТО з питань спільного кіберзахисту, зміцнює колективну безпеку.***

Висновки. ***Естонський досвід є цінним прикладом для країн, що прагнуть зміцнити національну інформаційну безпеку в умовах гібридних загроз. Медіаграмотність виступає ключовим елементом стійкості, однак подальше вдосконалення системи потребує адаптації до нових технологічних реалій, посилення державно-приватного партнерства та врахування специфіки окремих цільових аудиторій.***

Ключові слова: ***дезінформація, інформаційна безпека, Естонія, медіаграмотність, гібридні загрози, національна безпека, інформаційний вплив.***

Вступ

Упродовж останніх десятиліть світ став свідком безпрецедентної трансформації глобального інформаційного простору. Стрімкий розвиток цифрових технологій, повсюдне поширення соціальних медіа та інтеграція штучного інтелекту значно розширили можливості для поширення інформації, але водночас створили нові загрози для її достовірності та об'єктивності. У цьому новому ландшафті зовнішньополітична дезінформація постала як одна з найбільш значущих гібридних загроз. Вона підриває суспільну згуртованість, еродує довіру до державних інститутів, спотворює демократичні процеси та створює ризики для національної безпеки суверенних держав.

Актуальність дослідження зумовлена тим, що дезінформація більше не є лише інструментом впливу, а перетворилася на системний елемент гібридних воєн, здатний дестабілізувати держави зсередини. Це особливо відчутно для країн, що перебувають на передовій протистояння авторитарним режимам. Естонія, маючи унікальний геополітичний досвід і будучи однією з найбільш цифровізованих держав світу, є яскравим прикладом проактивної адаптації до цих викликів.

Метою дослідження є визначення особливостей функціонування системи протидії зовнішньополітичній дезінформації в Естонії, з урахуванням ролі медіаграмотності як чинника забезпечення інформаційної безпеки держави.

Завданням дослідження є аналіз концептуальних, нормативно-стратегічних та інституційних засад функціонування системи протидії зовнішньополітичній дезінформації в Естонії, а також вивчення ключових механізмів її застосування в контексті забезпечення національної інформаційної безпеки, зокрема через розвиток медіаграмотності населення.

Огляд літератури. Протидія зовнішньополітичній дезінформації привернула значну увагу як українських, так і зарубіжних науковців, що свідчить про її важливість у контексті сучасних гібридних загроз. У наукових працях системно розглядаються різні аспекти інформаційної безпеки, медіаграмотності та ефективні стратегії боротьби з дезінформаційними кампаніями.

Українські дослідники, зокрема О. Андрєєва, О. Запорожець, Н. Карпчук, Є. Макаренко, Н. Піпченко, М. Рижков, А. Шуляк та Б .Юськів, зробили значний внесок у розуміння природи та механізмів дезінформації, інформаційного протиборства та інформаційних війн, зосереджуючись на аналізі впливу міжнародних інформаційних загроз на національну безпеку й вивченні психологічних аспектів інформаційного впливу на суспільну свідомість і поведінку. На міжнародному рівні проблематика дезінформації, кіберзагроз і медіаграмотності досліджується деякими провідними фахівцями: наприклад, П. Померанцев глибоко аналізує тактики інформаційної війни та фабрик тролів, тоді як К. Вонг та К. Зенґер зосереджуються на трансформації загроз у кіберпросторі. Широкий спектр питань, від кібербезпеки до соціокультурного впливу дезінформації, вивчають Е. Белл, К. Вордл, Р ДіРеста, Т. Рід, Ю. Руохонен, Дж. Стенлі, К. Хіт. Вагоме місце у дослідженнях займає питання освіти як інструменту протидії дезінформації, зокрема в працях Т. Макґонґалла.

Незважаючи на значний обсяг наявних досліджень, існує нагальна потреба у всебічному й оновленому аналізі естонської моделі протидії дезінформації, яка б інтегрувала останні стратегічні зміни, законодавчі ініціативи та адаптацію до нових викликів, таких як використання штучного інтелекту в поширенні дезінформації.

© Юрій Аліна, 2025

ISSN 1728-2292 (Print)

Методи

З метою проведення дослідження було використано історичний аналіз для реконструкції еволюції та формування національної політики у сфері інформаційної безпеки Естонії, зокрема з огляду на такі ключові події, як кібератака 2007 р., що стали каталізатором для розвитку сучасної стратегії. Проведено аналіз численних стратегічних документів і відповідних законодавчих актів та публічних комунікацій. Дослідження також включає інституційний аналіз діяльності ключових державних органів і громадських об'єднань, що залучені до процесу протидії дезінформації.

Результати

Інтеграція протидії дезінформації в концепцію "тотальної оборони". Естонія визнає дезінформацію не просто комунікаційним викликом, а прямою загрозою національній безпеці. Така позиція глибоко вкорінена у державній концепції "тотальної оборони", яка є керівним принципом національної безпекової стратегії. Концепція "тотальної оборони" передбачає, що всі основні державні органи, а також приватний сектор і громадянське суспільство, роблять свій внесок у національну оборону, інтегруючи військові сили з невійськовими можливостями (Beitane et al., 2025). Окреслений підхід є результатом глибокого переосмислення національної безпеки після кібератаки 2007 р., яка продемонструвала, що загрози можуть бути гібридними, поєднуючи кібернетичні атаки з інформаційними психологічними операціями. З огляду на це, уряд Естонії розпочав стратегічний перехід від традиційної військово-орієнтованої оборони до цілісної моделі національної стійкості. В естонській моделі інформаційна безпека, включно із заходами протидії дезінформації, розглядається не просто як допоміжна функція, а як основний стовп національного виживання, що вимагає активної участі всіх секторів суспільства. Це означає, що дезінформація розглядається з такою самою серйозністю, як і конвенційні військові загрози, що зумовлює необхідність проактивної та глибоко вбудованої оборони на всіх рівнях суспільства, а не лише у спеціалізованих підрозділах.

Оновлена Концепція національної безпеки Естонії 2023 р., схвалена Рійгікогу, прямо вказує на постійну загрозу, яку становить діяльність російських спецслужб, зокрема їхня розкольницька активність і навмисне поширення дезінформації. У документі підкреслюється, що Російська Федерація систематично здійснює інформаційно-психологічний вплив як на Естонію, так і на інші демократичні держави, використовуючи, зокрема, проросійські групи населення для загострення суспільних суперечностей і підриву конституційного ладу (Government of the Republic of Estonia, 2023).

Інституційно-суспільна модель координації політики протидії дезінформації та розвитку медіаграмотності. Механізм реалізації державної політики Естонії у сфері протидії дезінформації та просування медіаграмотності ґрунтується на міжвідомчій координації та розподілі повноважень між ключовими державними інституціями. Такий підхід забезпечує охоплення різних аспектів інформаційної безпеки та сприяє формуванню цілісної системи суспільної стійкості. Естонія послідовно посідає високі позиції в Індексі медіаграмотності, що є свідченням ефективності її системного підходу. Країна входить до п'ятірки лідерів разом із Фінляндією, Норвегією та Данією. У 2021 р. Естонія посідала 3-тє місце з-поміж 35-ти європейських країн (Open Society Institute Sofia, 2021), а у 2023 р. розділила 4–5 місця зі Швецією (Open Society Institute Sofia, 2023).

Правову основу зазначеної політики було посилено внесенням змін до Закону про медіапослуги (Media Services Act) (Riigikogu, 2022). Закон, адаптований до вимог Європейського цифрового регулювання, уперше закріпив на національному рівні визначення медіаграмотності як поєднання знань, навичок і розуміння, необхідних для безпечного й ефективного використання медіа. Водночас було закріплено, що питання медіаосвіти належать до компетенції Міністерства освіти і науки, яке відповідає за інтеграцію відповідних положень у державну освітню політику.

Координація міжвідомчої діяльності у сфері стратегічних комунікацій покладена на відповідний департамент Канцелярії Уряду Естонії. Його завданням є забезпечення узгодженості державної інформаційної політики, у тому числі в частині психологічної оборони. У межах імплементації широкої безпекової концепції важливою є функція інформування населення щодо актуальних загроз інформаційного середовища. Для цього, зокрема, щорічно публікуються аналітичні звіти Служби внутрішньої безпеки, які містять детальний аналіз дезінформаційної діяльності, ключових акторів, платформ поширення та цілей впливу (Estonian Internal Security Service, 2025). До того ж, принципи підвищення інформаційної стійкості суспільства закріплені в низці національних стратегічних документів. З-поміж них – План розвитку національної оборони до 2031 року (Ministry of Defence of the Republic of Estonia, 2021), Цифровий порядок денний до 2030 року (Ministry of Economic Affairs and Communications of the Republic of Estonia, 2021), План розвитку внутрішньої безпеки до 2030 року (Siseministeerium, 2020) та План розвитку згуртованості Естонії до 2030 року (Kultuuriministeerium, 2021).

Естонія системно інтегрувала цифрову грамотність й обізнаність громадськості у свою освітню систему. Мета полягає в тому, щоб навчити громадян, особливо учнів, критично оцінювати інформацію в інтернеті, що дозволяє їм виявляти й запобігати поширенню дезінформації. Навчання медіаграмотності було включено до естонської шкільної програми ще у 2011–2012 навчальному році, хоча спочатку не як обов'язковий предмет (Propastop, 2025). На сьогодні 35-годинний освітній модуль з медіа та медіаекосистеми є обов'язковою частиною курсу естонської лінгвістики для учнів 11-х класів (Malts, 2025). Це свідчить про глибоке розуміння того, що майбутні покоління мають бути оснащені інструментами для навігації у цифровому світі. Крім того, програма AI Leap, запланована до запуску у вересні 2025 р., має на меті інтегрувати інструменти та навички штучного інтелекту в освіту (e-Estonia, 2025). Ініціатива, що ґрунтується на досвіді програми Tiger Leap 30-річної давності, яка запровадила комп'ютери та інтернет у всі естонські школи, покликана підготувати учнів і вчителів до ефективного використання штучного інтелекту в навчанні. Подібні інноваційні проєкти можуть значно посилити критичне мислення в цифрову еру, коли штучний інтелект сприяє активному поширенню дезінформації.

Громадянське суспільство Естонії відіграє ключову роль у боротьбі з інформаційними загрозами, демонструючи ефективну міжсекторальну взаємодію медіа, академічних кіл, технологічних розробників і волонтерських ініціатив, що може бути прикладом для інших демократичних суспільств. Одним із провідних суб'єктів є новинний портал Delfi (Delfi Meedia, 2025). Він поєднує журналістські розслідування із системною перевіркою фактів, що дозволяє не лише спростовувати окремі фейки, а й виявляти джерела, мотиви та інфраструктуру

дезінформаційних кампаній. Delfi також є ключовим учасником проєкту Балтійського центру взаємодії у сфері протидії інформаційним розладам, який функціонує як транснаціональна мережа фахівців із медіаграмотності, фактчекінгу та комунікацій, координована Тартуським університетом Естонії (Baltic Engagement Centre for…, 2025).

Окремий сегмент громадянського суспільства представляє волонтерський блог Propastop (Propastop, 2025). Його діяльність фокусується на виявленні та розвінчанні російських інформаційних операцій. Аналітичні матеріали блогу демонструють еволюцію пропагандистських наративів, виявляють цільові аудиторії та пояснюють механізми впливу. Особлива увага приділяється зміщенню кремлівських зусиль до використання естонської та англійської мов, що є спробою здобути довіру локальних спільнот. Залучення широкої аудиторії до аналізу фейків через інтерактивні формати (ігри, візуалізації) перетворює Propastop на важливий інструмент підвищення інформаційної грамотності та пильності громадян Естонії.

Міжнародна співпраця та кібердипломатія. Естонія визнає, що загрози інформаційній безпеці є транснаціональними, тому активно співпрацює з міжнародними партнерами для посилення колективної стійкості та формування глобальних норм. Естонія тісно співпрацює з НАТО та ЄС, обмінюючись розвідувальними даними й передовим досвідом у протидії дезінформації та кіберзагрозам (Baltic Centre for Media Excellence, 2025). Така проактивна взаємодія посилює національні оборонні можливості Естонії, сприяючи колективній стійкості та встановленню спільних стандартів з-поміж союзників. Це не просто пасивна участь, а активне лідерство, що вказує на стратегічне розуміння того, що національна інформаційна безпека не може бути досягнута ізольовано, і що створення міжнародних рамок і спільних оборонних можливостей є мультиплікатором сили проти спонсорованих державами дезінформаційних кампаній, які виходять за межі кордонів.

Важливою складовою міжнародної політики Естонії у сфері інформаційної та кібербезпеки є її активна участь у діяльності Центру передового досвіду НАТО з питань спільного кіберзахисту (CCDCOE), розташованого в Таллінні (NATO Cooperative Cyber Defence…, 2025). Центр виступає ключовим елементом архітектури євроатлантичної безпеки у цифровому вимірі, акумулюючи досвід, аналітичний потенціал і координаційні механізми з метою зміцнення спроможності союзників НАТО та партнерських країн до ефективного реагування на загрози у кіберпросторі, включно з такими гібридними викликами, як дезінформація.

Ще одним прикладом проактивного підходу Естонії є створення та участь в ініціативі "Франція та Естонія – разом проти дезінформації" (FREETAD), започаткованій у 2024 р. за фінансової підтримки Відділу публічної дипломатії НАТО (Braghiroli, 2024). Обидві держави зазнають системного впливу з боку російських дезінформаційних кампаній, що становлять складову гібридної агресії. Естонія як держава, що безпосередньо межує з Росією, має тривалий і практично орієнтований досвід протидії інформаційним і кіберзагрозам. Франція, зі свого боку, також активно реагує на виклики в інформаційному просторі, особливо після викриття у 2024 р. масштабної російської кампанії Portal Kombat, яка використовувала мережу фейкових новинних сайтів для маніпуляції європейською аудиторією (VIGINUM, Secrétariat général…, 2024). Метою FREETAD є не лише підвищення обізнаності громадськості, але й налагодження міцної транскордонної взаємодії, що є критично важливим для формування єдиного фронту проти деструктивних інформаційних впливів. У межах FREETAD було реалізовано кілька ключових напрямів діяльності. Зокрема, естонські та французькі університетські студенти пройшли інтенсивні курси навчання з ідентифікації та аналізу дезінформації, що сприяло розвитку їхніх навичок критичного мислення та медіаграмотності. Навчання базувалося на принципі формування практичних навичок, необхідних для навігації у складному інформаційному середовищі.

Такі проєкти, як FREETAD, демонструють проактивний, а не лише реактивний підхід до розбудови інформаційної стійкості. Оскільки сучасні дезінформаційні кампанії часто мають складну архітектуру та націлені на підрив суспільної довіри у кількох країнах одночасно, тому двостороння співпраця, особливо у сферах освіти та обміну експертами, свідчить про стратегічні інвестиції у спільну демократичну стійкість. Це відповідає засадам теорії інформаційної безпеки, яка підкреслює, що ефективний захист вразливостей вимагає інтегрованих зусиль на всіх рівнях – від індивідуальної медіаграмотності до міждержавних альянсів. Залучення студентів та експертів до таких ініціатив відображає довгострокові інвестиції в людський капітал і розвиток міжкультурного розуміння динаміки дезінформації, що є критично важливим для ефективної протидії наративам, які часто експлуатують суспільні розбіжності й культурні особливості для досягнення своїх деструктивних цілей.

Виклики та перспективи розвитку системи протидії дезінформації. Незважаючи на значні досягнення, Естонія стикається з низкою викликів у подальшому розвитку своєї системи протидії дезінформації, що вимагає постійної адаптації та інновацій. Попри те, що Естонія вважається доволі просуненою в медіаграмотності та має обов'язкову дисципліну з вивчення медіа та інформаційної грамотності у національному навчальному плані, країна все ще бореться з перетворенням теоретичних знань на повсякденну практику. Розрив є суттєвим для підвищення стійкості країни до дезінформації. Існує помітна різниця в медіаграмотності між поколіннями учнів і вчителів. Учителі потребують постійного оновлення своїх знань у сферах медіаграмотності та інформаційної безпеки, особливо з огляду на швидкий розвиток інформаційних технологій та штучного інтелекту. Таким чином, навіть у Естонії – країні з високим рівнем медіаграмотності, необхідно постійно інвестувати в освіту дорослих і професійний розвиток, щоб забезпечити ефективне застосування знань у реальних умовах.

Зауважимо, що російськомовне населення Естонії становить особливий виклик для інформаційної безпеки. Значна частина цієї демографічної групи має суттєві розбіжності у поглядах на зовнішню політику порівняно з естонськомовним населенням і залишається вразливою до проросійських наративів, часто перебуваючи у "російській інформаційній бульбашці" (Lagashina, 2025). Незважаючи на такі зусилля, як створення державного телеканалу ETV+ у 2014 р., який мав на меті надати російськомовним громадянам доступ до надійної інформації та сприяти соціальній згуртованості (Beitane et al., 2025), вплив російської пропаганди залишається значним. Отже, інформаційний вакуум і схильність до проросійських наративів з-поміж російськомовного населення є критичною враз-

ливістю внутрішньої безпеки. Суто інформаційний підхід (надання альтернативних медіа) виявляється недостатнім; для справжньої інформаційної стійкості у різноманітних суспільствах необхідна глибша соціокультурна інтеграція та робота з основними "культурними кодами". Такі ініціативи з медіаграмотності, що проводяться Естонською асоціацією Північноатлантичного договору (EATA) та громадською організацією Future Media, спеціально націлені на російськомовні громади, щоб подолати подібні критичні прогалини (Baltic Centre for Media Excellence, 2025).

Отже, стрімкий розвиток штучного інтелекту та зростаюча фрагментація інформаційного простору, зумовлена впливом соціальних медіа, не змінюють суті дезінформаційних кампаній, проте суттєво підсилюють їхню масштабність і впливовість. Поява нових форматів комунікації, алгоритмічні зміни на платформах і використання локальних мов для поширення пропагандистського контенту ускладнюють виявлення маніпуляцій. Значний виклик становить необхідність моніторингу великої кількості цифрових джерел та акторів впливу. В умовах постійної трансформації цифрового середовища Естонія стикається з потребою оперативно адаптувати національну систему протидії дезінформації. Хоча ініціатива AI Leap демонструє кроки до інтеграції штучного інтелекту в освітній та аналітичний процес, використання тих самих технологій з боку ворожих акторів фактично формує "цифрову гонку озброєнь". Це не лише актуалізує потребу в інноваційних інструментах для виявлення загроз, а й висвітлює обмеженість традиційних, зокрема людських, методів фактчекінгу. Навіть за умов високого рівня проактивності, Естонія має постійно оновлювати як технологічні, так і кадрові спроможності для прогнозування й нейтралізації еволюціонуючих, зокрема згенерованих штучним інтелектом, дезінформаційних кампаній.

Дискусія і висновки

Система протидії зовнішньополітичній дезінформації в Естонії є яскравим прикладом комплексного та проактивного підходу до забезпечення національної інформаційної безпеки. Її еволюція, значною мірою сформована досвідом російської кібератаки 2007 р., призвела до впровадження концепції "тотальної оборони", де протидія дезінформації визнається життєво важливим компонентом загальної безпекової стратегії. Це передбачає інтеграцію військових і невійськових можливостей, а також активну участь усіх секторів суспільства – від уряду та приватного сектору до медіа та громадянського суспільства.

Ключовим досягненням Естонії є системна інтеграція медіаграмотності в освітню систему, починаючи з раннього віку та продовжуючи через обов'язкові шкільні курси, що сприяло високим позиціям Естонії в Індексі медіаграмотності та є свідченням її здатності виховувати критично мислячих громадян. Важливу роль у цьому відіграють такі неурядові організації, як Propastop, що доповнюють державні зусилля, надаючи спеціалізовану перевірку фактів, розвиваючи цільові освітні програми та сприяючи формуванню критичного мислення на низовому рівні. Швидка та прозора комунікація уряду, у поєднанні з ефективним фактчекінгом, є центральними інструментами для підтримки суспільної довіри та запобігання поширенню неправдивих наративів.

На міжнародній арені Естонія активно співпрацює з НАТО та ЄС, обмінюючись розвідувальними даними й передовим досвідом, а також виступаючи за глобальні норми відповідальної поведінки в кіберпросторі. Роль Центру передового досвіду НАТО з питань спільного кіберзахисту (CCDCOE) у Таллінні та участь у двосторонніх проєктах, таких як FREETAD, підкреслюють стратегічне розуміння Естонією того, що інформаційна безпека є колективним викликом, який вимагає спільних зусиль.

Проте перед Естонією стоять суттєві виклики, які ускладнюють реалізацію національної стратегії протидії дезінформації. З-поміж них – потреба трансформувати теоретичні знання медіаграмотності у повсякденну практику, подолати міжпоколіннєвий розрив у рівні цифрової компетентності й налагодити ефективну комунікацію з російськомовним населенням, яке залишається вразливим до зовнішньої пропаганди. Додатковий тиск чинить стрімкий розвиток штучного інтелекту та постійна еволюція дезінформаційних технологій, що вимагають гнучкої, технологічно підготовленої та інституційно стійкої відповіді. У цьому контексті визначальним є комплексний і цілісний підхід Естонії, який передбачає мобілізацію державного, приватного та громадянського секторів для створення багаторівневого захисту інформаційного простору. Медіаграмотність у такій системі відіграє роль ключового елемента інформаційної стійкості, забезпечуючи громадян необхідними інструментами для самостійного критичного оцінювання інформації.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

Baltic Centre for Media Excellence. (2025, April 27). *Empowering Estonians Against Disinformation*. https://bcme.eu/en/articles/empowering-estonians-against-disinformation/

Baltic Centre for Media Excellence. (2025, May 27). *Inside Estonia's Strategy Against Disinformation and Cyber Threats*. https://bcme.eu/en/articles/inside-estonias-strategy-against-disinformation-and-cyber-threats/

Baltic Engagement Centre for Combating Information Disorders (BECID). (2025). https://becid.eu/fact-checking/

Beitane, A., Braghiroli, S., Dolbeau-Bandin, C., & Dufy, C. (2025, February 28). *All for one and one for all against disinformation to protect democracy.* New Eastern Europe. https://neweasterneurope.eu/2025/02/28/all-for-one-and-one-for-all-against-disinformation-to-protect-democracy/

Braghiroli, S. (2024, March 28). *New Estonian-French project on disinformation supported by NATO.* Centre for Sustainable Development. University of Tartu. https://kestlikuarengukeskus.ut.ee/en/content/new-estonian-french-project-disinformation-supported-nato

Delfi Meedia. (2025). Fact-checks in English. https://epl.delfi.ee/kategooria/120000471/fact-checks-in-english

e-Estonia. (2025, February 26). *Estonia's groundbreaking national initiative: AI Leap programme to bring AI tools to all schools*. https://e-estonia.com/estonia-announces-a-groundbreaking-national-initiative-ai-leap-programme-to-bring-ai-tools-to-all-schools/

Estonian Internal Security Service. (2025). *Annual review 2024–2025.* https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf

Government of the Republic of Estonia. (2023). *National security concept of Estonia*. https://www.kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_eng_22.02.2023.pdf

Kultuuriministeerium. (2021). *Kultuuri arengukava 2021–2030.* https://www.kul.ee/siduseesti2030

Lagashina, O. (2025, June 25). *The Russian-speaking population of Estonia does not support its foreign policy*. https://www.veridica.ro/en/opinions/the-russian-speaking-population-of-estonia-does-not-support-its-foreign-policy

Malts, K. (2025, January 10). *Disinformation landscape in Estonia.* EU DisinfoLab. https://www.disinfo.eu/wp-content/uploads/2025/03/20250110_Disinfo-landscape-in-Estonia-2.pdf

Ministry of Defence of the Republic of Estonia. (2021). *National Defence Development Plan 2031.* https://kaitseministeerium.ee/en/national-defence-development-plan-2031

Ministry of Economic Affairs and Communications of the Republic of Estonia. (2021). *Estonia's Digital Agenda 2030.* https://www.mkm.ee/sites/default/files/documents/2022-04/Digi%C3%BChiskonna%20arengukava_ENG.pdf

NATO Cooperative Cyber Defence Centre of Excellence. (2025). *The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub.* https://www.ccdcoe.org/

Open Society Institute Sofia. (2021, March). *Media Literacy Index 2021*. https://osis.bg/wp-content/uploads/2021/03/MediaLiteracyIndex2021_ENG.pdf

Open Society Institute Sofia. (2023, June). *Media Literacy Index 2023*. https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf

Propastop. (2025). Propaganda's First Rule: Don't Be a Useful Idiot. 3 Steps for a Quick Info Check. https://www.propastop.org/en/

Propastop. (2025, February 15). *There is a generational difference in the media literacy of students and teachers.* https://www.propastop.org/en/2025/02/15/julia-rodina-there-is-a-generational-difference-in-the-media-literacy-of-students-and-teachers/

Riigikogu. (2022). *Media Services Act* (Chapter 7). Riigi Teataja. https://www.riigiteataja.ee/en/eli/514062022001/consolide

Siseministeerium. (2020). *Siseturvalisuse arengukava 2020–2030*. https://www.siseministeerium.ee/stak2030

VIGINUM, Secrétariat général de la défense et de la sécurité nationale. (2024, February). *Portal Kombat: A structured and coordinated pro-Russian propaganda network* [Technical report]. https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

References

Baltic Centre for Media Excellence. (2025, April 27). *Empowering Estonians Against Disinformation*. https://bcme.eu/en/articles/empowering-estonians-against-disinformation/

Baltic Centre for Media Excellence. (2025, May 27). *Inside Estonia's Strategy Against Disinformation and Cyber Threats*. https://bcme.eu/en/articles/inside-estonias-strategy-against-disinformation-and-cyber-threats/

Baltic Engagement Centre for Combating Information Disorders (BECID). (2025). https://becid.eu/fact-checking/

Beitane, A., Braghiroli, S., Dolbeau-Bandin, C., & Dufy, C. (2025, February 28). *All for one and one for all against disinformation to protect democracy.* New Eastern Europe. https://neweasterneurope.eu/2025/02/28/all-for-one-and-one-for-all-against-disinformation-to-protect-democracy/

Braghiroli, S. (2024, March 28). *New Estonian-French project on disinformation supported by NATO.* Centre for Sustainable Development, University of Tartu. https://kestlikuarengukeskus.ut.ee/en/content/new-estonian-french-project-disinformation-supported-nato

Delfi Meedia. (2025). Fact-checks in English. https://epl.delfi.ee/kategooria/120000471/fact-checks-in-english

e-Estonia. (2025, February 26). *Estonia's groundbreaking national initiative: AI Leap programme to bring AI tools to all schools*. https://e-estonia.com/estonia-announces-a-groundbreaking-national-initiative-ai-leap-programme-to-bring-ai-tools-to-all-schools/

Estonian Internal Security Service. (2025). *Annual review 2024–2025.* https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf

Government of the Republic of Estonia. (2023). *National security concept of Estonia*. https://www.kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_eng_22.02.2023.pdf

Lagashina, O. (2025, June 25). *The Russian-speaking population of Estonia does not support its foreign policy*. https://www.veridica.ro/en/opinions/the-russian-speaking-population-of-estonia-does-not-support-its-foreign-policy

Malts, K. (2025, January 10). *Disinformation landscape in Estonia.* EU DisinfoLab. https://www.disinfo.eu/wp-content/uploads/2025/03/ 20250110_Disinfo-landscape-in-Estonia-2.pdf

Ministry of Culture. (2021). *Culture Development Plan 2021–2030* [in Estonian]. https://www.kul.ee/siduseesti2030

Ministry of Defence of the Republic of Estonia. (2021). *National Defence Development Plan 2031.* https://kaitseministeerium.ee/en/national-defence-development-plan-2031

Ministry of Economic Affairs and Communications of the Republic of Estonia. (2021). *Estonia's Digital Agenda 2030.* https://www.mkm.ee/sites/default/files/documents/2022-04/Digi%C3%BChiskonna%20arengukava_ENG.pdf

Ministry of the Interior. (2020). *Internal Security Development Plan 2020–2030* [in Estonian]. https://www.siseministeerium.ee/stak2030

NATO Cooperative Cyber Defence Centre of Excellence. (2025). *The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub*. https://www.ccdcoe.org/

Open Society Institute Sofia. (2021, March). *Media Literacy Index 2021*. https://osis.bg/wp-content/uploads/2021/03/MediaLiteracyIndex2021_ENG.pdf

Open Society Institute Sofia. (2023, June). *Media Literacy Index 2023*. https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf

Propastop. (2025). Propaganda's First Rule: Don't Be a Useful Idiot. 3 Steps for a Quick Info Check. https://www.propastop.org/en/

Propastop. (2025, February 15). *There is a generational difference in the media literacy of students and teachers.* https://www.propastop.org/en/2025/02/15/julia-rodina-there-is-a-generational-difference-in-the-media-literacy-of-students-and-teachers/

Riigikogu. (2022). *Media Services Act* (Chapter 7). Riigi Teataja. https://www.riigiteataja.ee/en/eli/514062022001/consolide

VIGINUM, Secrétariat général de la défense et de la sécurité nationale. (2024, February). *Portal Kombat: A structured and coordinated pro-Russian propaganda network* [Technical report]. https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

Отримано редакцією журналу / Received: 21.07.25
Прорецензовано / Revised: 30.07.25
Схвалено до друку / Accepted: 23.12.25

Alina YURII, PhD Student
ORCID ID: 0000-0003-2363-2409
e-mail: alinayuriy15@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

THE ROLE OF MEDIA LITERACY IN THE FUNCTIONING OF ESTONIA'S SYSTEM FOR COUNTERING FOREIGN POLICY DISINFORMATION

Background. ***The contemporary information environment, shaped by the rapid advancement of artificial intelligence and digital communication platforms, has transformed disinformation into a systemic threat of global scale, particularly for democratic states. In this context, Estonia – drawing upon its own geopolitical experience – has developed one of the most consistent and institutionalized models for countering foreign policy disinformation. This article aims to examine the operational mechanisms of Estonia's information security system, with particular emphasis on the role of media literacy as a tool for enhancing societal resilience to information influence.***

Methods. ***The methodological framework of this study combines historical analysis to reconstruct the development of national information security policy, content analysis of strategic documents, legislative acts, and public communications, as well as institutional analysis of the activities of key governmental and civil society institutions.***

Results. ***Estonia has developed a multi-level system for countering disinformation, based on the "whole-of-society" approach. Legislative instruments provide authorities with the power to restrict the activities of hostile information resources. Media literacy is systematically integrated into the educational process, contributing to consistently high rankings in international indices. The active involvement of non-governmental organizations, particularly in outreach to Russian-speaking communities, enhances the system's effectiveness. Estonia demonstrates the capacity for rapid response to foreign information threats. International cooperation, especially within the framework of the NATO Cooperative Cyber Defence Centre of Excellence, further strengthens collective security.***

Conclusions. ***The Estonian experience serves as a valuable example for countries seeking to strengthen national information security in the context of hybrid threats. Media literacy functions as a key element of societal resilience; however, further development of the system requires adaptation to emerging technological realities, strengthening of public-private partnerships, and greater consideration of the specific characteristics of target audiences.***

Keywords: ***disinformation, information security, Estonia, media literacy, hybrid threats, national security, information influence.***

Автор заявляє про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The author declares no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.