ПРАКТИКИ ТА ІНСТРУМЕНТИ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ: ДОСВІД ЗАРУБІЖНИХ КРАЇН

PRACTICES AND TOOLS TO COUNTERACT INFORMATION WARFARE: EXPERIENCE OF FOREIGN COUNTRIES

УДК 351:355:008
DOI https://doi.org/10.32782/pma2663-5240-2024.39.2

Грицай Р.О.
аспірант кафедри державного управління
Київський національний університет імені Тараса Шевченка

Загроза російської дезінформації для європейських країн є все більш очевидною та актуальною. Зважаючи, що початок інформаційної війни росії проти України розпочався в 2014 році, то в той же час кремлівська влада почала активніше впроваджувати операції впливу проти західноєвропейських демократій. У статті проаналізовано досвід органів публічної влади зарубіжних країни в протидії кіберінформаційним атакам та інформаційній війні у виробленні практик та інструментів боротьби проти їхніх проявів.

Встановлено, що і країни ЄС, і США свою інформаційну політику в сфері безпеки вибудовують в тандемі із захистом прав людини. Виявлено, що на сьогоднішній день європейський підхід щодо інформаційної безпеки є більш функціональний, оскільки в його основі лежить співвідношення транспарентності інформаційної політики і забезпечення інформаційної безпеки. США декларує високі стандарти прав і свобод людини в інформаційній сфері.

Зарубіжний досвід показує, що підвищення ефективності політики інформаційної безпеки, використання інструментів перешкоджання маніпулятивним технологіям та дезінформації, запровадження активної діяльності спеціальних викривачів деструктивного контенту (фактчекерів) дозволяє нам говорити про мобілізацію приватного сектору у боротьбі з інформаційними загрозами та двосторонню координацію держави та приватних компаній у протидії інформаційній війні.

Зроблено висновки, що з урахуванням функціонуючої моделі прав людини у Європейському Союзі сформовано низку дієвих інструментів, які спрямовані на організацію протидії інформаційній війні, а саме Закон про цифрові послуги, Посилений кодекс практики щодо дезінформації. Сполучені Штати Америки характеризуються політикою оцінювання, нагляду та координації влади і громадянського суспільства щодо регулювання інформаційного простору.

Ключові слова: *дезінформація, інформаційна війна, інформаційна загроза, інформаційна безпека.*

The threat of Russian disinformation to European countries is becoming more and more obvious and urgent. Given that Russia's information war against Ukraine began in 2014, at the same time the Kremlin began to actively implement influence operations against Western European democracies. The article analyzes the experience of public authorities of foreign countries in countering cyber information attacks and information warfare in developing practices and tools to combat their manifestations.

It is established that both the EU and the USA build their information security policy in tandem with the protection of human rights. It is found that today the European approach to information security is more functional, since it is based on the ratio of transparency of information policy and information security.

The foreign experience shows that increasing the effectiveness of information security policy, using tools to prevent manipulative technologies and disinformation, and introducing active work of special whistleblowers of destructive content (fact-checkers) allows us to talk about mobilizing the private sector in the fight against information threats and bilateral coordination of the State and private companies in countering information warfare.

It is concluded that, taking into account the functioning model of human rights, the European Union has formed a number of effective instruments aimed at organising counteraction to information warfare, namely the Digital Services Act and the Enhanced Code of Practice on Disinformation. The United States of America is characterised by a policy of assessment, oversight and coordination between the government and civil society in regulating the information space.

Key words: *disinformation, information warfare, information threat, information security.*

Постановка проблеми. На Всесвітньому економічному форумі (WEF), що проходив 15–19 січня 2024 року в Давосі Президентка Європейської Комісії Урсула фон дер Ляєн у своїй промові наголосила, що «головними ризиками наступних двох років є не конфлікт чи клімат. Це дезінформація та неправдива інформація, за якою слідує поляризація суспільств. Ці ризики є серйозними, оскільки вони обмежують здатність долати великі глобальні виклики, з якими ми стикаємося, а саме: зміни природнього клімату, геополітичні, технологічні зміни» [1]. Вона неодноразово поверталася до цього питання, згадуючи нашу країну, що ніде не було більше поширення дезінформації, ніж у питанні України. Називаючи дезінформацію «проблемою №1 серед глобальних ризиків», У. фон дер Ляєн з надією запевнила: «Цінності, які ми цінуємо офлайн, повинні також бути захищені онлайн» [1]. Підґрунтям таких висновків Президентки є Звіт про глобальні ризики 2024. Однією з головних тез Звіту є акцент, що 2024–2025 рр. ознаменується участю майже 4 мільярдів людей у національних та муніципальних виборах, включаючи США, Мексику, Індію, Пакистан, Індонезію. Наявність дезінформації у виборчих процесах може призвести до дестабілізації легітимності

новообраних урядів, а маніпулятивні кампанії можуть підірвати демократичні процеси в цілому. Така майбутня перспектива може призвести до того, що «поляризовані суспільства можуть стати поляризованими не лише за своїми політичними пристрастями, але й за сприйняттям реальності. Фальсифікована інформація також може розпалити ворожість до певних груп, від упередженості та дискримінації на робочому місці до насильства та злочинів на ґрунті ненависті» [2].

Зважаючи на роль та місце Європейського Союзу та США як стратегічних партнерів України, актуальним є ознайомлення з процесами вдосконалення їхньою владою системи державного управління у протидії сучасним зовнішнім інформаційним загрозам.

Аналіз останніх досліджень і публікацій. Серед вітчизняних дослідників, які вивчали зарубіжний досвід в протидії інформаційним загрозам є Бондар В. (інформаційна політика Євросоюзу та США), Золотар О. (правове регулювання відносин у сфері інформаційної безпеки), Солових В. (інституційні основи міжнародної інформаційної безпеки), Сунгурова С. (міжнародний досвід протистояння політичному насиллю в інформаційному просторі) та інші. Проте ці науковці не розглядали останні розробки та здобутки досвіду країн ЄС та США у сфері протидії інформаційній війні, що й зумовлює актуальність цієї публікації.

Метою статті є аналіз досвіду органів публічної влади Європейського Союзу та США в протидії кіберінформаційним атакам та інформаційній війні.

Виклад основного матеріалу. На сьогодні російська пропаганда та дезінформація залишаються важливою складовою агресивної політики рф у війні проти України. Ставлячи за мету знизити рівень політичної підтримки, обсяги допомоги західних партнерів, рф намагається за допомогою дезінформації виправдовувати російську військову агресію та підірвати консенсус щодо підтримки України з боку Європейського Союзу. Проте російські зусилля у сфері інформаційної війни спрямовані не лише на Україну. Під загрозою може опинитися і Європа, і США, і будь-який регіон світу, оскільки російська інформаційна війна базується на глобальній стратегії дискредитації демократичних інституцій, симпатизації антидемократичним лідерам, дестабілізації демократії.

У Європейському Союзі сформована низка дієвих інструментів, які спрямовані на протидію інформаційним загрозам, включаючи дезінформацію. Основні засади політики Євросоюзу щодо інформаційної війни були вперше прийняті як реакція на російську анексію Криму в 2014 році. Щоб протистояти загрозі російської інформаційної війни у 2015 році Європейською комісією була створена і розпочала роботу оперативна робоча група зі стратегічних комунікацій Європейського Союзу East Stratcom Task Force (ESTF). Діяльність групи, в першу чергу, спрямована на підвищення обізнаності щодо прокремлівської дезінформації, інформаційних маніпуляцій. У тісній співпраці з Європейською комісією та представництвами ЄС ESTF працює над забезпеченням узгодженості комунікацій та стійкості до дезінформації. ESTF також приділяє підвищену увагу на зміцнення загального медіа-середовища у Східному сусідстві та сприяє наданню підтримки незалежних ЗМІ. З 2015 р. ESTF проводить кампанію EUvsDisinfo по моніторингу, аналізу та реагуванню на дезінформацію та маніпулювання інформацією [3]. EUvsDisinfo випускає щотижневий огляд дезінформації на сайті https://euvsdisinfo.eu.

Загалом можна виокремити такі кампанії з дезінформації:

– створення проблемних контентів з метою розпалювання ворожнечі в суспільстві, міжрасової та міжетнічної нетерпимості;

– вплив на політичні дебати через соціальні мережі та ЗМІ;

– втручання у демократичні процеси;

– кібератаки на об'єкти критичної інфраструктури та злам мереж.

16 червня 2022 року Європейська комісія підписала та опублікувала «Посилений кодекс практики щодо дезінформації». Він містить 44 зобов'язання та 128 конкретних кроків, які спрямовані на забезпечення прозорості і підзвітності онлайн-платформ та соціальних мереж щодо дезінформації в Інтернеті [5]. Він є основою для компаній, які можуть періодично та систематично звітувати про свої втручання з протидії дезінформації. Звернемо увагу на деякі з них. В межах 15-го Зобов'язання підписанти встановлюють свою політику щодо протидії забороненим маніпулятивним практикам для систем штучного інтелекту, які генерують або маніпулюють контентом, наприклад, шляхом попередження користувачів та проактивного виявлення такого контенту.

Так, наприклад, Зобов'язання 18 закликає підписантів «зобов'язатися мінімізувати ризик вірусного розповсюдження дезінформації шляхом впровадження безпечних практик проектування під час розробки своїх систем, політик і функцій» [5]. Виходячи за рамки якісного звітування, оцінка впливу змін алгоритму може включати перевірку того, чи люди частіше залучаються до високоякісного кон-

тенту та рідше до шкідливого. Зобов'язання 29 передбачає, що підписанти зобов'язуються проводити дослідження на основі прозорої методології та етичних стандартів, а також обмінюватися наборами даних і результатами досліджень з відповідною аудиторією.

Серед 34 підписантів, окрім онлайн-платформ і представників рекламної індустрії, є спеціалісти з перевірки фактів, представники громадянського суспільства, дослідницькі організації та компанії, які пропонують послуги з виявлення дезінформації. Компаніями-підписантами є Adobe, Google, Microsoft, Meta, TikTok, Twitch тощо. Наразі компанії подали два комплекти звітів, опублікованих у лютому 2023 року та вересні 2023 року. Підписанти зобов'язалися вживати заходів у таких сферах як:

– демонетизація поширення дезінформації (скорочення фінансових стимулів для розповсюджувачів дезінформації);

– забезпечення прозорості політичної реклами (за рахунок більш ефективного маркування, зобо'язання розкривати спонсора, витрати на рекламу та період показу);

– посилення співпраці з фактчекерами (онлайн-платформи будуть послідовно використовувати роботу фактчекерів, щоб забезпечити покриття в усіх країнах ЄС та мовами, якими вони розмовляють. Фактчекери мають важливе значення і отримають за свою роботу справедливу фінансову винагороду);

– розширення прав та можливостей користувачів завдяки вдосконаленим інструментам розпізнавання дезінформації;

– надання дослідникам кращого доступу до даних.

Постійна робоча група переглядатиме та адаптуватиме зобов'язання з огляду на технологічні, соціальні суспільних, ринкові та законодавчі зміни. У складі робочої групи візьмуть участь представники підписантів, регуляторних органів, Європейської обсерваторії цифрових медіа та Європейської служби зовнішніх справ.

Кодекс практики щодо дезінформації працює над досягненням важливої мети – узгодженої оперативної звітності в різних країнах. Це важливий крок у правильному напрямку для демократій та онлайн-платформ у вирішенні безлічі проблем в Інтернеті. «У поєднанні з розширеним доступом дослідників до даних для довготривалих досліджень, що забезпечується статтею 40 Закону про цифрові послуги (DSA), яка зобов'язує дуже великі онлайн-платформи обмінюватися даними з перевіреними дослідниками, є надія, що дослідники, політики та платформи можуть спільними зусиллями зрозуміти наслідки онлайн-діяльності в реальному житті» [4].

Узагальнюючи наведене, можна зробити висновок, що для Європейського Союзу пріоритетним є системний підхід у боротьбі із поширенням дезінформації, який повинен сприяти виявленню неправдивих відомостей та способів їх поширення, з однієї сторони, та не допустити обмеження прав громадян на доступ до інформації – з іншої.

Зупинимося на Законі про цифрові послуги (Digital Services Act, DSA). Цей закон є одним з найважливіших документів у сфері захисту цифрового простору від поширення незаконного контенту та захисту основних прав користувачів. Після схвалення Радою, оскільки він також був схвалений Європейським парламентом, Закон про цифрові послуги було прийнято 19 жовтня 2022 р. Цей закон має регулювати соціальні мережі, онлайн-ринки, онлайн-платформи та онлайн-пошукові системи завдяки заходам протидії незаконному контенту в Інтернеті та зобов'язання платформ швидко реагувати, дотримуючись основних прав [6]. Також цей закон встановлює спеціальні зобов'язання для онлайн-ринків з метою боротьби з онлайн-продажем незаконних продуктів і послуг та забороняє оманливі інтерфейси, відомі як «темні шаблони», спрямовані на введення в оману.

В квітні 2023 р. Європейська комісія визначила 19 дуже великих онлайн-платформ, серед яких Twitter, YouTube, Instagram, Amazon, Alibaba AliExpress, Wikipedia дві найбільші онлайн-пошукові системи (Google, Bing). Представники ЄС наголошують, що онлайн-платформи, які не відповідають вимогам DSA, можуть бути піддані значним штрафам або навіть забороонам. За порушення Закону про цифрові послуги на онлайн-платформи очікують санкції, що передбачать до 6% світового річного обороту [6].

Однією з особливостей Digital Services Act є те, що він застосовується до постачальників посередницьких послуг, які надаються в ЄС незалежно від того, де розташовані ці компанії, тобто він має екстериторіальну дію.

У грудні 2022 року Європейська комісія, Європейський парламент і Рада Європейського Союзу спільно підписали Європейську декларацію про цифрові права та принципи, документ, який закріплює зобов'язання щодо безпечного та сталого цифрового майбутнього в Європі. Декларація містить шість розділів, що окреслюють права та принципи, які європейські громадяни можуть мати в Інтернеті, зокрема сприяння участі у цифровому публічному просторі та підвищення без-

пеки, захисту та розширення можливостей у цифровому середовищі [7].

Підґрунтям у прийнятті цих важливих актів є низка супутніх програмних документів, що передували їм.

У квітні 2018 року було представлено Європейською комісією програмний документ «Боротьба з дезінформацією в Інтернеті: європейський досвід». Визнаючи загрозу онлайн-дезінформації, зокрема щодо розробки політики та виборчих процесів, а також транскордонний вимір онлайн-дезінформації, цей документ викладає основні принципи та цілі, які мають на меті керувати діями з підвищення обізнаності громадськості щодо дезінформації та ефективного управління нею, разом із конкретними заходами, які Комісія має намір вжити для боротьби з дезінформацією в Інтернеті [8]. Згідно з документом, пропонується кілька заходів, які має вжити Комісія. До них належать сприяння освіті та медіаграмотності; започаткування постійного діалогу для підтримки держав-членів у забезпеченні стійкості виборів проти дедалі складніших кіберзагроз, включаючи онлайн-дезінформацію та кібератаки; підтримка якісної журналістики як важливого елемента демократичного суспільства; протидія внутрішнім і зовнішнім загрозам дезінформації за допомогою стратегічної комунікації.

У грудні 2018 року в ЄС прийнято План дій проти дезінформації, метою якого є захист демократичних систем Європейського Союзу та боротьба з дезінформацією [9]. Згідно з цим документом, дезінформація здійснювана з боку російської федерації представляє найбільшу загрозу для Європейського Союзу. Серед нагальних кроків в даному напрямку планується створення і запуск спеціальної системи швидкого сповіщення (Rapid Alert System, RAS).

У грудні 2020 року Європейська комісія представила План дій щодо європейської демократії, який мав на меті визначити подальші дії у вирішенні нагальних заходів [10]. Він встановлює посилені рамки політики ЄС і конкретні заходи щодо:

– сприяння вільним і справедливим виборам і активній демократичній участі;

– підтримки вільних та незалежних ЗМІ;

– протидії дезінформації.

В межах третього пункту Плану Комісія заявила про зміцнення співпраці в цій сфері з Агентством ЄС з кібербезпеки (ENISA), Європейською обсерваторією цифрових медіа (EDMO), Групою експертів з медіаграмотності. У протидії загрозам, включаючи інформаційні, великий наголос ставиться також на розширення можливостей громадян та громадянського суспільства, оскільки цифрова грамотність дозволяє людям безпечно брати участь в онлайн-середивищі.

Інформаційна війна між росією і Сполученими Штатами Америки не є новим феноменом. Але досить активної форми це явище набуло після повномасштабного вторгнення росії в Україну, створивши виклик для Сполучених Штатів, при цьому змусивши офіційних осіб розробити інноваційні інструменти боротьби з інформаційними атаками кремля. Путінський режим ставить перед собою цілі, що росія повинна підірвати позиції США всередині країни, в Європі та в усьому світі, оскільки переконані, що США проводять політику, спрямовану на збереження американської гегемонії та ізоляцію Росії. Дискредитуючи демократичні інститути через дезінформаційні кампанії, росія прагне створити розкол в американському суспільстві.

Активізація зусиль в інформаційній війні з боку авторитарних режимів не залишились непоміченою для влади США. У той же час адміністрація Б. Обами почала активізувати свій загальноурядовий підхід щодо протидії насильницькому екстремізму як усередині країни, так і на міжнародному рівні.

У 2016 році президентом Б. Обамою було підписано указ про офіційне створення Глобального центру взаємодії (Global Engagement Center, GEC), завданням якого було викриття різних форм пропаганди та протидія дезінформаційним зусиллям, спрямованим на підрив або вплив на політику, безпеку або стабільність Сполучених Штатів Америки, їхніх союзників та країн-партнерів [11]. На сьогодні це агентство зазнає всебічної критики зі сторони представників свободи ЗМІ, хоча GEC систематично публікує звіти, в яких описує тактику розповсюдження дезінформації по всьому світу. В рамках боротьби з дезінформацією кремля щодо вторгнення в Україну, GEC почав випускати «Бюлетені кремлівської дезінформації» (Kremlin Disinformation Bulletins).

Крім того, у 2018 році Міністерство внутрішньої безпеки і Міністерство юстиції створили міжвідомчу робочу групу з протидії російській дезінформації Ця робоча група об'єднала Цільову групу з протидії іноземному впливу Міністерства національної безпеки та Цільову групу з кіберцифрових технологій Міністерства юстиції.

Ще одним кроком у руслі забезпечення інформаційної безпеки було «заснування при офісі Директора Національної розвідки США у 2021 році Центру протидії деструктивному іноземному впливу» [12, с. 96].

Розвідувальні структури застосовують тактику розкриття розвідувальної інформації щодо російських кампаній інформаційної війни, діючи з метою попередження і застереження як державного, так і приватного секторів. Так було у випадку підготовки до виборів 2020 року, коли представники ФБР і ЦРУ попередили, що Росія знову спробує ще більше поляризувати американців і втрутитися у вибори. Крім того, розвідувальне співтовариство та адміністрація Байдена в режимі реального часу попереджали про спроби дезінформації щодо COVID-19 та вторгнення в Україну.

З метою громадського контролю та нагляду, «директору Національної розвідки США у координації з міністром оборони було доручено створити в червні 2021 року Центр з аналізу загроз і даних соціальних медіа (Social Media Data and Threat Analysis Center)» [12, с. 96]. Багато аналітиків та експертів вважають, що такі зусилля можуть бути корисними для перемоги над росією та зупинити поширення дезінформації.

Поза межами розвідувальних структур і виконавчої влади, Конгрес почав вирішувати цю проблему, проводячи слухання щодо цієї загрози, розгляд законодавства і тиск на компанії та власників соціальних мереж, щоб вони робили більше для запобігання використанню їхніх платформ як російських інструментів. Більшість запропонованих законопроектів варіюється від санкцій проти Росії до спроб зробити інформацію соціальних мереж більш прозорою щодо джерела інформації Однак через поляризацію поглядів в Конгресі багато законодавчих зусиль зайшли в глухий кут.

В результаті, під тиском уряду та громадськості в цілому, приватні компанії дещо активізували свої зусилля у боротьбі з російською дезінформацією, в тому числі шляхом посилення моніторингу контенту, позначення неправдивої інформації. Зокрема, політичну рекламу почали маркувати як рекламу, яка може містити неправдиві дані або оманливу інформацію. Вплив на приватні медіакомпанії з боку уряду США характеризуються ліберальністю, оскільки свобода слова та свобода вираження поглядів є важливим аспектом американської демократії. Обмеження цих свобод, навіть в розрізі протидії інформаційній війні, може сприйматися як цензура. На відміну від ЄС, де уряд має більше можливостей регулювати приватний сектор, уряд в США, в першу чергу, захищає громадянські свободи.

Використання кіберзасобів задля безпеки критичної інфраструктури, інформаційних мереж, фінансового сектору США, протидія викраденню конфіденційної інформації – це завдання основної збройної організації для наступальної та оборонної кібератівності США, якою є Кіберкомандування США (USCYBERCOM). З огляду на джерела з відкритим доступом, зважаючи на закритість організації, за інформацією Джеймса Ді Пане, аналітика Центру національної оборони США відомо, що «оперативним підрозділом Кіберкомандування США є його Кібермісія (CMF), а команди CMF розподілені між різними наборами місій. Команди CMF CYBERCOM розподілені по функціональних сферах»[14]. Перспективи розвитку цієї організації можна оцінити за сумою бюджетування. Так, в 2022 році бюджет складав 10,4 млрд. доларів, в 2023 р. – 11,2 млрд. доларів. Бюджетний запит Міністерства оборони адміністрації Байдена на 2024 фінансовий рік включає 13,5 мільярдів доларів США на діяльність у кіберпросторі, згідно з Джейсом Ді Пане.

Висновки. В ході дослідження відзначено, що з урахуванням функціонуючої моделі прав людини у Європейському Союзі сформовано низку дієвих інструментів, які спрямовані на організацію протидії інформаційній війні. Закон про цифрові послуги та Посилений кодекс практики щодо дезінформації, в першу чергу, є тими інструментами Європейської комісії. В межах управлінської діяльності запроваджено більше підзвітності та прозорості онлайн-платформ, тісну співпрацю з фактчекерами (дослідниками, які перевіряють контент на наявність підозрілих деталей, спотворених елементів), надання їм кращого доступу до даних, в той же час забезпечення приватності та безпеки даних.

Сполучені Штати Америки характеризуються політикою оцінювання, нагляду та координації влади і громадянського суспільства щодо регулювання інформаційного простору. Експертно-аналітична діяльність акумулюється в Глобальному центрі взаємодії, Центрі протидії деструктивному іноземному впливу, Центрі з аналізу загроз і даних соціальних медіа. У боротьбі з дезінформацією для США необхідно докласти зусиль, а саме федеральному уряду, приватному сектору, засобам масової інформації та пересічним громадянам, щоб ефективно протистояти загрозам інформаційної війни.

ЛІТЕРАТУРА:

1. Звернення Президентки Європейської Комісії фон дер Ляєн на Всесвітньому економічному форумі URL: https://www.eeas.europa.eu/delegations/ukraine/special-address-president-von-der-leyen-world-economic-forum_en?s=232

2. How to Survive an Era of Disruption, Misinformation, and Division URL: https://www.weforum.org/agenda/2024/01/how-to-navigate-an-era-of-disruption-disinformation-and-division/

3. Yuliia Ivashkevych Cooperation between the EU and Ukraine to fight disinformation during wartime URL: https:// https://euneighbourseast.eu/young-european-ambassadors/blog/blog-cooperation-between-the-eu-and-ukraine-to-fight-disinformation-during-wartime/

4. Samantha Lai, Kamya Yadav Operational Reporting in Practice: The EU's Code of Practice on Disinformation URL: https://carnegieendowment.org/2023/11/21/operational-reporting-in-practice-eu-s-code-of-practice-on-disinformation-pub-91060

5. The Strengthened Code of Practice on Disinformation 2022 URL: https://disinfocode.eu/wp-content/uploads/2023/01/The-Strengthened-Code-of-Practice-on-Disinformation-2022.pdf

6. Digital Services Act URL: https://www.eu-digital-services-act.com/

7. European Declaration on Digital Rights and Principles for the Digital Decade URL: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

8. Tackling online disinformation: A European approach. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

9. Action Plan against Disinformation. Brussels, 5.12.2018 URL: https://www.eeas.europa.eu/sites/default/files/action_plan_against_disinformation.pdf

10. On the European Action Plan for Democracy. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0790

11. Evans Jacqueline (2022) Putin's Information War Against the United States Russian Analytical Digest, 282, p.9-12. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/RAD282.pdf

12. Бондар В.Т. Фактор перспективи США та протидія дезінформації: удосконалення системи національної безпеки Вчені записки ТНУ імені В.І. Вернадського . Серія: Публічне управління та адміністрування. Том 34 (73). №5. 2023. С. 94-98. URL: http://www.pubadm.vernadskyjournals.in.ua/journals/2023/5_2023/16.pdf

13. James Di Pane Cyber Warfare and U.S. Cyber Command URL: https://www.heritage.org/military-strength/assessment-us-military-power/cyber-warfare-and-us-cyber-command