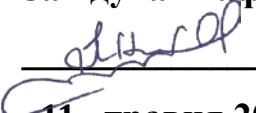


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІСТОРИЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА ПОЛІТОЛОГІЇ ТА МІЖНАРОДНИХ ВІДНОСИН

До захисту допустити:

Завідувач кафедри

 **Максим БУЛИК**
«11» травня 2026 р.

СТРАТЕГІЧНІ НАРАТИВИ І ТЕХНОЛОГІЇ РОСІЙСЬКОЇ
ПРОПАГАНДИ В НІМЕЧЧИНІ

Кваліфікаційна робота здобувача вищої освіти першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Міжнародні відносини» Орловського Дмитра Валерійовича

Науковий керівник: Пахоменко Сергій Петрович, к.і.н., доцент, доцент кафедри політології та міжнародних відносин

Рецензент: Сараєва Ольга Віталіївна, к.і.н., доцент кафедри філософських наук та історії України ДВНЗ «Приазовський державний технічний університет»

Кваліфікаційна робота захищена з оцінкою 93 / А / відмінно

Секретар ЕК



Анастасія ТРОФИМЕНКО

«11» червня 2026 р.

Київ – 2026

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1: ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ.....	10
РОЗДІЛ 2: ГРАНДНАРАТИВИ РОСІЙСЬКОЇ ПРОПАГАНДИ ДЛЯ НІМЕЦЬКОМОВНОЇ АУДИТОРІЇ.....	24
РОЗДІЛ 3: ЕКОСИСТЕМИ РОСІЙСЬКОЇ ПРОПАГАНДИ В НІМЕЧЧИНІ. ВИКОРИСТАННЯ AI ТА LLM.....	31
РОЗДІЛ 4: СТРАТЕГІЇ ПРОТИДІЇ ІНФОРМАЦІЙНОГО ВПЛИВУ.....	46
ВИСНОВКИ.....	53
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	56

ВСТУП

Актуальність теми. У сучасних умовах загострення геополітичної конкуренції інформаційний простір стає ключовим полем протиборства між державами. Російські інформаційні впливові операції в Німеччині набувають особливої актуальності у зв'язку з їх системним, цілеспрямованим і технологічно вдосконаленим характером. Зростання інтенсивності дезінформаційних кампаній, кібератак та пропагандистських наративів, спрямованих на формування громадської думки та вплив на політичні процеси, створює суттєві виклики для демократичної стабільності та національної безпеки Федеративної Республіки Німеччини.

Особливої ваги ця проблема набуває в контексті використання новітніх технологій, зокрема штучного інтелекту (AI) та великих мовних моделей (LLM), які значно підвищують ефективність і масштаб інформаційних операцій. Такі інструменти дозволяють адаптувати пропагандистські повідомлення до конкретних аудиторій, посилювати поляризацію суспільства та підривати довіру до державних інституцій.

З огляду на стратегічну роль Німеччини як одного з провідних політичних та економічних центрів Європейського Союзу, дослідження російських інформаційних впливових операцій є не лише науково релевантним, а й практично значущим завданням. Аналіз стратегічних наративів, каналів поширення та технологічних інструментів пропаганди дозволяє глибше зрозуміти природу сучасних гібридних загроз та сприяє розробці ефективних механізмів протидії.

Таким чином, дослідження стратегічних наративів і технологій російської пропаганди в Німеччині є важливим кроком у зміцненні інформаційної безпеки, підвищенні стійкості демократичних інститутів та забезпеченні стабільності європейського безпекового середовища.

Об’єкт дослідження: операції інформаційного впливу Російської Федерації в Німеччині.

Предмет дослідження: стратегічні наративи, методи, технології та інструменти, які використовуються Росією для здійснення інформаційного впливу на німецьке суспільство.

Постановка проблеми: Проблематика дослідження полягає у необхідності комплексного виявлення та аналізу впливу російських інформаційних операцій на політичні процеси, суспільну думку та соціокультурну динаміку в Німеччині, а також у визначенні ролі новітніх технологій у посиленні цього впливу.

Мета дослідження: Метою роботи є комплексне дослідження характеру, інструментарію та масштабів російських інформаційних впливових операцій у Німеччині з метою оцінки їхнього впливу на політичну систему, суспільство та інформаційне середовище держави.

Завдання дослідження:

- Визначити сутність поняття інформаційної війни, її основні види та сучасні форми прояву; проаналізувати ключові методи інформаційного впливу.
- Дослідити ідеологічне, політичне та стратегічне підґрунтя російських інформаційних операцій, а також їхні цілі та мотиви у німецькому контексті.
- Проаналізувати стратегічні наративи російської пропаганди, адаптовані для німецькомовного інформаційного простору.
- Дослідити екосистему поширення пропаганди, включаючи роль цифрових платформ, соціальних мереж, а також використання AI та LLM.
- Оцінити наслідки інформаційного впливу Росії для політичної стабільності, суспільної довіри та безпеки Німеччини.

Методологічну основу дослідження становить комплекс загальнонаукових та спеціальних методів, застосування яких забезпечило досягнення поставленої мети та виконання завдань дослідження.

Для повного розкриття теоретичних засад інформаційної війни, пропаганди та дезінформації використано метод аналізу та синтезу, що дозволив узагальнити наукові підходи до дослідження інформаційного впливу в сучасних міжнародних відносинах.

Історичний метод застосовано для вивчення еволюції російських інформаційно-пропагандистських практик та особливостей їх трансформації в умовах цифровізації інформаційного простору.

Метод контент-аналізу використано для дослідження змісту стратегічних наративів російської пропаганди, спрямованих на німецькомовну аудиторію, а також для виявлення ключових меседжів і тематичних напрямів інформаційного впливу.

Компаративний метод дав змогу зіставити різні канали поширення пропаганди, особливості функціонування проросійських медіа та підходи до протидії дезінформації в Німеччині й Європейському Союзі.

Системний метод використано для дослідження екосистем російської пропаганди як сукупності взаємопов'язаних акторів, платформ, інформаційних ресурсів та технологій впливу.

Прогностичний метод застосовано для оцінки перспектив використання технологій штучного інтелекту (AI) та великих мовних моделей (LLM) у майбутніх інформаційно-психологічних операціях і для формування рекомендацій щодо протидії цифровій дезінформації.

Стан наукової розробки проблеми. Теоретичні засади інформаційної війни, пропаганди та інформаційного впливу досліджували М. Лібіцький [53; 58], В. Гатчінсон та М. Воррен [43], П. Бланнін [19], М. Аджир та Б. Вайян [5], Дж. Прієр [75], Д. Паркер [76], І. Порче та ін. [70]. У працях зазначених авторів розкрито сутність інформаційної війни, її інструменти, механізми впливу та роль інформаційного середовища у сучасних конфліктах.

Теоретичну основу дослідження стратегічних наративів становлять праці А. Міскіммона, Б. О'Лафліна та Л. Розель [59], а також дослідження у сфері політичної комунікації та масових комунікацій, зокрема теорія „agenda-

setting“ М. Маккомбса та Д. Шоу [60], концепція „фреймінгу“ [35] та сучасні підходи до формування інформаційного порядку денного [32].

Проблематика російської пропаганди та дезінформації в Європі й Німеччині висвітлена у роботах М. Бокші [42], Л. Ламберті та Л. Фрювірт [51], О. Набожняка та співавторів [62], експертів EU DisinfoLab [78], Konrad-Adenauer-Stiftung [47; 48], German Marshall Fund [42], а також у матеріалах Центру протидії дезінформації [3]. У зазначених дослідженнях проаналізовано механізми поширення проросійських наративів, особливості впливу російських інформаційних операцій на європейські суспільства та інструменти протидії дезінформації.

Окремий напрям досліджень становлять питання використання цифрових технологій, соціальних мереж, бот-мереж, штучного інтелекту та великих мовних моделей у процесах інформаційного впливу. Ці аспекти висвітлено у роботах RAND [33; 79], Cyabra [27], Alliance4Europe [64], Politico [54], Sky News [83] та інших аналітичних центрів і медіаплатформ.

Наукова новизна одержаних результатів полягає в тому, що:

1. набуло подальшого розвитку дослідження стратегічних наративів російської пропаганди в німецькому інформаційному просторі шляхом комплексного аналізу їхнього змісту, цілей та механізмів впливу на громадську думку;
2. удосконалено підходи до аналізу екосистеми поширення російської пропаганди в Німеччині через виокремлення взаємозв'язку між традиційними медіа, альтернативними інформаційними платформами, соціальними мережами та цифровими комунікаційними каналами;
3. набуло подальшого розвитку дослідження ролі сучасних цифрових технологій, зокрема штучного інтелекту (AI) та великих мовних моделей (LLM), у процесах створення, адаптації та поширення дезінформаційного контенту в межах російських інформаційно-впливових операцій;
4. на основі аналізу сучасних інформаційних кампаній з'ясовано, що використання технологій AI та LLM підвищує ефективність персоналізації

пропагандистських повідомлень, сприяє їхньому швидкому масштабуванню та ускладнює виявлення дезінформації в цифровому середовищі.

Практичне значення одержаних результатів полягає в можливості використання результатів дослідження у сфері протидії дезінформації, підвищення медіаграмотності та зміцнення інформаційної стійкості суспільства.

Систематизовані в роботі стратегічні наративи російської пропаганди та механізми їх поширення можуть бути використані під час підготовки навчальних і просвітницьких матеріалів з медіаграмотності для студентів, учнів закладів середньої освіти, представників громадських організацій та широкої громадськості.

Результати дослідження можуть бути застосовані у діяльності громадських організацій, волонтерських ініціатив та органів студентського самоврядування для розробки інформаційних кампаній, спрямованих на виявлення та протидію дезінформації в цифровому середовищі.

Практичну цінність становлять також висновки щодо використання технологій штучного інтелекту (AI) та великих мовних моделей (LLM) у сучасних інформаційно-психологічних операціях, які можуть бути враховані під час розробки заходів із протидії цифровій дезінформації та вдосконалення стратегій інформаційної безпеки.

Окремі положення дослідження можуть бути використані для підготовки англomовних інформаційно-аналітичних матеріалів, спрямованих на донесення до міжнародної аудиторії особливостей російських інформаційних операцій у Європі та зміцнення міжнародної підтримки України в умовах російсько-української війни.

Апробація результатів дослідження. Основні положення та результати дослідження були апробовані на науково-практичних конференціях різного рівня, зокрема:

➤ V Міжнародній науково-практичній конференції «Феномен культури постглобалізму: повоєнні світи та культурна демократія» (Маріупольський

державний університет, 27 листопада 2024 р.), де було представлено доповідь на тему „Ukrainian Resilience in an Era of Disinformation“;

➤ Третій Всеукраїнській науково-практичній конференції «Суспільно-політичні трансформації у XXI столітті: локальні, національні та глобальні контексти» (Маріупольський державний університет, 22 травня 2026 р.), де було представлено доповідь на тему „Стратегічні наративи і технології російської пропаганди в Німеччині“.

Результати дослідження опубліковано у матеріалах зазначених науково-практичних конференцій. Загальна кількість публікацій за темою дослідження становить 2 тези доповідей.

Структура бакалаврської роботи зумовлена метою та завданнями дослідження і складається зі вступу, чотирьох розділів, висновків та списку використаних джерел (92 найменування).

У першому розділі досліджено теоретико-методологічні засади вивчення інформаційної війни, пропаганди, дезінформації та кібервійни. Проаналізовано основні наукові підходи до розуміння інформаційного протиборства, його місце в сучасних міжнародних відносинах та особливості функціонування в умовах гібридних конфліктів.

У другому розділі здійснено аналіз основних гранднративів російської пропаганди, спрямованих на німецькомовну аудиторію. Визначено їхній зміст, цільові аудиторії та механізми впливу на суспільну думку Німеччини щодо російсько-української війни та міжнародної політики.

У третьому розділі досліджено екосистеми поширення російської пропаганди в Німеччині, охарактеризовано діяльність проросійських медіа, альтернативних інформаційних платформ і цифрових каналів комунікації. Окрему увагу приділено використанню технологій штучного інтелекту (AI) та великих мовних моделей (LLM) у процесах створення та поширення дезінформаційного контенту.

У четвертому розділі проаналізовано сучасні стратегії протидії інформаційному впливу та дезінформації. Розглянуто досвід Німеччини,

Європейського Союзу та громадянського суспільства у сфері протидії пропаганді, а також визначено перспективні напрями підвищення інформаційної стійкості демократичних держав.

Загальний обсяг роботи становить 71 сторінку, з яких основного тексту — 58 сторінок.

РОЗДІЛ 1.

ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

Методологія дослідження російських інформаційних впливових операцій у Німеччині базується на міждисциплінарному підході, який поєднує політичну науку, міжнародні відносини, медіадослідження, безпекові студії та аналіз цифрових комунікацій. Такий підхід дозволяє комплексно дослідити сучасні форми інформаційної війни, особливості стратегічних наративів та технології, які використовуються Російською Федерацією для впливу на німецьке суспільство. Методологічна база роботи сформована на основі сучасних теорій інформаційної війни, масової комунікації, пропаганди та цифрового інформаційного впливу [19; 43; 53; 70; 75]

Теоретичною основою дослідження виступає концепція інформаційної війни. У сучасних дослідженнях інформаційна війна розглядається як система дій, спрямованих на досягнення стратегічної переваги шляхом контролю інформаційного середовища та впливу на процеси прийняття рішень [43; 76]. На відміну від традиційних форм військового протистояння, інформаційна війна охоплює не лише військову сферу, а й політичні, економічні, соціальні та культурні процеси. Сучасні дослідники підкреслюють, що цифровізація комунікацій значно розширила можливості інформаційного впливу та створила нові інструменти для маніпуляції громадською думкою [19; 70].

Першим етапом дослідження є теоретичний аналіз наукової літератури, присвяченої інформаційній війні, пропаганді та стратегічним наративам. Аналіз літератури дозволяє визначити основні поняття, сформулювати категоріальний апарат дослідження та окреслити ключові підходи до вивчення інформаційного впливу. Особлива увага приділяється роботам, у яких розглядаються принципи інформаційної війни, роль інформаційної переваги та трансформація інформаційного середовища у цифрову епоху [43; 53; 76].

Наступним етапом є аналіз стратегічних наративів російської пропаганди. Для цього використовується концепція стратегічних наративів, відповідно до якої держави формують певне бачення міжнародної політики через комунікаційні практики та інформаційні повідомлення [59].

У межах дослідження аналізуються основні російські наративи, адаптовані до німецького інформаційного простору. До них належать наративи про кризу демократії, «занепад Заходу», недовіру до політичних еліт, економічну нестабільність та загрозу традиційним цінностям. Ключовим методом дослідження є контент-аналіз. Даний метод використовується для систематичного аналізу матеріалів російських медіа, проросійських платформ, Telegram-каналів та контенту соціальних мереж.

Контент-аналіз дозволяє виявити домінуючі теми, повторювані повідомлення та маніпулятивні елементи інформаційних кампаній. Аналізуються не лише тексти, але й візуальні елементи, символіка та емоційні конструкції, які використовуються для впливу на аудиторію. Важливе місце у методології дослідження займає дискурс-аналіз. Цей метод дозволяє дослідити механізми конструювання політичної реальності через мову та символи. Дискурс-аналіз використовується для вивчення способів формування образу Росії, Заходу та Німеччини у пропагандистських повідомленнях. Особлива увага приділяється використанню емоційної риторики, історичних аналогій та поляризаційних наративів. Для аналізу впливу медіа на суспільну думку використовується agenda-setting theory [32; 60]. Відповідно до цієї теорії, медіа впливають на аудиторію шляхом визначення тем, які стають центральними у суспільному дискурсі. У контексті дослідження це дозволяє визначити, які саме теми російська пропаганда просуває у німецькому інформаційному просторі. Особлива увага приділяється питанням війни в Україні, енергетичної кризи, міграційної політики та економічної нестабільності. Поряд із цим використовується framing theory, яка пояснює механізми інтерпретації інформації через певні смислові рамки [35].

Теорія фреймінгу дозволяє дослідити, як одна й та сама подія може бути представлена різними способами залежно від політичної мети. Російська пропаганда активно використовує фреймінг для створення негативного образу Заходу та формування недовіри до демократичних інституцій. Окреме місце у дослідженні займає аналіз соціальних мереж як середовища інформаційної війни. Сучасні цифрові платформи створюють сприятливі умови для поширення дезінформації, використання бот-мереж та маніпулятивного контенту [75].

Соціальні мережі дозволяють швидко поширювати інформацію, створювати ілюзію масової підтримки та здійснювати таргетований вплив на окремі групи населення. Для збору та аналізу інформації використовується OSINT-аналіз. OSINT визначається як систематичний збір та аналіз інформації з відкритих джерел [66; 67; 69]. У межах роботи цей метод застосовується для моніторингу соціальних мереж, аналізу цифрових платформ та виявлення мереж поширення пропаганди. OSINT дозволяє дослідити координацію інформаційних кампаній, цифрову активність та механізми поширення дезінформації. Таким чином, методологія дослідження поєднує теоретичний аналіз, контент-аналіз, дискурс-аналіз, OSINT-аналіз та теорії масової комунікації. Комплексне використання цих методів створює основу для всебічного дослідження стратегічних наративів і технологій російської пропаганди у Німеччині.

Концептуалізація дослідження спрямована на визначення ключових понять, категорій та взаємозв'язків між ними. Центральним поняттям роботи є «інформаційна впливова операція». У межах даного дослідження інформаційна впливова операція розглядається як комплекс координованих дій, спрямованих на формування, зміну або маніпулювання громадською думкою та політичними процесами шляхом використання інформаційних ресурсів, цифрових технологій і комунікаційних інструментів.

Теоретичною основою концептуалізації виступає концепція інформаційної війни. Сучасні дослідники визначають інформаційну війну як

діяльність, спрямовану на досягнення інформаційної переваги шляхом впливу на інформаційні системи, медіа та суспільну свідомість [19; 43; 53; 76]. Інформаційна війна охоплює пропаганду, психологічні операції, дезінформацію, кібероперації та цифрові комунікації. В умовах цифрового суспільства вона стає одним із ключових інструментів геополітичного впливу. Важливим елементом концептуалізації є поняття «стратегічний наратив». Відповідно до сучасних досліджень, стратегічні наративи є комунікаційними конструкціями, за допомогою яких держави формують певне бачення міжнародної політики та власної ролі у світі [59].

Російська Федерація використовує стратегічні наративи для легітимізації власної політики та дискредитації західних демократичних інститутів. У межах дослідження стратегічні наративи розглядаються як один із ключових інструментів інформаційного впливу. Основними російськими наративами у німецькому інформаційному просторі є:

- наратив про «занепад Заходу»;
- антиамериканські та антинатовські меседжі;
- твердження про кризу демократії;
- дезінформація щодо війни в Україні;
- наративи про енергетичну кризу та економічну нестабільність.

Ці наративи спрямовані на посилення соціальної поляризації, формування недовіри до державних інституцій та послаблення європейської єдності. Наступним важливим поняттям є «пропаганда».

Пропаганда визначається як систематичне використання комунікації для впливу на переконання, емоції та поведінку аудиторії [46]. У сучасному цифровому середовищі пропаганда поєднується з алгоритмічними механізмами поширення контенту, соціальними мережами та технологіями штучного інтелекту. Особливе місце у дослідженні займає поняття «дезінформація».

Дезінформація розглядається як навмисне поширення неправдивої або маніпулятивної інформації з метою введення аудиторії в оману. Вона

використовується для створення альтернативної інтерпретації політичних подій, посилення недовіри до медіа та поляризації суспільства. У роботі також використовується поняття «інформаційний вплив».

Інформаційний вплив трактується як процес зміни переконань, політичних позицій та емоційних реакцій аудиторії через комунікаційні механізми. В умовах цифрового суспільства інформаційний вплив здійснюється не лише через традиційні медіа, але й через соціальні мережі, цифрові платформи та алгоритмічні системи. Важливим компонентом концептуальної моделі є цифрові технології впливу. До них належать бот-мережі, алгоритмічне просування контенту, технології мікротаргетингу, штучний інтелект та великі мовні моделі.

Використання AI та LLM дозволяє автоматизувати створення інформаційних повідомлень, адаптувати їх до конкретних аудиторій та значно масштабувати дезінформаційні кампанії. Значну роль у сучасних інформаційних операціях відіграє OSINT. Аналіз відкритих джерел дозволяє збирати інформацію про аудиторії, досліджувати цифрову активність та виявляти мережі поширення пропаганди [66; 67; 69]. У контексті російських інформаційних операцій OSINT використовується для аналізу суспільних настроїв та адаптації інформаційних кампаній до конкретних груп населення.

Таким чином, концептуальна модель дослідження базується на взаємодії трьох основних компонентів: стратегічних наративів, технологічних інструментів та цифрових каналів поширення інформації. Їхня взаємодія створює основу сучасних російських інформаційних впливових операцій у Німеччині та визначає їхній вплив на політичну систему, суспільство та інформаційне середовище держави.

У наш час, існує безліч підходів до трактування поняття «інформаційна війна». Частина науковців вважають, що інформаційна війна – це форма ведення інформаційного протиборства між різними суб'єктами (державами, неурядовими та іншими структурами), який передбачає проведення комплексу заходів із нанесення шкоди інформаційній сфері конфронтуючої сторони й

захисту власної інформаційної безпеки. Інформаційну війну розглядають також як сукупність спеціалізованих (фізичних, інформаційних та програмних) методів і засобів тимчасового або безповоротного виводу з ладу функцій, або служб інформаційної інфраструктури загалом, або окремих її елементів [2].

Інформаційна війна є цілісною стратегією, яка обумовлена всезростаючою значимістю та цінністю інформації в питаннях керування, політики, міжнародних відносин, економіки, та громадського життя. Інформаційна війна є систематичною серією нападів на цивільне та військове населення держави, державою-противником через дезінформацію та пропаганду для досягнення значних політичних та військових цілей. Також, інформаційна війна визначається як дії, які спрямовані задля досягнення інформаційної переваги шляхом впливу на основні інформаційні процеси, комп'ютерні мережі інформації противника.

Підсумувавши вище зазначене, можемо зробити висновок про те, що основною метою інформаційної війни є саме, в послабленні не тільки моральних, так і в матеріальних сил супротивника, при цьому якнайшвидше робити посилення власних, використовуючи порушення обміну інформації. Інформаційна війна включає заходи пропагандистського впливу на свідомість суспільства, які безпосередньо не призводять до кровопролиття та руйнувань, проте порушують державний управлінський механізм. Це є прихована війна, наслідки якої призводять до повільного знищення держави.

Головне завдання інформаційних війн полягає в маніпулюванні масами. Мартін Лібікі є одним із провідних теоретиків у галузі інформаційних війн – у своїй книзі «Що таке інформаційна війна?», визначає 7 форм інформаційної війни:

- 1) Командно-штабна війна (Command-and Control Warfare), яка завдає ударів по голові та шиї противника. Метою цього типу війни є усунення або рішуче виведення з ладу загальновійськового керівництва та його засобів управління. Це може бути зроблено двома способами: з одного боку, шляхом

безпосередньої атаки на командний склад або об'єкти командування і управління ("проти голови (Antihead)"), а з іншого боку, шляхом знищення або порушення роботи засобів зв'язку ("проти шиї(Antineck)") [58, с. 9-54, 67-81].

2) Війна на основі розвідки (Intelligence-based Warfare), яка полягає в розробці, захисті систем, які прагнуть отримати достатньо інформації для домінування на полі бою. Це стосується безпосереднього включення результатів розвідки в бойові операції в режимі реального часу. Це покращує координацію сил під час операцій і дозволяє уражати цілі більш швидко і безпосередньо. Датчики використовуються для створення видимості бойового простору і забезпечення комплексної ситуаційної обізнаності [58, с. 9–54, 67–81].

3) Радіоелектронна боротьба (Electronic Warfare), радіоелектронні або криптографічні методи. Радіоелектронна боротьба або "електронна війна" - це сукупність усіх військових заходів, що використовують електромагнітне випромінювання для отримання інформації про супротивника:

- для збору інформації про противника
- для запобігання використанню електромагнітного спектра електромагнітного спектру противником, а також для забезпечення використання електромагнітного спектру у власних цілях [58, с. 9–54, 67–81].

4) Психологічна війна (Psychological Warfare), в якій інформація використовується для зміни свідомості друзів, нейтралів і ворогів. З розвитком інформаційних технологій можливості і засоби психологічної війни також досягли нових вимірів. Інформацію та дезінформацію тепер можна набагато легше донести до ширшої або більш конкретної цільової групи. Психологічна війна спрямована як зовні проти ворогів, так і всередині проти власного народу. Лібічкі розрізняє чотири форми психологічної війни: [58, с. 9-54, 67-81].

- проти волі: спрямована проти національної волі держави/народу; включає всі наміри вплинути на громадську думку; в цьому контексті можна розглядати, наприклад, військові паради Радянського Союзу, які мали на меті

привнести військову міць у свідомість західного населення, а також "вісь зла" або часткові, цензуровані репортажі з війни в Іраку. До цієї сфери також належать ЗМІ та компанії, які намагаються впливати на громадську думку у власних цілях.

- контрсили: спрямовані проти ворожих сил; сюди відносяться, наприклад, спроби переконати ворожих солдатів здатися або дезертирувати, або підірвати довіру до власного керівництва; тут також є багато прикладів в Іраку, коли коаліційні сили пояснювали іракським солдатам безнадійність їхньої боротьби і, таким чином, переконували їх здатися.

- контркомандир: спрямований проти ворожих командирів; тут велике значення надається плутанині та обману; плутанина використовується для створення несподіванки, в той час як видимість того, що ми діємо у спосіб, який очікує ворог, передбачає безпеку.

- контркультура: культурна війна; це насправді суперечлива форма психологічної війни; в принципі, під нею розуміють вплив іноземних норм і цінностей на власну культуру під страхом втрати власної ідентичності або, навпаки, розпалювання страхів, націоналізму і почуття "ми" і пов'язаного з цим виключення іноземців. Важливу роль тут відіграють нові, важко контрольовані медіа, такі як Інтернет.

5) Хакерська війна (Hacker Warfare), коли атакують комп'ютерні системи. Цей тип інформаційної війни передбачає використання вразливостей безпеки в цивільних комп'ютерних мережах для атак на інфраструктуру, бізнес і фінанси. Низькі витрати в поєднанні з високим впливом, якого можна досягти, роблять цю сферу ключовим полем для ведення інформаційної війни. Військовий аналог цього явища, швидше за все, можна знайти в C2W, хоча цю межу, безумовно, не можна провести чітко [58, с. 9–54, 67–81].

6) Економічна інформаційна війна (Economic Information Warfare), блокування інформації або спрямування її для досягнення економічного домінування. ЕІВ є сполучною ланкою між економічною та інформаційною війнами. Лібічкі розрізняє дві форми: інформаційну блокаду та інформаційний

імперіалізм. З одного боку, за аналогією з економічною блокадою, країна повинна бути змушена переслідувати власні інтереси шляхом блокування знань та інформації. З іншого боку, спеціалізація на певних галузях промисловості покликана підтримувати конкурентоспроможність і закріплювати цю позицію за рахунок високої наукоємності та ноу-хау [58, с. 9-54, 67-81].

7) Кібервійна (Cyberwarfare), набір футуристичних сценаріїв. У цьому контексті Лібіцкі говорить про інформаційний тероризм, семантичні атаки, симуляційну війну та війну Гібсона.

- Інформаційний тероризм: фактично є продовженням ГВ, але націлений не на самі мережі, а на людей та організації, що стоять за ними.

- Семантичні атаки: на перший погляд ідеально функціонуюча система повинна бути обманута і таким чином спровокована на певні реакції; наприклад, обман сейсмічних датчиків атомної електростанції може призвести до її зупинки.

- Симуляційна війна: основна ідея полягає в тому, що війна більше не відбувається на полі бою, а моделюється у віртуальному просторі, причому результат є обов'язковим для всіх сторін конфлікту.

- Війна Гібсона: заснована на творах письменника-фантаста Вільяма Гібсона, війна Гібсона є подальшим розвитком симуляційної війни. Автор перетворює своїх протагоністів на персонажів віртуального світу, які воюють один з одним [58, с. 9–54, 67–81].

Тепер розглянемо таке явище, як Гібридна війна. В загальному, це використання низки різних методів для нападу на супротивника, до прикладу, поширення неправдивої інформації або ж атаки на важливі комп'ютерні системи супротивника та традиційні військові дії.

Джозеф Най (Joseph S. Nye, Jr.) - «гібридна війна», «м'яка сила» та «розумна сила». Його основні ідеї: по-перше, «Класичні війни перестали бути основним способом досягнення політичних цілей, вони трансформувалися і

стали гібридами. Це «війни четвертого покоління», в них немає чітких меж боїв, зникають відмінності між цивільними і військовими.[63]

По-друге, у гібридних війнах беруть участь не лише держави, а й недержавні гравці: повстанці, терористи, бойовики, кримінальні організації. Конфлікт виглядає як насильницькі операції нерегулярних збройних формувань. Вони здійснюються протягом тривалого періоду часу і дозволяють встановити силовий контроль над місцевим населенням.[63]

Інформація стає ключовим ресурсом влади, і все більше людей отримують доступ до цього ресурсу. Це означає, що політика більше не є прерогативою лише урядів. На відміну від засобів масової інформації (радіо, телебачення, газети), які контролюються видавцями, Інтернет забезпечує необмежену комунікацію між користувачами. Той факт, що кожна людина має мобільний телефон з камерою та комп'ютер з будь-яким графічним редактором, робить кожного з нас інформаційними воїнами.

Все це призводить до трансформації сили, її розмивання, однак великі держави все одно матимуть більше ресурсів для війни. Ці ресурси не тільки технологічні. Цей ресурс - м'яка сила. М'яка сила - це культура, політичні та соціальні цінності, спосіб життя, зовнішня політика. Ненасильницькі методи індоктринації, завоювання довіри до своєї країни через інформаційне просування своїх цінностей.[63]

Розумна сила - це поєднання «м'якої» та «жорсткої» сили. Жорстка сила - це класичні фізичні насильницькі методи, наприклад, у боротьбі з терористами.

М'яка сила - залучення і завоювання довіри маси, тобто переконання, вплив, маніпуляції, стимулювання.[63]

Отже, поняття інформаційної війни трактується за допомогою різних підходів. Їх об'єднує одна головна зброя такої війни - інформація. Через технологічний підхід - інформаційна війна - це дії, спрямовані на виведення з ладу комп'ютерних систем збору, обробки та розповсюдження інформації супротивника. Це виведення з ладу комп'ютеризованих систем управління

економікою, державним управлінням, критичною інфраструктурою, збройними силами противника.

Інформаційна перевага досягається шляхом впливу на інформацію, інформаційні процеси та комп'ютерні мережі противника. Згідно з однією точкою зору, «інформаційна війна» та «інформаційне протиборство» розглядаються як синоніми. Однак, згідно з іншої точкою зору, інформаційна війна, як більш широке поняття, є вищим рівнем інформаційного протиборства, яке складається з різних інформаційних операцій. Тобто, інформаційні операції є частиною інформаційної війни.

Інформаційні операції - це сплановані дії, спрямовані на ворожу, дружню або нейтральну аудиторію з метою впливу на прийняття управлінських рішень або вчинення дій, вигідних суб'єкту інформаційного впливу. [1]

Щодо періоду ведення інформаційної війни. На відміну від класичних війн, його важко визначити. Одна справа, коли інформаційна війна супроводжує фізичний військовий конфлікт (а вона завжди його супроводжує). Тоді ми можемо визначити її початок і кінець, відповідно до того, коли почався і закінчився відкритий фізичний конфлікт. Це тільки на перший погляд все просто. Інформаційна війна може бути частиною гібридної війни. Вона починається задовго до початку фізичного зіткнення і може тривати після його завершення. Тому показники періоду інформаційної війни є дуже нечіткими та розмитими.

Таким чином, інформаційна війна є комплексним поняттям. У найзагальнішому вигляді - це широкомасштабний вплив на інформаційні системи, комп'ютерні мережі, масову свідомість з метою досягнення інформаційної переваги над супротивником. Інформаційна війна поєднує в собі дві складові, а саме технологічну та психологічну.

Походження терміну «Кібервійна» за Аркіллою і Ронфельдом. Термін «Кібервійна» є військово-політичним терміном і має на меті врахувати глобальні зміни, які особливо відбуваються в політиці та військовій сфері. Можливе застосування АВС-зброї (зброї масового знищення) також розкриває

межі війни, оскільки такі війни неминуче стануть «тотальними війнами» і загрожуватимуть самому існуванню людства. Аркілла і Ронфельдт бачать вихід з цієї дилеми в інформаційній революції і масовому поширенні ІКТ-технологій (Інформаційно-комунікаційні технології) [25, с. 23-55; 26].

Інформація залишається центральним ресурсом інформаційної війни, але з нею також потрібно поводитися належним чином, саме тому Аркілла і Ронфельдт підкреслюють можливості ІКТ-технологій і, як наслідок, розрізняють «кібер-війну» і «мережеву війну»: «Ми пропонуємо розрізняти “ідеологічні конфлікти” на рівні суспільства, що ведуться за допомогою інтернет-комунікацій, які ми називаємо “мережевою війною”, і “кібер-війну” на суто військовому рівні» [25, с. 23–55; 26]. На думку Аркілли і Ронфельдта, «кібервійна» відноситься до будь-якого військового конфлікту «на інформаційній основі», зокрема, до атак на інфраструктуру ІКТ:

«Кібервійна означає проведення і підготовку до проведення військових операцій відповідно до принципів, пов'язаних з інформацією. Це означає підрив, якщо не знищення інформаційно-комунікаційних систем, що в широкому розумінні включає навіть військову культуру, на які супротивник покладається для того, щоб «знати» себе: хто він, де він, що він може зробити, коли, чому він воює, яким загрозам протидіяти в першу чергу і т.д. Це означає намагання знати все про супротивника, не даючи йому знати багато про себе» [25, с. 23–55; 26].

«Мережева війна», у свою чергу, базується на суспільних конфліктах, які виникають внаслідок діяльності у віртуальному світі. В першу чергу це стосується дій, спрямованих на вплив на ЗМІ.

«Нетворк відноситься до інформаційного конфлікту на великому рівні між націями або суспільствами. Це означає намагання підірвати, пошкодити або змінити те, що цільова група населення «знає» або думає, що знає про себе та навколишній світ. Мережева війна може бути зосереджена на громадській або елітній думці, або, що більш ймовірно, на обох. Вона може включати заходи публічної дипломатії, пропагандистські та психологічні кампанії,

політичну та культурну підривну діяльність, обман або втручання в роботу місцевих ЗМІ, а також зусилля з просування дисидентських або опозиційних рухів через комп'ютерні мережі» [25, с. 23-55; 26].

Якщо тенденція між «кібервійною» та «мережевою війною» матиме аналітичний характер і поступово буде усвідомлена, або якщо емпірично буде виявлено протиріччя між ними, вона все одно залишатиметься відкритою. Однак Аркілла і Ронфельдт припускають зміну парадигми і те, що «кібервійна» матиме багато облич, а саме: вона буде адаптована до різних контекстів; вона не представлятиме і не нав'язуватиме єдиного, структурованого підходу.

Кібервійна може бути наступальною і оборонною, на стратегічному і тактичному рівнях. Вона охоплюватиме весь спектр інтенсивності - від конфліктів, що ведуться важкими механізованими військами на широких театрах, до контрповстанських дій, де «мобільність черевики» може бути головним засобом маневру.

Аркілла також описав ройову тактику в мережевих війнах. Для цього слід застосовувати принцип «роїння» (роїтися, як бджоли). Рой характеризується наступними ознаками: автономні або напівавтономні одиниці, аморфна, але скоординована атака в усіх напрямках, постійне застосування сили або вогню, багато розрізнених маневрених одиниць з підключенням до Інтернету, загальний нагляд і координація на самому верху, спрямування атак на знищення ворожої одиниці. Роїння також використовують терористи та повстанці [25, с. 23–55; 26].

Рой - це організація спонтанного натовпу за допомогою цілеспрямованих дій. Неорганізований натовп повинен бути зібраний тоді і там, де вже присутні підготовлені спеціальні бойові групи. Їх основна функція - вміло використовувати неорганізований натовп на власну користь. У деяких випадках головне завдання полягає в тому, щоб спровокувати натовп на насильство. Але в набагато більшій кількості випадків першочерговим завданням рою є організація кровопролиття.

Оскільки натовп зовні неорганізований і включає в себе не тільки чоловіків, але й жінок і дітей, саме вони, як найменш пристосовані члени рою, найчастіше стають жертвами сутичок, тисняви та інших ексцесів, характерних для натовпу. Як наслідок, терористи і повстанці налаштовують цих жертв проти урядових сил і будують на цьому свої наступальні операції в інформаційному просторі та політичному вимірі. Тактика натовпу використовується різними сторонами. Кровопрлиття і сакральні жертвоприношення мають дуже сильний емоційний ефект, а особливо, коли це все доступно в прямому ефірі телебачення [25, с. 23–55; 26].

РОЗДІЛ 2:

ГРАНДНАРАТИВИ РОСІЙСЬКОЇ ПРОПАГАНДИ ДЛЯ НІМЕЦЬКОМОВНОЇ АУДИТОРІЇ

Наративи, які поширює Росія у Німеччині:

➤ Наратив: **„Втрата суверенітету та зовнішнє управління США та НАТО“** є твердження про те, що ФРН нібито втратила свій суверенітет і перебуває під зовнішнім управлінням США та НАТО. У межах цього наративу Німеччина подається не як незалежний геополітичний актор, а як держава, що реалізує американські стратегічні інтереси навіть у супереч власним політичним та економічним потребам (30; 48).

Поширення такого наративу спрямоване на формування уявлення про обмежений суверенітет Німеччини та дискредитацію її зовнішньополітичних рішень, насамперед у сфері безпеки та співпраці з НАТО (48). Дослідження також показують, що ця теза активно відтворюється німецькими ультраправими альтернативними медіа, зокрема Compact та Junge Freiheit, де вона використовується як інструмент критики федерального уряду та чинного політичного курсу [91]. У результаті наратив про «зовнішнє управління» виконує ширшу стратегічну функцію — підриває довіру до державних інституцій ФРН та послаблює підтримку трансатлантичного партнерства [47].

➤ Наратив: **„Економічне самогубство“**. Ще одним важливим наративом російської пропаганди в Німеччині є теза про те, що санкції проти Росії та відмова від російських енергоносіїв нібито призводять до «економічного самогубства» країни. У межах цього наративу стверджується, що антиросійські санкції завдають більшої шкоди німецькій економіці, ніж російській, спричиняючи деіндустріалізацію, закриття підприємств і масове зuboжіння населення [78] .

Для посилення цього меседжу в інформаційному просторі поширювалися фейкові новини та маніпулятивні матеріали про нібито неминучий економічний колапс Німеччини. Такі повідомлення активно розповсюджувалися через скоординовані мережі ботів і проросійських інформаційних ресурсів, що збільшувало їхню видимість та охоплення аудиторії [33; 78].

Основною метою цього нарративу було формування страху серед німецьких виборців і бізнес-спільноти, а також посилення суспільного тиску на уряд щодо перегляду санкційної політики та скорочення підтримки України [48; 78].

➤ Наратив: **„Загроза Третьої світової війни“** - військова допомога Україні нібито робить Німеччину безпосереднім учасником війни та наближає початок Третьої світової війни. У межах цього нарративу постачання озброєння Києву подається як крок, що провокує Росію до ескалації конфлікту, включно із застосуванням ядерної зброї [30; 91].

Для посилення цього меседжу російські державні медіа та проросійські німецькі інформаційні ресурси представляють військову підтримку України не як допомогу державі, що захищається від агресії, а як «розпалювання війни» та безвідповідальне втягування Європи у масштабний конфлікт [30; 47]. Таким чином увага зміщується з питання російської агресії на потенційні ризики для самої Німеччини.

Цей наратив спрямований на використання традиційно сильних пацифістських настроїв у німецькому суспільстві та історичного страху перед великою війною в Європі. Його метою є послаблення суспільної підтримки оборонної політики Берліна та зменшення готовності Німеччини надавати військову допомогу Україні [30; 48].

➤ Наратив: **„Дискредитація України та українців“**. У межах цього нарративу Україна зображується як штучна, корумпована та «нацистська» держава, яка не заслуговує на міжнародну підтримку. Одночасно українські біженці в Німеччині подаються як економічні мігранти, що нібито

використовують соціальну систему країни та живуть за рахунок німецьких платників податків [78; 91].

Для поширення цих меседжів активно використовуються німецькомовні сегменти Telegram і TikTok, де циркулюють вигадані або непідтверджені історії про злочини, привілейоване становище чи надмірні соціальні виплати для українців [78]. Такі повідомлення апелюють до соціального невдоволення та економічних побоювань частини населення.

Основною метою цього наративу є зниження рівня підтримки України серед німецького суспільства та послаблення співчуття до українців як жертв російської агресії. Водночас поширення подібних тверджень сприяє загостренню соціальної напруги та провокує конфлікти між різними групами населення всередині Німеччини [48; 78].

➤ Наратив: **«Русофобія» та «занепад Заходу»**. У межах цього наративу західна ліберальна модель подається як така, що перебуває у стані морального та політичного занепаду, тоді як критика російської влади трактується не як реакція на дії Кремля, а як прояв упередженого та ірраціонального ставлення до Росії, яке визначається як «русофобія» [47; 91].

Важливу роль у поширенні цього наративу відіграють німецькі ультраправі медіа та альтернативні інформаційні платформи. У їхньому дискурсі Володимир Путін часто зображується як захисник традиційних цінностей і національного суверенітету, який протистоїть глобалізму та ліберальним тенденціям Заходу [91]. Така інтерпретація сприяє формуванню позитивного образу російського політичного керівництва серед частини аудиторії.

Окремим напрямом є вплив на російськомовну громаду Німеччини, зокрема на Russlanddeutsche. Через поширення наративів про нібито дискримінацію російськомовних мешканців формується відчуття відчуження від німецького суспільства та посилюється недовіра до державних інституцій [30; 48]. Таким чином цей наратив сприяє суспільній поляризації та зміцненню проросійських настроїв серед окремих груп населення.

➤ Наратив: „**Росія воює проти фашистів**“. Війна в Україні, яку в Росії називають спецоперацією, є домінуючою темою російських новин і ток-шоу. Наратив про «фашистську Україну» є одним із найбільш часто повторюваних спотворень у ефірах. Після анексії Криму в 2014 році російські державні ЗМІ стверджували, що Україною правили фашисти чи нацисти. Це відбувається незважаючи на те, що з травня 2014 року праві екстремісти не були представлені жодною партією в київському парламенті та не входили до уряду. Існують правоекстремістські групи, але вони не є політичною силою, яка домінує в усій країні, оскільки RT DE регулярно піддає аудиторії в Німеччині, щоб дискредитувати Україну на міжнародному рівні.

Терміни «фашисти» і «нацисти» використовуються як синоніми; вони відірвані від свого початкового значення і стосуються політичних опонентів. З одного боку, наратив виконує функцію покладання відповідальності за військову агресію на ворога. З іншого боку, це слугує легітимізації війни Росії та має на меті послабити міжнародну солідарність з Україною. За її власними заявами, Росія не тільки воює проти фашистів чи нацистів в Україні, а й звинувачує у фашизмі всі ті держави, які підтримують Україну у війні проти Росії. Це стосується і Німеччини, особливо коли йдеться про постачання зброї в Україну [15].

➤ Наратив: „**Росіяни й українці — один народ**“. Важливий наратив у російських державних ЗМІ спрямований на заперечення права України на існування як суверенної держави. Для цього пропагується уявлення про те, що це «один народ» і що Україна, як частина Росії, не є окремою нацією зі своєю історією. Однак таке тлумачення суперечить українській історіографії та процесу деколонізації від Російської імперії та Радянського Союзу. «Денацифікація», якої Росія нібито прагнула у війні, насправді означає «звільнення» України не від фашизму, як стверджується, а від власної історії та власної незалежної від Росії держави – тобто де-факто знищення її незалежності. Повернення на російську територію вимушене війною.

Відповідно, державні ЗМІ говорять про «повернення на культурну батьківщину».

Російські пропагандисти зображують українців земляками, яких заплутав Захід. Наприклад, ведучий Дмитро Кисельов у «Новинах тижня» на телеканалі «Россия 1» 24 липня 2022 року стверджував: «Радикальних націоналістів і нацистів завжди турбувала традиційна церква і віра, їх віддирали назад. і далі (...) Є мода на ЛГТБ, наркотики, усілякі покидьки». Україна — це поле битви цивілізацій: «Захід не тільки наповнив країну зброєю, але й всадив у голови всяку нісенітницю». Кисельов був першим російським журналістом, який потрапив до санкційного списку ЄС у 2014 році через підтримку анексії Криму через пропаганду [15].

➤ Наратив: **„Захід веде війну проти Росії“**. Згідно з наративом у російських державних ЗМІ, не Росія напала на Україну, а Захід вів війну проти Росії в Україні. З одного боку, це легітимізує війну: Росія з винуватця перетворюється на жертву і змушена захищатися від Заходу. З іншого боку, мета полягає в тому, щоб викликати сумніви серед населення за кордоном щодо нібито агресивного курсу західних урядів щодо Росії і таким чином поставити під сумнів підтримку України.

Тому в Німеччині особливо обговорюють передбачувані помилки Заходу. Автор RT DE Ульріх Гейден у своїй статті від 27 лютого 2022 року написав: «Путін бачить Україну як плацдарм НАТО. Їхні ракети наблизяться до Росії навіть без членства України в НАТО. Тож хто грає з Третьою світовою війною? Захід чи Путін?», – риторично запитав він. Цей аргумент свідчить про те, що у Росії не було іншого вибору, як напад на Україну. У статтях часто припускають, що на «Заході» є «русофобія» по всьому світу, тобто образа на росіян [15].

➤ Наратив: **„Підтримка України призводить до занепаду Німеччини“**. Репортажі іноземного мовника RT DE конкретно стосуються страхів людей перед економічним занепадом або військовою конфронтацією з Росією, щоб використати їх у політичних цілях і послабити підтримку

політики німецького уряду щодо Росії. RT DE в кількох статтях попереджав, що своєю політикою німецький уряд ризикує ядерною війною з Росією. Сам президент Росії Путін у вересні 2022 року погрожував Заходу застосуванням ядерної зброї, викликавши побоювання в німецькому суспільстві. Також прогнозується економічний колапс: федеральний уряд хоче «повного знищення німецької економіки», попередив економіст Ейке Хамер. В експертному інтерв'ю 6 вересня 2022 року на RT DE, він побоювався найгіршої економічної кризи, «яку Європа бачила за останні 200 років».

Підвищення цін, особливо на енергоносії, часто обговорюється в статтях, створюючи враження, що Німеччині загрожує економічний спад без російського газу. Індивідуальні дописи часто присвячені політикам, які підтримують цей наратив, наприклад, лівому політику Сахрі Вагенкнехт з її промовою в Бундестазі 8 вересня. Вагенкнехт звинуватив «федеральний уряд у забезпеченні того, що мільйони німецьких громадян занурені в бідність, тому що вони просто не хочуть визнати, що процвітання та промисловість Німеччини не можуть підтримуватися без дешевої російської енергії», цитує Вагенкнехт RT DE [15].

➤ Наратив: „**Росія на боці протестів**“. Поки протести та демонстрації в Росії придушуються поліцією, RT DE позитивно розповідає про демонстрації проти уряду в Німеччині та висловлює солідарність з незадоволеними своїми репортажами. З моменту свого запуску в Німеччині в 2014 році RT DE і SNA використовували кризи, щоб атакувати демократію та зобразити політичну систему як нефункціональну. Невдоволених звертаються і використовують як «ресурс в інформаційній війні» проти Заходу відповідно до стратегії, яку пояснює бос RT Симоньян. Якщо раніше це були демонстрації Корони та сторонні мислителі, то тепер у центрі уваги протести проти економічної політики уряду [15].

Російська дезінформаційна машина в Німеччині працює не через поодинокі фейки, а через структурні моделі:

- Модель «Потоку фальші» (Firehose of Falsehood): Висока інтенсивність повідомлень, багатоканальність (соцмережі, Telegram, підробні сайти) та повне ігнорування об'єктивних фактів. Головна мета — перевантажити когнітивні спроможності аудиторії, посіяти сумніви («не все так однозначно») та викликати тотальний цинізм до будь-яких джерел інформації [79].
- Кампанія «Двійник» (Doppelgänger): Масштабні операції в німецькому інформпросторі, що включали створення точних клонів авторитетних німецьких видань (наприклад, Der Spiegel, Bild, Sueddeutsche Zeitung), на яких розміщувалися прокремлівські статті [33; 78].
- Ідеологічна конвергенція: російські геополітичні міфи легко адаптуються німецькими радикальними силами, оскільки вони мають спільного ворога — ліберальний уряд Німеччини та євроатлантичний вектор розвитку [47; 91].

РОЗДІЛ 3.

ЕКОСИСТЕМИ РОСІЙСЬКОЇ ПРОПАГАНДИ В НІМЕЧЧИНІ.

ВОКРИСТАННЯ AI ТА LLM

Багато ЗМІ з ідеологічним „ультралівим чи ультраправим“ ухилом або конспірологічним спрямуванням, позиціонуючи себе як "альтернативу мейнстріму" у своїх наративах підтримують Росію та її агресивні дії в Україні.

Серед них, наприклад, видання Arolut [6], засноване Кеном Єбсеном: він же „Кайван Суфі-Сіаваш“, автори якого дуже скептично оцінюють шанси України на перемогу у війні з Росією, називають Україну "нацистською державою", звинувачують її в переслідуванні релігійних громад та перекладають провину за агресію на Захід. Окрім статей, медіа-група "Аполут" також виробляє відео та подкасти. Раніше Єбсен був відомий як засновник радіо „KenFM“ та активіст, який брав участь у заходах проти вакцинації. Зараз він часто коментує різні питання для пропагандистських ЗМІ, в тому числі для державного інформаційного агентства Білорусі.

Ще одним впливовим гравцем у світі "альтернативних" медіа є журнал „Contrast“, щомісячний політичний журнал під керівництвом Юргена Ельзессера. З 2015 року „Contrast“ позиціонує себе як рупор правопопулістської партії "Альтернатива для Німеччини" (AfD) та антиісламського руху „Pegida“. У його публікаціях регулярно з'являються теорії змови, історичні ревізіоністські та антисемітські теми [21].

Однак у 2022 році, це не завадило журналу розмістити на обкладинці фотографію лівої партії. Сахра Вагенкнехт „Лідерка (Лівих - Die Linke)“ з підписом "Найкраща канцлерка" [24]. Щодо Росії, журнал вихваляє "нову еру політики", ініційовану Володимиром Путіним, нагнітає напруженість у відносинах між Польщею та Україною і поширює конспірологічні теорії про можливий поділ України між Росією і НАТО. Юрген Ельзессер є не лише

активним учасником проросійських мітингів, але й коментує європейські події та російсько-українську війну для маргінальних російських пропагандистських ЗМІ. Його статті також використовуються в пропагандистських цілях. „Comrast“ також вважається ключовою платформою для руху Querdenken ("Латеральних мислителів") - прихильників теорії змови, які часто становлять значну електоральну групу серед виборців (AfD).

Під час пандемії COVID-19 цей рух поширював дезінформацію про здоров'я. Але зі зростанням напруженості між Росією та Україною, особливо після початку повномасштабного вторгнення, вони активно транслиують наративи російської пропаганди. До них належать історії про те, що війна організована США, що імперіалістичний Захід пригнічує антиколоніальну Росію, а також про те, що в Україні широко поширені таємничі біолабораторії.

Також варто згадати сайт „Manova News“ [55; 56; 57], раніше відомий як "Рубікон". Тут в унісон з російською пропагандою розповідають про жорстоких бійців "Азова", які розстрілюють мирних жителів Донбасу, про „обраність“ і „високу духовність“ російського народу, а також про необхідність якнайшвидшого переходу до мирних переговорів з агресором - імовірно, на його умовах [28].

Антиєвропейські, антизахідні та проросійські меседжі також поширюють такі видання, як „Nachdenkseiten“ - цей конспірологічний альтернативний блог пов'язують з колишнім політиком (СДПН - Альбрехтом Мюллером), ліва марксистська газета „Junge Welt“, антикапіталістичний „Overton Magazin“ [68], ультраправий журнал „Zuerst!“ та „Report24“ [80], близький до правої опозиційної партії (AfD). Подібні наративи публікують і менші видання, такі як нішевий консервативний таблоїд „Weltexpress“, який прямо повторює російські наративи про "уक्रофашизм" і значну роль російських миротворців у конфлікті в Нагірному Карабасі, або видання „Unzensuriert.de“, її ще називають дочірньою компанією однойменного австрійського видання, близького до ультраправої партії „FPÖ“.

Крім того, у німецькомовному інформаційному просторі з російськими наративами працюють такі портали, як „Unser Mitteleuropa“ [72], це є австрійське багатомовне видання з непрозорим засновником "Європейський інститут політичних досліджень і медіа-мереж" з Гонконгу, вважається близьким до „FPÖ“ та „AfD“, домен зареєстрований у Росії, австрійський медіа-холдинг „AUF1“ - розповсюджувачі теорій змови та російської пропаганди, анонімний швейцарський портал "альтернативних новин" (Uncut News), тощо.

Окрім "традиційних" ЗМІ, які все ще користуються популярністю серед німецьких глядачів і читачів, набирають обертів Telegram-канали - "нові медіа" на платформі, яка, як вважають, співпрацює з російськими спецслужбами. Окрім офіційних каналів традиційних видавництв і мовників, таких як „RT.de“ або „AUF1“, у Telegram також є блоги окремих особистостей або анонімні дискусійні платформи.

Більшість значущих конспірологічних Telegram-каналів для німецькомовної аудиторії так чи інакше підтримували Росію та її "спеціальну військову операцію" в Україні в лютому 2022 року. Серед них - канали відомих німецькомовних конспірологів, а саме: Єви Герман, Бодо Шиффмана (Alles Ausser Mainstream, букв. "Все, крім мейнстріму") та Райнера Фюельміха. Також, на бік Путіна стали канали саксонської маргінальної політичної партії Freie Sachsen ("Вільні саксонці") та "альтернативні" ЗМІ AUF1, Freie Medien ("Вільні медіа") і Ken Jebsen - Aufklärung und Information ("Кен Єбсен - роз'яснення та інформація"), стверджують дослідники.

Найактивніше посилання на новини „RT.DE“ поширювали різні анонімні групи, такі як: „QANONYMOUS KANAL DEUTSCHLAND“, „17News17“, „Folge dem Plan“, „KOPP Report“, тощо. Основні теми, які вони піднімають, є традиційними для російської дезінформації: наклепи на українських біженців, заклики до "примирення" з Росією, покладання відповідальності за війну на західні країни та підлив солідарності на підтримку України серед союзників.

Варто зазначити, що в інфопросторі існують десятки груп, які підтримують Росію та дії Володимира Путіна. Наприклад, дослідники „Reuters“ наводять приклад Telegram-каналу „Putin Fanclub“, який веде чоловік на ім'я В'ячеслав Зевальд з Баварії, прихильник "арійських теорій" і ультраправої партії "Альтернатива для Німеччини".

Кілька інших анонімних Telegram-каналів поширюють специфічні наративи не лише про війну, а й про українських біженців, часто використовуючи фейкові імена справжніх мейнстрімних німецьких ЗМІ. Дослідники з Інституту стратегічного діалогу наводять як приклад канал „Deutsche Wahrheit“, який, ймовірно, пов'язаний з великою прокремлівською операцією, що видає себе за легітимні ЗМІ та поширює дезінформацію на різних платформах, здебільшого зосереджуючись на темі біженців. Канал систематично поширював дезінформацію проти українських біженців і зображував їх як загрозу громадському здоров'ю, безпеці або німецьким сім'ям, неправдиво звинувачуючи їх у скоєнні злочинів, антисемітизмі та нацизмі. Частина постів була спеціально спрямована проти жінок і підлітків з України. Така активність може бути прирівняна до розпалювання ненависті, а в деяких випадках - до підбурювання до заколоту, зазначають дослідники. Німецькі ЗМІ регулярно повідомляють про арешти адміністраторів подібних каналів, що поширюють російську пропаганду [51; 82; 85].

Східноєвропейська історик і політолог — Сюзанна Шпан — представляє статтю 12 січня 2023 року: «Центральні комунікаційні стратегії російського керівництва». „Які наративи Росія поширює в Німеччині про війну в Україні? І які цілі він цим переслідує?“ [15].

Вже більше двох років, найважливішою темою в російських державних ЗМІ є «військова спецоперація», яку називають російсько-загарбницькою війною в Україні. Репортажі покликані легітимізувати війну та дискредитувати Україну як фашистську державу. Щоб успішно вести інформаційну війну, Росія звертається до аудиторії в Німеччині через різні ЗМІ: іноземні ЗМІ RT DE

(раніше Russia Today) і SNA (Інформаційне агентство Sputnik) звертаються до населення німецькою мовою.

Російські державні ЗМІ за кордоном служать рупором Кремля. Іноземний мовник „RT“ вважає себе «інформаційною зброєю», як заявила головний редактор RT Маргарита Симоньян в інтерв'ю новинному порталу „Lenta.ru“ - 7 березня 2013 року. Стратегія її за кордоном полягає у створенні альтернативної мейнстріму контргромадськості та вербуванні «борців із системою», яких Росія може використати як ресурс «у наступній інформаційній війні» [15].

Відколи вони почали працювати в Берліні в 2014 році, російські іноземні ЗМІ „RT“ і „Sputnik“ використовували кризи, щоб поставити під сумнів демократію в Німеччині та зобразити уряд як некомпетентний. Мета полягала в тому, щоб розпалити невдоволення користувачів перебільшеними кризовими сценаріями та спотвореннями, а також мобілізувати їх на протест.

Від початку повномасштабної війни у 2022 році має місце подібний підхід: метою є зламати опір уряду Німеччини агресії Росії у вигляді санкцій і поставок зброї, легітимізувати власну загарбницьку війну та поставити під сумнів солідарність з Україною.

Приклади шпигунства та поширення дезінформації. Стаття - 18 квітня 2024 р. В ній йдеться про двох чоловіків, яких затримали за підозрою в підготовці диверсії з боку Росії. „Арешти в Баварії“. У цій справі двох німецьких росіян заарештували в Байройті 17 квітня. Їх підозрюють у шпигунстві за військовими об'єктами та плануванні диверсій – можливо, щоб перервати німецьку військову підтримку України. Співробітника BND восени 2022 року звинуватили у передачі секретної інформації російській спецслужбі ФСБ. Кажуть, що за це він отримав чималі гроші [20].

У березні 2024 року російські ЗМІ опублікували запис розмови високопоставлених офіцерів Бундесверу, включно з командувачем ВПС США Інго Герхарцем. Під час відеоконференції обговорили можливі сценарії розміщення крилатої ракети TAURUS у разі її доставки в Україну. Справи

свідчать про новий вимір російського шпигунства в Німеччині. Журналіст „ARD“ - Міхаель Гьотшенберг, говорить про «нову якість», якщо звинувачення проти заарештованих у Баварії правдиві. Гетшенберг, який займається такими питаннями, як тероризм і внутрішня безпека, описує потенційну загрозу, яку створює така діяльність, як «кошмар для німецьких органів безпеки». Росія може спробувати «перенести війну з України в Німеччину».

Австрієць Ян Марсале, опинився в центрі ще однієї справи про ймовірне шпигунство. За даними ЗМІ, колишній член правління „Wirecard“ роками працював на російські спецслужби. Він перебував у бігах відтоді, як компанія збанкрутувала у 2020 році. Він перебуває у міжнародному розшуку за економічні злочини. Будучи членом правління групи „DAX“, Марсале мав тісні зв'язки з канцелярією та федеральним міністерством фінансів [86].

«Ви можете назвати це шедевром, якщо вам вдасться поставити когось так помітно, ймовірно, після багатьох років співпраці», — каже політолог Софія Гоффманн з Ерфуртського університету. Це говорить про те, що Росія спеціально намагається вплинути на німецькі компанії та установи. За словами політолога, шпигунство та діяльність спецслужб у Німеччині зросли після окупації Криму в 2014 році і знову після нападу на Україну в 2022 році. Після висилки російських дипломатів спецслужби реорганізували свою діяльність.

Росія хоче зібрати інформацію про військові об'єкти в Німеччині, щоб отримати уявлення про розташування, системи озброєння та діяльність. Ця інформація могла бути використана для підготовки диверсій. Метою могло бути переривання німецької військової підтримки України або навіть перенесення конфлікту між Росією та Україною в Німеччину.

Російська пропаганда часто спирається на відкриті листи, петиції та заклики до мирних переговорів між Україною та Росією, яким Захід нібито перешкоджає.

Лівий політик Сахра Вагенкнехт (Sahra Wagenknecht), часто використовує спотворені заяви Володимира Зеленського чи західних політиків, які зазвичай вириваються з контексту та поширюються російськими

пропагандистськими ЗМІ. Вагенкнехт неодноразово заявляла, що український президент виступає проти мирних переговорів, і публічно виступала за припинення всього експорту зброї в Україну, щоб підштовхнути її до столу переговорів. Її партія — Альянс Сахри Вагенкнехт — Розум і Справедливість (Bündnis Sahra Wagenknecht – Vernunft und Gerechtigkeit), заснована в січні 2024 року, вже має 6% по всій країні, що вказує на те, що вона може бути обрана до Бундестагу в 2025 році та до Європарламенту в червні 2024 року. Маніфест партії Вагенкнехт про європейські вибори відхиляє Вступ України до ЄС і підкреслює, що війна в Україні є кривавою проксі-війною між НАТО та Росією.

Після того, як канцлер Олаф Шольц публічно спростував поставку Україні ракет Taurus, російські ЗМІ опублікували прослуханий запис розмови німецьких військових офіцерів Webex. Серед інших тем у розмові йшлося про те, чи зможуть ракети «Таурус» технічно зруйнувати збудований Росією міст, що з'єднує материкову частину Росії з Кримським півостровом. Також обговорювали, чи зможе Україна впоратися з обстрілами без залучення Бундесверу, наприклад, до цільового програмування. Зрозуміло, що справа Taurus продемонструвала силу Кремля, показавши, що ФСБ може слухати німецьких генералів та їхню систему зв'язку. Залишається відкритим питання про те, де ще і наскільки глибоко ФСБ проводить такі операції стеження в Німеччині. Крім того, точно не випадково запис був опублікований через день після похорону Навального та викриття скандалу „Wirecard“. Однак головною метою цього витоку було переконатися, що ракети „Taurus“ не будуть відправлені в Україну.

Переважна більшість німців підтримує канцлера Шольца у його відмові від постачання крилатих ракет «Таурус» в Україну, і цю позицію він повторив наприкінці лютого. За результатами дослідження ARD „DeutschlandTrend“, 61% респондентів висловилися за те, щоб Німеччина не постачала Україні цю високоточну зброю. Лише 29% опитаних висловилися за постачання крилатих ракет. Найвищий рівень схвалення постачання «Таурусів» був серед

прихильників Партії зелених (Grünen) (53%), тоді як найвищий рівень несподобання - серед прихильників БСЗ (BSW) (85%).

Відсутність поставок зброї в Україну останнім часом має далекосяжні наслідки у війні, оскільки країна все частіше опиняється в стані оборони вздовж усієї лінії фронту. Причиною цього не в останню чергу є кричуща нестача боєприпасів в українській армії. З одного боку, республіканці в Конгресі США блокують подальшу допомогу, а з іншого - фактичні поставки від європейських союзників не відповідають обіцяним обсягам. На цьому фоні в Німеччині, і не лише в Бундестазі, знову активізувалися дискусії про постачання крилатих ракет. У цілому, підтримка більших поставок зброї Україні останнім часом зросла [81].

Таким чином Кремль не тільки створив, а й продовжує створювати атмосферу, в якій більшість німецького населення ще більше виступає проти доставки ракет „Taurus“ в Україну; згідно з останніми опитуваннями, 59% німців проти, і лише 34% - за. Крім того, справа Taurus призвела до того, що канцлер продовжувала категорично виключати поставку Taurus, незважаючи на зростання протилежних думок у правлячій коаліції та фракції ХДС-ХСС (CDU-CSU-Bundestagsfraktion).

Справа також посилює побоювання канцлера Шольца, що ракети можуть бути випущені по цілях у Росії без контролю Німеччини, і що таким чином Німеччина буде втягнута у війну. Цим він перш за все сигналізує про недовіру до своїх українських партнерів. І посіяти недовіру між Україною та Німеччиною, очевидно, є метою, якої прагне досягти російська пропаганда.

Справа „Taurus“ продемонструвала, як проросійські сили в Німеччині сприйняли російський наратив про те, що німецькі військові готуються до агресивної війни проти Росії. Сахра Вагенкнехт (BSW), Дітмар Барч (Linke) і Тіно Хрупалла (AfD), незважаючи на різні політичні платформи, із задоволенням сприйняли цей спіл, який виник у Москві з російських пропагандистських ЗМІ.

Аналітичний звіт «Інформаційний вплив РФ у Німеччині», поданий Центром протидії дезінформації в 2024 році. Центром було проаналізовано інформаційний простір ФРН.

Медіа, які поширюють російську пропаганду. Були виявлено, що російські наритиви просувають наступні медіа: „Berliner Zeitung“ та „Anti-spiegel.ru“. Мова йде не тільки про медіа, а й ще про газети, які випускає дане видавництво. Berliner Zeitung регулярно поширює кремлівські не тільки медіа, а й публікації інших російських медіа, а саме RT [31].

Наведено статтю від 23 січня 2024 року із заголовком «Україна: Медіаасоціація скаржиться на напади на журналістів» («Ukraine: Medienverband beklagt Angriffe auf Journalisten»), який йдеться про нібито відсутність свободи слова в Україні: «З 24 лютого 2022 року, коли Росія вторглася в Україну, журналістам, які критикують владу, стало складно» [16].

„The Washington Post“, опублікував російські документи, в яких зазначено те, що кремль організував масштабну дезінформаційну компанію не тільки в Україні, та й в Європі, з метою дискредитації керівництва України, дезорієнтації українців та деморалізації українського війська [14]. Ще проросійською від „Berliner Zeitung“ є стаття із заголовком «Мовчання США та НАТО щодо листів Росії від 17 грудня 2021 року» [«Das Schweigen von USA und NATO auf Russlands Briefe von 17. Dezember 2021»]. У матеріалі було надано інформацію про вигаданий росіянами наратив, що війна РФ проти України, була спровокована США та ЄС [18].

Також на німецьку аудиторію для поширення російських наративів діє медіа „Anti-spiegel.ru.“, очолюваний Томасом Рьюпером. 17 березня 2024 року Томас Рьюпер взяв інтерв'ю у Василя Прозорова, який є зрадником та колишнім співробітником СБУ. У інтерв'ю обговорювали так званий «незаконний обіг зброї в Україні» та «злочини українських військових» [36]. Особи, які здійснюють підривну діяльність на користь Росії. Томас Рьюпер (Thomas Röper), 26 листопада 1971 року народження, експерт з питань Східної Європи, обіймав керівні та наглядові посади у фінансових компаніях у Східній

Європі та Росії. Зараз він живе у своєму прийомному будинку в Санкт-Петербурзі. Він живе в Росії понад 15 років і вільно володіє російською мовою. Його медіа-критична робота зосереджена на (медійному) іміджі Росії в Німеччині, критиці репортажів західних ЗМІ загалом, а також на темах (гео-) політики та економіки. З 1992 року Рьюпер живе на теретирії Росії, очолює та веде блог „Anti-spiegel.ru“, який у свою чергу підтримується кремлем та зареєстрований у Росії. Він регулярно відвідує ТОТ України. Його бачили як «незалежного іноземного спостерігача» на псевдореферендумах, організовані РФ у вересні 2022 року. Крім того, він був «іноземним спостерігачем» на псевдовиборах президента РФ 2024 року, в особливості на ТОТ Запорізької області України. Також, Т. Рьюпер звинувачував українських військових у використанні цивільного населення як «живого щита», стверджував те, що більшість населення тимчасово окупованого міста Мелітополь висловлює підтримку російської «спеціальної воєнної операції» [3].

Кім Дотком (Kim Dotcom), народжений 21 січня 1974 року, місто Кіль, Німеччина. Він є підприємцем та блогером. Кім Дотком поширює антиукраїнські наративи та проросійські фейки, він звинувачує Україну у знищенні російськомовного населення на Донбасі, ставить сумнів суверенітет України. Він перекладає відповідальність за розпочату Росією війну проти України на США, просуває кремлівську тезу про програш України у цій війні. Також Кім Дотком виступає за нібито дипломатичне вирішення війни та просуває наратив про якусь готовність В. Путіна до мирних переговорів [71].

Аліна Ліпп ще один представник „шістірки“ Кремля, поширює російську пропаганду через свої канали. Однак санкції ЄС ускладнюють фінансування таких прихильників Путіна, як вона. Аліна Ліпп у своєму Telegram-каналі «Новини з Росії», один із найпоширеніших каналів російської пропаганди в Німеччині. На даний момент з у Ліпп понад 186 000 підписників, і кількість її підписників швидко зросла після початку російського вторгнення. У своєму каналі вона послідовно поширює російські наративи, наприклад, завжди

говорить про «спецвійськову операцію», а не про війну, а також про нібито «геноцид» російського населення на сході України [61].

Розслідування „Суабга“ викрило понад 1000 скоординованих фейкових профілів, багато з яких просували наративи, узгоджені з ультраправими ідеологіями, які були спрямовані проти центристських демократичних структур [27]. Ці зусилля були пов'язані як з внутрішніми екстремістськими мережами, так і з операціями іноземних розвідок, насамперед пов'язаних з Росією [65; 83]. Телеканал Sky News задокументував використання впливових осіб зі штучним інтелектом і сфабрикованих акаунтів, які суттєво вплинули на дискурс навколо федеральних виборів у Німеччині [83].

Кіберпростір став одним із ключових напрямів загроз для Німеччини. За даними Федерального відомства з інформаційної безпеки (BSI), протягом останніх років спостерігається постійне зростання кількості та складності кібератак, спрямованих проти державних установ, закладів охорони здоров'я та об'єктів критичної інфраструктури. Особливу увагу у звіті приділено використанню штучного інтелекту та автоматизованих інструментів, які дедалі частіше застосовуються для підготовки, проведення та адаптації кібератак до конкретних цілей. Це дозволяє зловмисникам швидше реагувати на захисні заходи та підвищує ефективність атак. У результаті виявлення та нейтралізація кіберзагроз стають більш складними завданнями для німецьких органів безпеки та відповідальних державних інституцій [38].

Вразливість кібербезпеки Німеччини стала особливо помітною під час федеральних виборів 2025 року, коли зафіксовано кібератаки із застосуванням штучного інтелекту, спрямовані на компрометацію баз даних виборців та виборчого програмного забезпечення [65]. Ці інциденти продемонстрували здатність сучасних ШІ-інструментів імітувати поведінку легітимних користувачів, обходити системи захисту та поширювати поліморфне шкідливе програмне забезпечення, яке складно виявити традиційними засобами кіберзахисту [87]. У відповідь на зростання таких загроз Федеральне відомство з інформаційної безпеки (BSI) у своїй стратегії наголосило на необхідності

модернізації національної системи кібербезпеки. Зокрема, було запропоновано посилити координацію між державними установами, децентралізувати механізми реагування на інциденти та розширити обмін розвідувальною інформацією про кіберзагрози між різними секторами [39]. Зростаюча складність кіберзагроз свідчить про необхідність комплексного підходу до кіберзахисту, який передбачає тісну співпрацю державних органів, приватного сектору та партнерів з Європейського Союзу.

Додатковим свідченням зростання кіберзагроз для Німеччини стали DDoS-атаки на федеральні веб-сайти, зафіксовані під час важливих політичних подій. Як зазначає Plaß (2022), такі атаки тимчасово виводили з ладу урядові онлайн-ресурси, ускладнюючи комунікацію між державними органами та громадянами [77]. Подібні дії мають не лише технічний, а й політичний ефект, оскільки формують уявлення про неспроможність держави забезпечити стабільне функціонування своїх цифрових сервісів та сприяють поширенню дезінформаційних наративів щодо її вразливості.

Водночас розвиток цифрових технологій сприяв комерціалізації кіберзлочинної діяльності. Зростаюча цифровізація економіки Німеччини створила нові можливості для хакерських угруповань та кіберзлочинних мереж, які пропонують широкий спектр послуг — від викрадення конфіденційних даних до проведення атак із використанням програм-вимагачів [23; 89]. Особливу небезпеку становить той факт, що діяльність таких суб'єктів нерідко перетинається з інтересами окремих держав, що ускладнює розмежування між організованою кіберзлочинністю та інструментами геополітичного впливу.

Серйозною проблемою для кібербезпеки Німеччини залишаються тривалі та цілеспрямовані кібершпигунські операції. Про це свідчать численні кібератаки на Бундестаг та установи сектору охорони здоров'я, відповідальність за які часто покладають на групи типу Advanced Persistent Threat (APT) [40; 50]. Особливістю таких атак є їхня довготривалість, високий рівень підготовки та спрямованість на отримання конфіденційної інформації,

що становить загрозу для державної безпеки та функціонування критично важливих інституцій.

Водночас сучасні кіберзагрози дедалі частіше виходять за межі традиційного шпигунства та набувають економічного виміру. У «Кіберпрогнозі до 2025 року» наголошується, що кібератаки можуть стати інструментом економічної війни, спрямованим на порушення ланцюгів поставок, викрадення комерційної інформації та послаблення конкурентоспроможності підприємств [87]. У таких умовах кібербезпека перетворюється не лише на питання захисту інформаційних систем, а й на важливий елемент забезпечення економічної стійкості та національної безпеки Німеччини.

„СВР замість Пригожина“. Після того як Служба зовнішньої розвідки РФ (СВР) повністю перебрала на себе активи колишньої ПВК «Вагнер», структура управління дезінформацією стала суворо вертикальною [17]. Це ліквідувало колишню конкуренцію між різними російськими відомствами і дозволило проводити масштабніші операції.

Екосистема сьогодні складається з 3 рівнів:

- Аналітичний центр „Кремль + СВР“: Моніторить німецьке медіаполе, виявляє «гарячі» теми (наприклад, дебати про міграцію, вибори до Бундестагу, постачання зброї чи економічні проблеми) [17; 90].
- Технічне ядро „Storm-1516 + R-FBI“: Спеціалізовані кіберпідрозділи, які пишуть алгоритми для ботів, створюють ШІ-шаблони та координують операції «двійників» (Doppelgänger) [54; 64].
- Мережа дистрибуції: Тисячі ШІ-аккаунтів у соцмережі X, Telegram-канали, TikTok-інфлюенсери та фейкові копії німецьких новинних сайтів [54; 90].

Технологічний прорив: як ШІ та LLM змінили правила гри. Раніше російську «фабрику тролів» було легко викрити: найняті оператори в Санкт-Петербурзі робили граматичні помилки, не розуміли німецького сленгу, культурного контексту або локальних політичних нюансів Баварії чи Саксонії.

Інтеграція великих мовних моделей (LLM) повністю вирішила ці проблеми [90]:

- Гіпер-персоналізація (Microtargeting): ШІ аналізує профілі реальних німецьких користувачів у соцмережі X і автоматично підбирає аргументи, які здатні зачепити саме їх [54].

Консервативному виборцю ШІ згенерує пост про «загрозу міграції та крах традиційних цінностей», а лівому пацифісту — про «небезпеку ескалації з РФ та ядерну війну» [54; 90].

Подолання лінгвістичного бар'єра: LLM пишуть тексти бездоганною німецькою мовою, використовуючи природні мовленнєві звороти, іронію та специфічні політичні терміни, притаманні німецькому дискурсу [90].

Ефект «Ехо-камери» (Echo Chambers): Один оператор СВР за допомогою штучного інтелекту може керувати мережею з тисяч ботів, які ведуть дискусії між собою під постами німецьких політиків [54]. Вони створюють ілюзію, що нібито «весь німецький народ» виступає проти підтримки України чи уряду в Берліні [64; 90].

Операційні кейси: Storm-1516 та кампанія 2025–2026 років. Під час підготовки та проведення виборів у Німеччині угруповання Storm-1516 та R-FBI продемонстрували нові типи атак [64]:

- Кампанія "R-FBI" (Російське ФБР): Ця операція була спрямована на імітацію «офіційних розслідувань» [64]. За допомогою ШІ фабрикувалися нібито секретні документи німецьких спецслужб (BfV або BND), аудіозаписи «прослушки» політиків та підроблені звіти про корупцію всередині німецького уряду. Оскільки тексти виглядали як офіційні релізи, їх підхоплювали альтернативні німецькі медіа та опозиційні політики [64; 90]

Масове клонування медіа за допомогою ШІ: Замість ручного створення фейкових сайтів, автоматизовані скрипти миттєво генерували тисячі дзеркал провідних видань („Der Spiegel“, „Bild“, „DW“). ШІ наповнював ці дзеркала реальними німецькими новинами, але додавав туди 10–15% вигаданих або

маніпулятивних статей, які дискредитували вибори або висміювали допомогу Україні [54; 90].

Штучний хаос в соцмережі X: Бот-армії Путіна діяли за принципом «насичення» [11]. Коли у Німеччині відбувалася важлива політична подія (наприклад, теледебати), ШП-боти за лічені хвилини випускали десятки тисяч постів із певними хештегами, повністю викривляючи алгоритми трендів платформи X і змушуючи реальних користувачів бачити прокремлівські інтерпретації подій [54; 64].

РОЗДІЛ 4.

СТРАТЕГІЇ ПРОТИДІЇ ІНФОРМАЦІЙНОГО ВПЛИВУ

Після початку повномасштабного вторгнення Росії в Україну у 2022 році, Німеччина суттєво посилила інституційні механізми протидії дезінформації та зовнішньому інформаційному впливу. Важливу роль у цьому процесі відіграє Федеральне міністерство закордонних справ, діяльність якого зосереджена на виявленні та аналізі випадків іноземного інформаційного маніпулювання та втручання (FIMI). Водночас Федеральне міністерство внутрішніх справ координує міжвідомчу співпрацю у сфері виявлення та нейтралізації гібридних загроз, включаючи дезінформаційні кампанії [10].

Особлива увага приділяється моніторингу інформаційного простору в контексті російської агресії проти України. Федеральне міністерство закордонних справ, Федеральне управління преси та інформації (BPA), Міністерство внутрішніх справ і підпорядковані йому структури здійснюють постійний аналіз поширення неправдивої та маніпулятивної інформації, забезпечуючи оперативний обмін даними між федеральними та земельними органами влади [10]. Така координація дозволяє своєчасно виявляти дезінформаційні кампанії та формувати узгоджену державну відповідь.

Водночас німецький підхід до протидії дезінформації не обмежується лише спростуванням неправдивих повідомлень. Пріоритетним напрямом державної політики є зміцнення суспільної стійкості до інформаційних загроз шляхом розвитку медіаграмотності та критичного мислення громадян. У цьому контексті особливого значення набуває інформування населення про механізми дезінформації та підтримка здатності критично оцінювати інформацію, особливо в соціальних мережах. Такий підхід спрямований не лише на реагування на інформаційні атаки, а й на формування довгострокової

стійкості демократичного суспільства до зовнішніх маніпулятивних впливів [10].

Важливим елементом німецької стратегії протидії дезінформації є розвиток медіаграмотності та підтримка незалежного інформаційного середовища. Федеральний уряд розглядає підвищення рівня новинної грамотності як один із ключових інструментів зміцнення суспільної стійкості до маніпулятивного впливу. У зв'язку з цим реалізуються численні освітні та інформаційні проєкти, спрямовані на різні вікові та соціальні групи населення. Особлива увага приділяється підтримці незалежної журналістики та фактчекінгових ініціатив, які відіграють важливу роль у виявленні та спростуванні неправдивої інформації. Водночас федеральний уряд визнає важливість діяльності незалежних дослідницьких центрів та неурядових організацій, що здійснюють перевірку фактів і аналіз інформаційних загроз [8; 28].

Практична реалізація цих заходів здійснюється, зокрема, через діяльність Федерального міністерства внутрішніх справ. Серед інструментів протидії дезінформації використовуються інформаційні ресурси федерального уряду, регулярні пресбрифінги та взаємодія з парламентом щодо актуальних інформаційних загроз. Важливим кроком стало представлення у 2024 році стратегії боротьби з правим екстремізмом, яка передбачає створення спеціального механізму раннього виявлення іноземних дезінформаційних кампаній [9].

Німецький підхід ґрунтується не лише на національних заходах, а й на широкій міжнародній співпраці. Протидія інформаційним загрозам здійснюється в межах європейських та міжнародних форматів, зокрема через Робочу групу ради ЄС з питань гібридних загроз і механізм G7 Rapid Response Mechanism. Важливу роль також відіграє координація між федеральним урядом, урядами земель, муніципалітетами та органами безпеки. Така багаторівнева взаємодія забезпечує узгоджене реагування на дезінформаційні

кампанії та сприяє формуванню цілісної системи захисту інформаційного простору Німеччини.

Важливу роль у протидії дезінформації відіграють і оператори соціальних мереж, оскільки саме цифрові платформи є основним каналом поширення маніпулятивного контенту та інформаційних операцій. У зв'язку з цим німецький уряд наголошує на необхідності забезпечення прозорих правил функціонування соціальних мереж та їхнього послідовного застосування з боку платформ. Регулярна взаємодія державних органів із представниками цифрових платформ розглядається як важливий інструмент для виявлення та обмеження поширення неправдивої або оманливої інформації [8; 28].

Посилення міжнародної координації також стало одним із ключових напрямів протидії російському інформаційному впливу. У лютому 2024 року міністри закордонних справ Німеччини, Франції та Польщі домовилися про створення спільного механізму раннього попередження для виявлення та нейтралізації діяльності російських ботів і тролів у цифровому просторі [4]. Така ініціатива стала відповіддю на очікуване зростання дезінформаційних кампаній напередодні виборів до Європейського парламенту, коли інформаційні операції можуть використовуватися для впливу на громадську думку та політичні процеси в країнах Європейського Союзу.

Важливим показником ефективності заходів протидії є зростання суспільної обізнаності щодо інформаційних загроз. Після початку повномасштабної російської агресії проти України проблема дезінформації набула значно більшої уваги з боку державних інституцій та громадянського суспільства Німеччини. За даними березня 2024 року, переважна більшість громадян країни розглядає спроби Росії впливати на німецьку політику через дезінформацію та розвідувальну діяльність як серйозну загрозу. Це свідчить про зростання суспільної стійкості до зовнішнього інформаційного впливу та усвідомлення ризиків, пов'язаних із сучасними інформаційними операціями [4].

Важливим напрямом протидії дезінформації в Німеччині є розвиток медіаграмотності та підготовка громадян до розпізнавання маніпулятивного контенту. У зв'язку з цим дедалі більше уваги приділяється освітнім програмам у школах та університетах, спрямованим на формування критичного мислення та навичок аналізу інформації. Особливе значення має підхід Prebunking, який передбачає завчасне інформування громадян про механізми дезінформації та методи інформаційного впливу [49]. На відміну від традиційного спростування неправдивої інформації після її поширення, Prebunking дозволяє підвищити стійкість аудиторії до маніпуляцій ще до контакту з дезінформаційним контентом, що робить його одним із найбільш ефективних інструментів профілактики інформаційних загроз.

Попри реалізацію численних заходів, дослідники наголошують на необхідності подальшого посилення політичної та суспільної уваги до проблеми російської дезінформації. Важливим завданням залишається інформування громадян про механізми російського інформаційного впливу та його наслідки для європейської безпеки. Особливо актуальним це питання стало напередодні федеральних виборів 2025 року, коли інформаційні кампанії навколо військової підтримки України та постачання ракет Taurus продемонстрували значний вплив на суспільні дискусії та політичні рішення. Це свідчить про те, що німецьке суспільство, як і інші європейські країни, залишається вразливим до зовнішніх інформаційних маніпуляцій.

Відповіддю Німеччини на нові виклики стала модернізація системи цифрової безпеки. Держава реалізує комплекс заходів, що поєднують законодавчі зміни, удосконалення механізмів реагування та розширення міжнародної співпраці у сфері кібербезпеки. Зокрема, було посилено повноваження та ресурсне забезпечення ключових інституцій, таких як Федеральне відомство з інформаційної безпеки (BSI) та Федеральне відомство кримінальної поліції (ВКА), що має сприяти підвищенню кіберстійкості країни в умовах зростання гібридних загроз [89].

Участь країни в Будапештській конвенції створює правову основу для транскордонної взаємодії правоохоронних органів та сприяє координації зусиль у розслідуванні кіберзлочинів, які дедалі частіше мають транснаціональний характер [23]. З метою підвищення ефективності реагування на кіберінциденти в Німеччині також було створено Національний центр кібернетичного реагування, який забезпечує координацію між цивільними, військовими та розвідувальними структурами під час виявлення та нейтралізації кіберзагроз [39].

Водночас важливе місце в системі кіберзахисту посідають освітні та кадрові заходи. Німеччина активно інвестує у підготовку фахівців з кібербезпеки та реалізує програми підвищення обізнаності населення щодо цифрових ризиків, оскільки людський фактор залишається однією з найпоширеніших причин успішних кібератак [38; 39]. До таких ініціатив належать програми кібергігієни, сертифікація кібербезпеки для малого та середнього бізнесу, а також підтримка освітніх програм і стипендій у сфері кібербезпеки.

Окрім розвитку людського потенціалу, Німеччина посилює технологічні можливості протидії кіберзагрозам. Особлива увага приділяється впровадженню систем виявлення загроз на основі штучного інтелекту, інструментів поведінкової аналітики та архітектури нульової довіри (Zero Trust), які дозволяють оперативно виявляти підозрілу активність у мережах та локалізувати потенційно скомпрометовані системи [39; 87]. Використання таких технологій підвищує здатність державних і приватних структур реагувати на складні кіберзагрози в режимі реального часу та зміцнює загальну кіберстійкість країни.

Напрямом сучасної політики безпеки Німеччини стала протидія дезінформації та інформаційним маніпуляціям у цифровому середовищі. Для цього державні органи активно співпрацюють із організаціями громадянського суспільства, медійними наглядовими структурами та технологічними компаніями з метою виявлення, моніторингу та спростування

дезінформаційних наративів [27; 37; 83]. Особливого значення така взаємодія набула під час федеральних виборів 2025 року, коли уряд координував свої дії з великими цифровими платформами для посилення прозорості інформаційного простору та оперативного реагування на маніпулятивний контент [27; 37].

Разом з тим, Німеччина приділяє значну увагу міжнародному співробітництву у сфері кібербезпеки. Федеральне міністерство внутрішніх справ наголошує на необхідності узгодження стандартів кіберзахисту та кризового реагування на рівні Європейського Союзу. У цьому контексті Німеччина підтримала розвиток механізмів європейської кіберсолідарності, які передбачають взаємодопомогу держав-членів у випадку масштабних транскордонних кібератак [37]. Такий підхід відображає усвідомлення того, що сучасні кіберзагрози виходять за межі національних кордонів і потребують колективних механізмів реагування.

Новинкою було те що, стало включення показників кіберстійкості до системи оцінки національних загроз. Ці індикатори, що публікуються у щорічних звітах BSI, дозволяють оцінювати рівень готовності держави до кіберінцидентів та більш ефективно розподіляти ресурси для зміцнення безпеки [38]. Водночас німецький підхід дедалі більше враховує психологічний вимір інформаційних і кіберзагроз. Усвідомлюючи, що метою багатьох атак є поширення страху, невизначеності та суспільної дезорієнтації, державна політика акцентує увагу на зміцненні громадської довіри, прозорій комунікації та підтриманні суспільної згуртованості як важливих складових національної стійкості [7; 37; 38].

Формування здатності перевіряти джерела та оцінювати достовірність повідомлень зменшує ефективність дезінформаційних кампаній і підвищує стійкість суспільства до маніпулятивного впливу [41]. У цьому контексті особливого значення набуває підтримка незалежних засобів масової інформації та фактчекінгових організацій, які сприяють оперативному виявленню та спростуванню неправдивих повідомлень. Їхня діяльність не

лише обмежує поширення дезінформації, а й підвищує якість суспільної дискусії шляхом забезпечення доступу до перевіреної та достовірної інформації [41].

Не менш важливим напрямом протидії є міжвідомча та міжнародна координація. Оскільки російські інформаційні операції мають транскордонний характер і використовують глобальні цифрові платформи для поширення свого впливу, ефективна протидія потребує узгоджених дій на національному та міжнародному рівнях. У зв'язку з цим важливого значення набуває співпраця між державними інституціями, громадянським суспільством, технологічними компаніями та міжнародними партнерами, зокрема в межах Європейського Союзу та НАТО. Така взаємодія дозволяє оперативно обмінюватися інформацією про нові загрози, координувати заходи реагування та підвищувати загальну стійкість інформаційного простору до зовнішніх маніпуляцій. Своєчасне виявлення скоординованих кампаній впливу дає змогу обмежити їхнє поширення на ранніх етапах та мінімізувати їхній вплив на громадську думку і політичні процеси [42].

ВИСНОВКИ

Підсумовуючи усе вище зазначене, можемо зробити висновок про те, що російські інформаційні впливові операції в Німеччині є складовою ширшої стратегії гібридного протистояння Російської Федерації із західними демократичними державами. На сучасному етапі інформаційний простір став одним із ключових театрів геополітичної боротьби, де інформація використовується як інструмент впливу на суспільну свідомість, політичні процеси та систему прийняття рішень. Проведений аналіз підтверджує, що російська пропаганда в Німеччині має системний, довготривалий та адаптивний характер, поєднуючи традиційні пропагандистські методи із сучасними цифровими технологіями.

У процесі дослідження було встановлено, що інформаційна війна являє собою комплексний феномен, який охоплює психологічні, політичні, медійні, кібернетичні та технологічні інструменти впливу. На відміну від традиційних форм конфлікту, її головною метою є не фізичне знищення противника, а формування вигідного інформаційного середовища, послаблення суспільної стійкості та підриг довіри до державних інституцій. Таким чином, інформаційні операції виступають важливим елементом сучасних гібридних загроз та дедалі частіше використовуються як інструмент досягнення зовнішньополітичних цілей.

Аналіз стратегічних наративів російської пропаганди дозволив виявити найбільш поширені тематичні конструкції, адаптовані до німецькомовної аудиторії. До них належать наративи про втрату Німеччиною суверенітету, «економічне самогубство» через санкційну політику, загрозу Третьої світової війни, дискредитацію України та українських біженців, «русофобію», «занепад Заходу», а також твердження про те, що Захід нібито веде війну проти Росії. Встановлено, що всі зазначені наративи мають спільну стратегічну мету

— посилення соціальної поляризації, зниження рівня довіри до політичного керівництва Німеччини, послаблення підтримки України та підрив євроатлантичної єдності.

Важливим результатом дослідження стало визначення особливостей екосистеми поширення російської пропаганди в Німеччині. З'ясовано, що сучасні інформаційні кампанії функціонують не через окремі інформаційні ресурси, а через розгалужену мережу взаємопов'язаних платформ, до якої входять альтернативні медіа, соціальні мережі, Telegram-канали, блогери, політичні активісти та окремі радикальні політичні сили. Особливу роль у поширенні дезінформації відіграють цифрові платформи, алгоритми рекомендацій контенту та механізми вірусного поширення інформації, які дозволяють швидко охоплювати великі аудиторії та створювати ілюзію суспільного консенсусу.

Окрему увагу було приділено використанню технологій штучного інтелекту та великих мовних моделей. Дослідження показало, що AI та LLM створюють нові можливості для автоматизації інформаційних операцій, персоналізації повідомлень та масштабування дезінформаційних кампаній. Водночас використання таких технологій ускладнює процес виявлення маніпулятивного контенту та створює нові виклики для системи інформаційної безпеки демократичних держав. Таким чином, технологічний розвиток суттєво змінює характер сучасної пропаганди та потребує відповідного оновлення механізмів протидії.

Практичне значення дослідження полягає в тому, що його результати можуть бути використані під час розробки державних програм протидії дезінформації, удосконалення стратегічних комунікацій, підготовки фахівців з інформаційної безпеки та формування політики цифрової стійкості. Отримані висновки також можуть бути корисними для державних установ, аналітичних центрів та громадських організацій, які займаються моніторингом інформаційних загроз.

Разом із цим проведене дослідження дозволило виявити низку проблем. Насамперед це високий рівень адаптивності російських інформаційних кампаній, швидка трансформація наративів відповідно до актуального політичного порядку денного, а також недостатня готовність суспільства до розпізнавання складних форм цифрових маніпуляцій. Важливою проблемою залишається і зростання ролі генеративного штучного інтелекту, який здатний значно підвищувати ефективність дезінформаційних операцій.

З огляду на це доцільно рекомендувати подальше посилення медіаграмотності населення, розвиток механізмів верифікації цифрового контенту, удосконалення співпраці між державними структурами, академічним середовищем та технологічними компаніями, а також розширення міжнародної координації у сфері протидії інформаційним загрозам. Особливого значення набувають створення інструментів виявлення AI-генерованої дезінформації та розвиток систем раннього попередження інформаційних атак.

Таким чином, головним результатом нашого дослідження є підтвердження того, що російські стратегічні наративи та сучасні технології пропаганди становлять реальну загрозу інформаційній безпеці Німеччини та стабільності демократичних інститутів. Водночас ефективна протидія таким впливам можлива за умови поєднання технологічних, політичних, правових та освітніх механізмів. Перспективним напрямом подальших наукових досліджень є більш детальне вивчення використання генеративного штучного інтелекту в інформаційних операціях, а також порівняльний аналіз російських кампаній впливу в різних країнах Європейського Союзу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. С. С. Троян. Спеціальні інформаційні операції. ВУЕ. (2023) Режим доступу до ресурсу: https://vue.gov.ua/Спеціальні_інформаційні_операції (дата звернення: 15.02.2026).
2. Ткаченко Максим. Інформаційна війна. ВУЕ. (2023) Режим доступу до ресурсу: https://vue.gov.ua/Інформаційна_війна (дата звернення: 15.02.2026)
3. Центр протидії дезінформації. Головна сторінка. (2024). Аналітичний звіт «Інформаційний вплив РФ у Німеччині» Режим доступу до ресурсу: <https://cpd.gov.ua/reports/analitychnyj-zvitinformacijnyj-vplyv-rf-u-nimechchyni/?fbclid> (дата звернення: 04.04.2026).
4. Auswärtiges Amt. Ideenschmiede und Impulsgeber für Europa: Außenministerin Baerbock beim Weimarer Dreieck. URL: <https://www.auswaertiges-amt.de/de/aussenpolitik/europa/zusammenarbeit-staaten/weimarer-dreieck/2643220> (date of access: 10.03.2026).
5. Ajir, M., & Vailliant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, 12(3), 70–89. URL: <http://www.jstor.org/stable/26481910> (date of access: 10.02.2026).
6. Apolut.net. Du hast nach ukraine gesucht. URL: <https://apolut.net/?s=ukraine> (date of access: 08.03.2026).
7. BMI - Bundesministerium des Innern und für Heimat (n.d.-a). Disinformation as a hybrid threat. URL: <https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/article-disinformation-hybrid-threat.html?nn=9388812> (date of access: 09.03.2026).
8. Bundesministerium des Innern und für Heimat. Maßnahmen der Bundesregierung gegen Desinformation. Bundesministerium des Innern und für Heimat. (2024). URL:

<https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation/massnahmen-der-bundesregierung.html> (date of access: 08.03.2026).

9. Bundesministerium des Innern und für Heimat. Desinformation zu Russlands Angriffskrieg gegen die Ukraine. Bundesministerium des Innern und für Heimat. (2024). URL: <https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation/desinformation-russlands-angriffskrieg.html> (date of access: 09.03.2026).
10. Bundesministerium des Innern und für Heimat. Maßnahmen gegen Rechtsextremismus. Bundesministerium des Innern und für Heimat. (2024) URL: <https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/gegen-rechtsextremismus/artikel-massnahmen-gegen-rex.html;jsessionid=A4D4A7F5408E21416B7F95086BD42D04.live862> (date of access: 16.03.2026).
11. Bundesregierung. Die Bundesregierung informiert. Was ist FIMI 2023? URL: <https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/fimi-fake-news-international-2227610> (date of access: 07.03.2026).
12. Bundesministerium der Verteidigung. (2016). Desinformation als Mittel der hybriden Kriegsführung. URL: <https://www.bmvg.de/de/themen/dossiers/weissbuch/gedanken/desinformation-als-mittel-der-hybriden-kriegsfuehrung-12286> (date of access: 11.03.2026).
13. Belton C., Mekhennet S., Harris S. Kremlin tries to build antiwar coalition in Germany, documents show. Washington Post. (2023). URL: <https://www.washingtonpost.com/world/2023/04/21/germany-russia-interference-afd-wagenknecht/> (date of access: 11.03.2026).
14. Belton C. Kremlin runs covert disinformation campaign to undermine Zelensky, documents show. Washington Post. (2024). URL:

<https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/> (date of access: 15.03.2026).

15. Bundeszentrale für politische Bildung. Nachrichten aus dem Kreml. bpb.de. (2023). URL: <https://www.bpb.de/themen/medien-journalismus/digitale-desinformation/517057/nachrichten-aus-dem-kreml/> (date of access: 14.03.2026).
16. Becchi F. Ukraine: Medienverband beklagt Angriffe auf Journalisten. Berliner Zeitung. URL: <https://www.berliner-zeitung.de/politik-gesellschaft/journalisten-in-der-ukraine-gefoltert-erpresst-gestorben-li.2179436> (date of access: 09.05.2026).
17. Berkane, L. (May 5, 2026). Sixty Russian agents identified: Prigozhin's influence network taken over by the Foreign Intelligence Service. Forbidden Stories. <https://forbiddenstories.org/russian-agents-prigozhins-influence-network-taken-over-by-the-intelligence-service/> (date of access: 10.05.2026).
18. Berliner Zeitung. (2023). Das Schweigen von USA und Nato auf Russlands Briefe vor dem Ukraine-Krieg. URL: <https://www.berliner-zeitung.de/open-source/das-schweigen-von-usa-und-nato-auf-russlands-briefe-vom-17-dezember-2021-li.2168703> (date of access: 07.04.2026).
19. Blannin, P. (2021). Modelling Information Warfare: Visualising Definitions, Fundamental Characteristics, and Foundational Theories of Contemporary Information Warfare. *Journal of Information Warfare*, 20(3), 90–107. URL: <https://www.jstor.org/stable/27125001> (date of access: 01.04.2026).
20. BR24. (2024) Zwei Männer in Bayern wegen Spionage für Russland festgenommen. URL: <https://www.br.de/nachrichten/bayern/zwei-maenner-in-bayern-wegen-spionage-fuer-russland-festgenommen,UAHE1Sv> (date of access: 02.04.2026).
21. COMPACT. (2023). Die Putin-Doktrin. URL: <https://www.compact-online.de/die-putin-doktrin/> (date of access: 04.03.2026).

22. COMPACT. (2023). Jetzt diskutiert die NATO die Ukraine-Teilung. URL: <https://www.compact-online.de/jetzt-diskutiert-die-nato-die-ukraine-teilung/> (date of access: 03.03.2026).
23. Council of Europe. Octopus Cybercrime Community. (n.d.-k). Germany. URL: <https://www.coe.int/en/web/octopus/-/germany> (date of access: 03.05.2026).
24. Connolly K. Sahra Wagenknecht: heroine of German left could become ally of far right. the Guardian. (2022) URL: <https://www.theguardian.com/world/2022/dec/29/sahra-wagenknecht-german-left-die-linke-breakaway-far-right-afd> (date of access: 01.05.2026).
25. Cyberwar - Eine Begriffsgeschichte über die Disziplinen hinweg. Texter gesucht? Lass-andere-schreiben.de - Marktplatz für Schreibarbeiten. (1992). – C. 23-55 - URL: <https://www.rand.org/pubs/reprints/RP223.html> (date of access: 06.04.2026).
26. Cyberwar - Eine Begriffsgeschichte über die Disziplinen hinweg. Texter gesucht? Lass-andere-schreiben.de - Marktplatz für Schreibarbeiten. (2015). URL: <https://www.lass-andere-schreiben.de/referenzen-unserer-experten/cyberwar-eine-begriffsgeschichte-ueber-die-disziplinen-hinweg> (date of access: 06.04.2026).
27. Cyabra. (Feb. 20, 2025). 1,000+ fake accounts disrupting German elections. URL: <https://cyabra.com/blog/1000-fake-accounts-disrupting-german-elections/> (date of access: 22.03.2026).
28. Die Nachrichten. (2022). Asow-Regiment, Stepan Bandera & Co - Rechtsextremisten in der Ukraine und ihr Einfluss im Land. URL: <https://www.deutschlandfunk.de/asow-regiment-stepan-bandera-ukraine-100.html> (date of access: 14.03.2026).
29. Delcker J. Deutschland wappnet sich gegen russische Einflussnahme – DW – 28.03.2024. URL: <https://www.dw.com/de/hybride-kriegsführung-deutschland-wappnet-sich-gegen-russische-einflussnahme/a-68677715> (date of access: 08.03.2026).

30. Dmitry Gorenburg. Russian Strategic Messaging: Propaganda and Disinformation Efforts. Chapter 15. URL: <https://www.marshallcenter.org/de/media/4777/download> (date of access: 03.04.2026).
31. Deutschlandfunk. (2024). Wie Russland in Deutschland spioniert. URL: <https://www.deutschlandfunk.de/spionage-russland-deutschland-sabotage-100.html#spionagefaelle> (date of access: 10.03.2026).
32. EBSCO. (n.d.). Agenda-setting theory: Communication and mass media: Research starters: EBSCO research. URL: <https://www.ebsco.com/research-starters/communication-and-mass-media/agenda-setting-theory> (date of access: 20.03.2026).
33. Elina Treyger, Heather J. Williams, Anthony D'Arrigo. (May 23, 2025). Measuring the reach of Russia's propaganda in the Russia-Ukraine war | Rand. URL: https://www.rand.org/pubs/research_briefs/RBA3450-2.html (date of access: 02.05.2026).
34. Friedrich-Naumann-Stiftung. (2021). Hackangriff Russland: Information als Waffe. URL: <https://www.freiheit.org/de/information-als-waffe> (date of access: 05.04.2026).
35. Framing theory. In Heath R L, ed. Encyclopedia of Public Relations. Vol. 2. Thousand Oaks, CA: SAGE Publications, Inc.; 2013: 361-363. url. doi:10.4135/9781452276236.n202 (date of access: 24.02.2026).
36. Fundierte Medienkritik – Thomas Röper. (2024) Interview mit einem übergelaufenen Agenten des ukrainischen Geheimdienstes – Anti-Spiegel. URL: <https://anti-spiegel.ru/2024/interview-mit-einem-uebergelaufenen-agenten-des-ukrainischen-geheimdienstes/> (date of access: 25.03.2026).
37. Federal Ministry of the Interior and Community. (March 28, 2024). Protecting the European elections from hybrid threats, including disinformation. URL: <https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/european-election2024.html> (date of access: 23.03.2026).

38. Federal Office for Information Security. (November 25, 2024). The state of IT security in Germany 2024. URL: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2024.html?nn=1021082> (date of access: 23.03.2026).
39. Federal Office for Information Security. (July 27, 2022). Cybersecurity strategy for Germany. URL: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Strategie/strategie_node.html (date of access: 23.03.2026).
40. Gerling, Rainer W. Hackerangriff auf die Wahlfreiheit. Wissenschaftsmagazin der Max Planck Forschung. Ausgabe 1/2017. URL: https://www.mpg.de/11248402/MPF_2017_1.pdf (date of access: 28.03.2026).
41. GEOPolitics. WI, devops. (September 3, 2025). Impact of Russian disinformation in Germany. URL: <https://politicsgeo.com/impact-of-russian-disinformation-in-germany/> (date of access: 29.03.2026).
42. German Marshall Fund of the United States. BOKŠA, M. (2019). Russian Information Warfare In Central And Eastern Europe: Strategies, Impact, Countermeasures. URL: <http://www.jstor.org/stable/resrep21238> (date of access: 29.03.2026).
43. Hutchinson, W., & Warren, M. (2001). Principles of Information Warfare. Journal of Information Warfare, 1(1), 1–6. URL: <https://www.jstor.org/stable/26485918> (date of access: 26.02.2026).
44. ISD. (2022). Deutsche Wahrheit: a pro-Kremlin effort to spread disinformation about Ukrainian refugees. URL: https://www.isdglobal.org/digital_dispatches/deutsche-wahrheit-a-pro-kremlin-effort-to-spread-disinformation-about-ukrainian-refugees/ (date of access: 07.04.2026).
45. Jüdische Allgemeine. Gensing P. Putins treue Garde. (2022). [Електронний ресурс] – Режим доступу до ресурсу: <https://www.juedische-allgemeine.de/politik/putins-treue-garde/> (date of access: 05.04.2026).

46. Johnnie Manzaria & Jonathon Bruck. War & Peace: Media and War. Media's use of propaganda to persuade people's attitudes, beliefs, and behaviors. (n.d.). URL:
https://web.stanford.edu/class/e297c/war_peace/media/hpropaganda.html
 (date of access: 14.04.2026).
47. Konrad-Adenauer-Stiftung. (n.d.). Russische Desinformation: Der unsichtbare krieg gegen die Wahrheit - die politische Meinung. URL:
<https://www.kas.de/de/web/die-politische-meinung/blog/detail/-/content/russische-desinformation-der-unsichtbare-krieg-um-die-wahrheit>
 (date of access: 22.03.2026).
48. Konrad-Adenauer-Stiftung. Russlands strategische Kommunikation zur Beeinflussung innenpolitischer Prozesse in Deutschland. URL:
<https://www.kas.de/en/web/baltischestaaten/single-title/-/content/russlands-strategische-kommunikation-zur-beeinflussung-innenpolitischer-prozesse-in-deutschland-1> (date of access: 20.03.2026).
49. Klicksafe.de. Prebunking - Schutz vor Desinformation. URL:
<https://www.klicksafe.de/desinformation-und-meinung/prebunking-schutz-vor-desinformationen> (date of access: 18.03.2026).
50. Kuhn, J. Bundestagswahl und Sicherheit. Cyberangriffe auf die Demokratie. 2021. URL: <https://www.deutschlandfunkkultur.de/bundestagswahl-und-sicherheit-cyberangriffe-auf-die-100.html> (date of access: 17.03.2026).
51. Lamberty P., Frühwirth L. Pro-Russian Disinformation and Propaganda in Germany: Russia's full-scale Invasion of Ukraine. (2023). URL:
https://cemas.io/en/publications/pro-russian-disinformation-and-propaganda-in-germany/2023-02-24_ProRussianDisinformationAndPropagandaInGermanyRussiasFullScaleInvasionInUkraine.pdf (date of access: 21.02.2026).
52. Libmod.de. (2024). Impact of Russian Disinformation in Germany. URL:
<https://libmod.de/en/impact-of-russian-disinformation-geopolitics/> (date of access: 12.03.2026).

53. Libicki, M. C. (2017). The Convergence of Information Warfare. *Strategic Studies Quarterly*, 11(1), 49–65. URL: <http://www.jstor.org/stable/26271590> (date of access: 19.02.2026).
54. Lunday, C. (February 9, 2025). Putin's Bot Army tries to swing the German election. *POLITICO*. URL: <https://www.politico.eu/article/germany-election-flood-social-media-x-russia-bots-kremlin-operation-false-news/> (date of access: 19.03.2026).
55. Manova Magazin. (2023). Der Himmel auf Erden. URL: <https://www.manova.news/artikel/der-himmel-auf-erden> (date of access: 10.03.2026).
56. Manova Magazin. (2023). Eine Chance für den Frieden. URL: <https://www.manova.news/artikel/eine-chance-fur-den-frieden> (date of access: 10.03.2026).
57. Manova Magazin. (2023). Gesichter des Krieges. URL: <https://www.manova.news/artikel/gesichter-des-krieges> (date of access: 10.03.2026).
58. Martin C., Libicki. THE CENTER FOR ADVANCED. TECHNOLOGY. ACT (1995). What is Information Warfare? – C. 9-54, 67-81 URL: <https://smallwarsjournal.com/documents/libicki.pdf> (date of access: 12.02.2026).
59. Miskimmon, Alister, Ben O'Loughlin, and Laura Roselle, 'Strategic Narratives, Soft Power, and Foreign Policy', in Juliet Kaarbo, and Cameron G. Thies (eds), *Foreign Policy Statecraft*, in Juliet Kaarbo, and Cameron G. Thies (eds), *The Oxford Handbook of Foreign Policy Analysis*, Oxford Handbooks (2024; online edn, Oxford Academic, 22 Feb. 2024). URL: <https://doi.org/10.1093/oxfordhb/9780198843061.013.25> (date of access: 01.03.2026).
60. McCombs, M. E., & Shaw, D. L. (1972). The Agenda-Setting Function of Mass Media. *The Public Opinion Quarterly*, 36(2), 176–187. URL: <http://www.jstor.org/stable/2747787> (date of access: 05.03.2026).

61. Neues aus Russland. (2023). Film: "Donbass 2022" von Alina Lipp. URL: <https://neuesausrussland.com/donbass-2022-von-alina-lipp-video/> (date of access: 06.03.2026).
62. Nabozhniak, O., Tsekhanovska, O., Castagna, A., Khutkyy, D., Melenchuk, A. Revealing Russian influence in Europe: Insights from Germany, France, Italy and Ukraine. (2023). – C. 26-46 URL: <https://www.gmfus.org/sites/default/files/2024-01/revealing-russian-propaganda-3%5B71%5D.pdf> (date of access: 07.03.2026).
63. Nye Joseph S.,. Protecting Democracy in an Era of Cyber Information War. (2019). URL: <https://www.belfercenter.org/sites/default/files/files/publication/ProtectingDemocracy.pdf> (date of access: 25.02.2026).
64. Nazari, S. (October 28, 2025). Storm-1516 and R-FBI: Russian attempts to interfere in the German election. Alliance4Europe. URL: <https://alliance4europe.eu/storm-1516-german-elections> (date of access: 03.03.2026).
65. Nquiringminds. AI cyberattacks threaten the integrity of the German election scheduled for February 2025. URL: <https://nquiringminds.com/cybernews/ai-cyber-attacks-threaten-integrity-of-german-election-scheduled-for-february-2025/> (date of access: 09.03.2026).
66. OSINT: Open source intelligence. Bundesamt für Verfassungsschutz. (March 28, 2024). URL: <https://www.verfassungsschutz.de/SharedDocs/glossareintraege/DE/O/osint.html> (date of access: 26.03.2026).
67. OSINT-analyse: Was sie ist, wie sie funktioniert und Wofür Sie Verwendet wird. ACS. (n.d.). URL: <https://www.acs.it/de/blog/cybersicherheit/osint-analyse-was-ist-wie-funktioniert-und-wofur-verwendet-wird/> (date of access: 26.03.2026).
68. Overton Magazin. Startseite. URL: <https://overton-magazin.de/> (date of access: 08.03.2026).

69. OSINT: Open-source intelligence. (n.d.). What is OSINT: Open-source intelligence?. URL: <https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence> (date of access: 26.03.2026).
70. Porche, I. R., Paul, C., York, M., Serena, C. C., Sollinger, J. M., Axelband, E., Min, E. Y., & Held, B. J. (2013). The Information Environment and Information Warfare. In *Redefining Information Warfare Boundaries for an Army in a Wireless World* (pp. 11–18). RAND Corporation. URL: <http://www.jstor.org/stable/10.7249/j.ctt3fh1qp.10> (date of access: 10.03.2026).
71. POLYGRAPH.info. Pro-Russian Falsehoods From Kim Dotcom, Alleged Racketeer. POLYGRAPH.info. (2022). URL: <https://www.polygraph.info/a/fact-check-pro-russian-falsehoods-kim-dotcom/6743375.html> (date of access: 04.03.2026).
72. Psiram. Unser Mitteleuropa. URL: https://www.psiram.com/de/index.php/Unser_Mitteleuropa (date of access: 12.03.2026).
73. Psiram. Uncut-News. URL: <https://www.psiram.com/de/index.php/Uncut-News> (date of access: 12.03.2026).
74. Psiram. Wilhelm Domke-Schulz – Psiram. URL: https://www.psiram.com/de/index.php/Wilhelm_Domke-Schulz (date of access: 12.03.2026).
75. Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, 11(4), 50–85. URL: <http://www.jstor.org/stable/26271634> (date of access: 20.02.2026).
76. Parker, Daniel M.. "Information Warfare: Technology and the Information Advantage" (1996). Master of Arts (MA), Thesis, Political Science & Geography, Old Dominion University, DOI: 10.25777/2gex-5j02. URL: https://digitalcommons.odu.edu/gpis_etds/174 (date of access: 03.05.2026).
77. Plaß, C. Behörden-Seiten nicht erreichbar. Bundesregierung bestätigt HackerAngriffe. ARD Berlin, 2022. URL:

- <https://www.tagesschau.de/inland/cyberattacke-bundesregierung-ddos-101.html> (date of access: 26.03.2026).
78. Raquel Miguel Serrano, EU DisinfoLab. (March, 2023). Disinformation Landscape in Germany. URL: https://www.disinfo.eu/wp-content/uploads/2023/03/20230224_GER_DisinfoFS_V2.pdf (date of access: 15.03.2026).
 79. Rand. The Russian “firehose of falsehood” propaganda model: Why it might work and options to counter it. URL: <https://www.rand.org/pubs/perspectives/PE198.html> (date of access: 17.03.2026).
 80. Report24. Redaktion. URL: <https://report24.news/redaktion/> (date of access: 08.03.2026).
 81. Statista. Taurus-Marschflugkörper: Meinung zur Lieferung an die Ukraine 2024. URL: <https://de.statista.com/statistik/daten/studie/1453704/umfrage/meinung-zur-lieferung-von-taurus-marschflugkoerpern-an-die-ukraine/> (date of access: 05.03.2026).
 82. Stickings T., The National News, (2022). Telegram user arrested over pro-Russian propaganda in Germany. URL: <https://www.thenationalnews.com/world/europe/2022/08/05/telegram-user-arrested-over-pro-russian-propaganda-in-germany/> (date of access: 11.03.2026).
 83. Sky News. Kaitlin Tosh, S. M., and T. C. (February 21, 2025). German election: From AI influencers to Russian disinformation, the far-right is getting a leg up online. URL: <https://news.sky.com/story/german-election-from-ai-influencers-to-russian-disinformation-the-far-right-is-getting-a-leg-up-online-13313167> (date of access: 23.03.2026).
 84. Tagesschau.de. (2023). Reveland C., Siggelkow P. EU-Sanktionen: Wie finanzieren sich Putin-Propagandisten?. URL:

- <https://www.tagesschau.de/faktenfinder/kontext/russland-propaganda-finanzierung-101.html> (date of access: 28.03.2026).
85. Tages-Anzeiger. (2014). Kohler F. Russlands schärfste Zunge. URL: <https://www.tagesanzeiger.ch/russlands-schaerfste-zunge-545292575900> (date of access: 05.03.2026).
 86. Tagesschau.de. Ex-Wirecard-Chef Marsalek soll für russische Dienste gearbeitet haben. tagesschau.de. (2024) URL: <https://www.tagesschau.de/inland/innenpolitik/marsalek-spionagevorwurf-102.html> (date of access: 28.03.2026)
 87. Teneo. Adante President, A. by Courtney, Adante President, C., Adante, C., President, Associate, R. C., Cole, R., Associate, S., Associate, L. M., Mansky, L., Menzie Associate, L., Menzie, L., Associate, Ryan Associate, E., & Ryan, E. (2025, January 6). 2025 Cyber Outlook: New Year, more risk. URL: <https://www.teneo.com/insights/articles/2025-cyber-outlook-new-year-more-risk/> (date of access: 20.03.2026).
 88. Ulrich Heyden, 03.05.2023. Donbass-Filmregisseur Domke-Schulz: „Sie wollten nicht Menschen zweiter Klasse sein“. NachDenkSeiten. URL: <https://www.nachdenkseiten.de/?p=97152> (date of access: 08.03.2026).
 89. Upguard. RSS. Chin, K. (2024, November 18). Cybersecurity laws and regulations in Germany: URL: <https://www.upguard.com/blog/cybersecurity-laws-and-regulations-germany> (date of access: 07.03.2026).
 90. Wesolowski, K., & Klug, T. (July 30, 2025). Fact checks: Russia’s influence on Germany’s 2025 election. <https://www.dw.com/en/russian-disinformation-aims-to-manipulate-german-2025-election/a-71664788> (date of access: 22.03.2026).
 91. Welker, B. (2025). Geopolitical mythmaking: A narrative study of German far-right media discourse on the Russian invasion of Ukraine. *Critical Discourse Studies*, 1-19. URL: <https://www.tandfonline.com/doi/pdf/10.1080/17405904.2025.2524372> (date of access: 18.03.2026).

92. YouTube channel Голос Германии (Voice of Germany).
<https://www.youtube.com/@Sergeyf617> (date of access: 09.03.2026).