

13. Залкін С. В. Системний аналіз наративів інформаційної війни Російської Федерації проти України. *Наука і техніка Повітряних Сил Збройних Сил України*. 2025. № 3. С. 93–102.

14. Петришин Г. Інформаційна війна Росії проти України: особливості, засоби та динаміка наративів. *Політичні дослідження*. 2025. Вип. 1. С. 117–128.

15. Драбюк С. Штучний інтелект, пропаганда та дезінформація в умовах гібридної війни. *Вісник Ужгородського національного університету*. 2025. Вип. 90. С. 348–356.

Honcharuk Oleksandra, cadet of Kharkiv National University of Internal Affairs;

Sichko Ilya, cadet of Kharkiv National University of Internal Affairs

Research Supervisor – **Yevtushok Volodymyr**, senior lecturer in the Department of Tactical and Special Training at Institute No. 2 of Kharkiv National University of Internal Affairs

DISINFORMATION AS A HYBRID THREAT: DETECTING AND COUNTERING FAKE NEWS, OSINT TOOLS, AND ENGAGEMENT WITH THE MEDIA

Today, disinformation is not just lies on the internet. It is a tool that the enemy uses to deliberately target public consciousness, undermine trust in the state, and sow panic. In the context of full-scale war, information and psychological operations have become weapons just as much as missiles and drones [1]. That is why the ability to recognize fake news, use open-source intelligence tools, and interact effectively with the media is no longer just a desirable skill, but an essential part of training for security professionals.

The main danger of modern disinformation is that it doesn't impose a single viewpoint – it undermines people's very ability to distinguish truth from falsehood. Hostile information campaigns are cleverly designed: they take real facts, pull them out of context, add the necessary emotional charge – fear, anger, despair – and spread them through bot farms and anonymous Telegram channels [2]. People see familiar faces, familiar words – and believe them. You can't fight this with isolated debunking. You need to understand the entire architecture of the campaign: who created the narrative, how it spreads, and what audience it's targeting.

Fact-checking is a specific algorithm, not intuition. First, we look at the source: if there are no links to official organizations or specific individuals, that's already a red flag. Then we assess the emotional tone: a clickbait headline with five exclamation points and a call to "share immediately" is a classic sign of manipulation [3]. Next, we check the context – is the quote taken out of context from another situation? If the fake news has already spread, arguing with its authors is pointless. The right tactic: quickly fill the information space with verified facts from official sources, leaving no vacuum for the enemy to fill with their own [5].

The technical aspects of verification are also important. Thanks to OSINT tools, what used to take weeks of work can now be done in a matter of hours. Google Lens, TinEye, and InVID allow you to trace a photo's original source and detect signs of editing. FotoForensics and ExifPilot reveal a file's metadata – where and when it was taken, and whether it was edited. Google Earth, Wikimapia, and Sentinel Hub help verify whether an event actually took place at the stated location. Whois, DNSDumpster, and the Wayback Machine show who owns a website, when it was registered, and what was on it before the page was deleted [4]. All of this is not just analytics, but a real evidence base for blocking harmful resources.

But no tool can replace proper communication with the media. The media is the primary channel between the government and society. If the government remains silent, the media fills the void with whatever information is available, and the enemy takes the opportunity to spread its own narrative [6]. Therefore, the official response must be swift, clear, and come from specific individuals – not abstract statements like "competent authorities report." A unified communications center with designated spokespersons eliminates the risk of contradictory statements, which the enemy immediately exploits to discredit [3]. It is worth mentioning the training of journalists separately – joint training sessions on cyber hygiene and working with open sources genuinely improve the quality of content and reduce the risk of inadvertently spreading enemy narratives [5].

There is no single magic solution to countering disinformation. It is an ongoing effort that combines personal media literacy, technical data analysis skills, and a well-thought-out communication strategy [6]. When all three components work together, the enemy's information operations lose their effectiveness. Where even one is missing, a vulnerability emerges that the enemy will inevitably exploit.

References

1. Ukraine. Law of Ukraine. On National Security of Ukraine: Law of Ukraine dated June 21, 2018, No. 2469-VIII. *Vidomosti Verkhovnoi Rady Ukrainy*. 2018. No. 31. Art. 241. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> [in Ukrainian]
2. Center for Countering Disinformation under the National Security and Defense Council of Ukraine: analytical materials and reports: website. URL: <https://cpd.gov.ua> [in Ukrainian]
3. Center for Strategic Communication and Information Security under the Ministry of Culture and Information Policy of Ukraine. How to spot a fake and counter manipulations in the information space: website. URL: <https://spravdi.gov.ua> [in Ukrainian]
4. Bellingcat Investigation Toolkit: practical guides and cases on data verification and OSINT investigations: website. URL: <https://www.bellingcat.com/resources/2021/11/09/the-bellingcat-toolkit-for-digital-investigators/>.
5. European Journalism Centre. Verification Handbook: a handbook on media literacy and fact-checking in crisis situations: website. URL: <https://verificationhandbook.com>.
6. Dutsyk, D. Ukrainian media and hybrid warfare: challenges for professional standards. *Collection of Scientific Papers on Strategic Communications and Countering Information Threats*. 2018. Iss. 1. P. 34–42. URL: <https://comms-journal.in.ua> [in Ukrainian]

Горбань Роман Владиславович, здобувач вищої освіти НАВС

Науковий керівник – **Резнік Юлія Степанівна**, старший викладач кафедри кримінального права та кримінології навчально-наукового інституту права та психології НАВС, кандидат юридичних наук

ПРОБЛЕМИ КРИМІНАЛЬНО-ПРАВОВОЇ КВАЛІФІКАЦІЇ ВОЄННИХ ЗЛОЧИНІВ В УКРАЇНІ В КОНТЕКСТІ ІМПЛЕМЕНТАЦІЇ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА

Розбудова ефективної системи притягнення до відповідальності за міжнародні злочини вимагає створення несуперечливого національного кримінально-правового підґрунтя, спроможного відобразити специфіку правопорушень, вчинених у контексті війни. Ключовим інструментом судочинства у цій сфері є ст. 438 Кримінального кодексу України (КК України), яка має бланкетний характер: її диспозиція не описує детальний перелік заборонених діянь, а відсилає до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України (зокрема, до Женевських конвенцій 1949 року, Гаазьких конвенцій тощо).

Досліджуючи архітектуру цієї норми, Н. В. Коломієць вказує, що абстрактність і відсутність чіткої дефініції поняття «воєнний злочин» безпосередньо у КК України тривалий час виступали деструктивним чинником [1, с. 145]. Слідчі органи та суди опинялися у ситуації правової невизначеності на етапі досудового розслідування. О. Жовтюк додає, що це породжувало «інформаційний та методологічний вакуум», де формулювання підозр та складання обвинувальних актів вимагало від слідчого функцій експерта з міжнародного публічного права [3, с. 132].

Ситуація змінилася після того, як Україна у 2024 році ратифікувала Римський статут Міжнародного кримінального суду [9]. На виконання цих зобов'язань було впроваджено пакет змін до Кримінального та Кримінального процесуального кодексів України, які повноцінно набули чинності з 2025 року. Це дозволило частково імплементувати положення ст. 8 Римського статуту, яка диференціює воєнні злочини на блоки залежно від характеру конфлікту та об'єкта посягання.

Водночас, як зауважують О. В. Кришевич та І. М. Ткаченко, у зв'язку з цим виникла нова доктринальна і практична проблема, пов'язана з дією кримінального закону в часі [4, с. 112].