

National Security and Defense Council of Ukraine
Center for Countering Disinformation

Published with the support of the
EU Advisory Mission Ukraine

MANUAL ON COUNTERING DISINFORMATION



Introduction	4
Techniques and tools of informational influence	7
Anatomy of informational influence campaigns	8
Vulnerabilities in the information space.....	10
Stages of public opinion formation.....	11
Narratives and a target audience in the system of informational influence exerted by Russia	12
Hostile resources and how to track them	18
1. Twitter	19
2. Media resources	22
3. Telegram	25
4. YouTube.....	27
5. Facebook	28
6. Deepfakes.....	30
Case studies of informational influence exerted by the Russian Federation (the Center’s practical experience)	32
The “Mobilization in Poland” campaign aimed at discrediting Ukrainian- Polish relations	33
A campaign to discredit Ukraine’s Euro-Atlantic aspirations.....	37
A campaign to discredit NATO assistance.....	40
A campaign to discredit Ukrainian-Japanese relations	43
Recommendations for countering harmful informational influence and com- municating with the target audience.....	46
Fact-based response	47
Glossary	52

INTRODUCTION



This manual has been created in response to the actions in the information space taken against Ukraine by its adversaries. Every month, Ukraine faces thousands of information and cybersecurity threats, psychological threats, and other types of threats from the Russian Federation and its satellite allies. The enemy is well aware that modern warfare is not limited to land, sea, air, and space. Modern warfare also involves information and cyberspace, which are used in concert to achieve one's main goal of forcing the enemy to do their bidding.

The main tool used to achieve hybrid warfare goals is informational influence. Unfortunately, the first year of war has revealed that this influence can be extremely aggressive, with the enemy exploiting all the vulnerabilities of the Ukrainian society to achieve its goals.

Therefore, in order to improve the system of countering enemy informational influence, to familiarize ourselves with its subtleties, as well as to demonstrate the tactics, techniques, and methods employed by the enemy, the Center for Countering Disinformation has collected all available



experience in this area and divided the information into the following sections:

1. The techniques and tools used to exert informational influence.

The objective of this section is to illustrate how the enemy operates in the information space.

2. Enemy resources: how to identify and track them.

The section covers the information channels used by the enemy to exert direct informational influence on Ukrainian society.

3. Case studies of informational influence exerted by the Russian Federation (the Center's practical experience).

The section presents examples of malign informational influence the Center for Countering Disinformation has successfully dealt with since the beginning of the large-scale invasion.

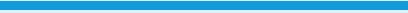
4. Recommendations for countering harmful informational influence and communicating with the target audience.

This section provides recommendations for countering malign informational influence and ensuring efficient communication of information to the target audience in order to avoid the harmful consequences of such influence.

5. Glossary.

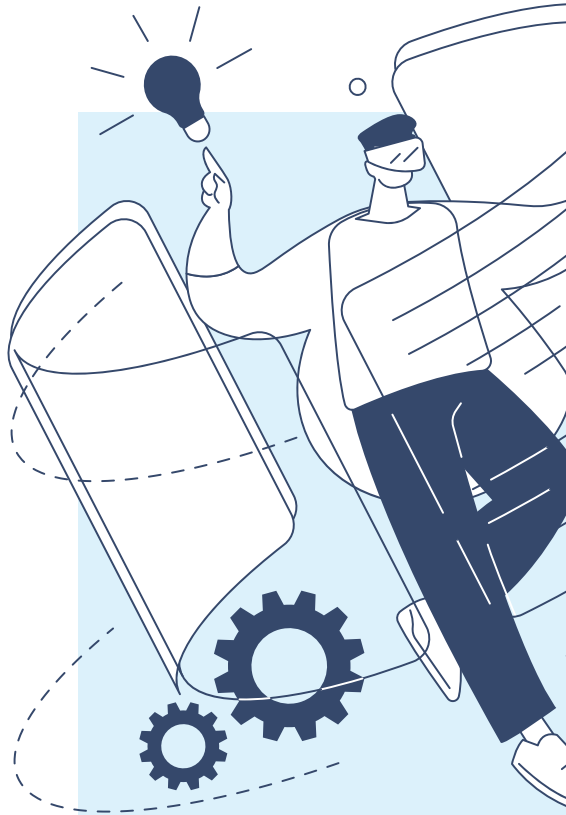
This section describes the terms used by the Center for Countering Disinformation in the course of its activities.

We hope that by mastering the knowledge contained in this manual, the reader will recognize the importance of countering hostile informational influence, as well as enrich their arsenal of tools and techniques that can be used for mounting effective resistance in the information space.



TECHNIQUES AND TOOLS OF INFORMATIONAL INFLUENCE

Informational influence involves potentially harmful forms of communication organized by state actors or other representatives of foreign countries. They deliberately interfere in the internal affairs of a country to create an atmosphere of distrust between the state and its citizens. Various forms of informational influence can be used separately or as part of a larger informational influence campaign employing a broad range of various technologies. Besides communication, any technique, ranging from diplomatic and economic sanctions to demonstrations of military force, can be used to influence society.



Anatomy of informational influence campaigns

1. Using influence techniques

Public relations, marketing, diplomacy, journalism, and lobbying are examples of widely recognized ways to influence people's views and behavior. Informational influence tools imitate the above forms of interaction, but are used in a destructive way.



2. Disrupting public discussions

Foreign states use information activities to influence areas and public discussions that they can benefit from. Such influence is exercised both directly and indirectly, using both open propaganda and covert funding of civil society groups. Furthermore, the interference of unauthorized actors in public debates can change the public perception of key views and influence decision-making.



3. Activities conducted to promote one's personal interests

Tools and techniques of informational influence are aimed at achieving specific goals benefiting a foreign state. Such goals may range from obtaining specific decisions to polarizing political debates.



4. Exploiting vulnerabilities

Every society faces certain challenges. These challenges can include social or class tensions, social inequality, corruption, security, or other issues that are key to social life. Hostile countries identify and systematically exploit these vulnerabilities to achieve their own goals.

Vulnerabilities in the information space



The very process of human cognition is highly susceptible to informational influence. Our thoughts are the result of a certain rational process, individual actions, or the emergence of new information. Witnesses, subject-matter experts, government officials who are considered to be the most competent, and others with deep expert knowledge interpret the situation in a broader context. The media collects this information and disseminates it to different segments of society, both online and offline. However, in practice, the algorithm may vary slightly, but in general, this is what the theory of public opinion formation in a democratic society looks like.

Stages of public opinion formation

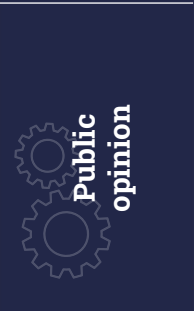


1. New information

Information about an event, scientific discoveries, media news, or political decisions.

2. Information received from experts, officials, and reliable sources

This information is commented on and analyzed by witnesses, experts, and officials who interpret it for the general public.



3. Public information

Information becomes public knowledge. It is then discussed and interpreted both in private discussions and on social media.



4. Recipient

A person receives information directly as a result of their belonging to a particular social group and through the information channels they use.

The distortion of information or its modification through malicious and harmful influence at any stage distorts the healthy process of forming public and personal opinions. To achieve this goal, the enemy engages fake experts, bribed public figures, fake resources, and “alternative” media, etc., which in turn are guided by narratives.

Narratives and a target audience in the system of informational influence exerted by Russia

The informational influence activities involve a certain type of storytelling. Images of events, phenomena, organizations, places, or groups are often shaped in such a way as to conform to a preconceived conception. Storytelling activities that are planned intentionally and used in communication activities are referred to as strategic narratives.

The key to predicting the response is to identify the strategic narratives involved and the logic behind them. The following three key types of strategic narratives are usually identified:

1. Positive or constructive: "It's the truth!"

The goal is to provide an alternative perspective on a certain issue. It fits into, or complements and expands, existing well-established strategic narratives.



2. Negative or destructive: "That's a lie!"

The purpose of this exercise is to prevent the formation of a coherent and complete view of the issue or to refute or undermine existing narratives of the subject.



3. Distracting: "Look at this!"

This narrative aims to distract attention from key issues by using, for example, humor, memes, conspiracy theories, or other entertaining and easy-to-read content. The content depends on the preferences of the target audience.



For years, the enemy has successfully used these simple, but very effective narrative-building techniques, and this situation has not changed until after the start of the full-scale war against Ukraine. This success was achieved through a qualitative analysis of the target audience.

The classic scheme employed to divide the target audience into groups:

General public: the widest sampling of the audience.

Tools and techniques of informational influence aimed at society as a whole through the coordination of messages with common narratives.

Social and demographic targeting: sampling from specific groups.

By identifying audiences through demographic factors such as age, income, education, and ethnicity, narratives can be tailored to influence specific groups.

Psychographic targeting: individuals.

Informational influence tools and techniques that are informed by an analysis and categorization of large amounts of data can be targeted at people with specific personality traits, political preferences, behavioral patterns, or other characteristics that define one's personality.

An analysis of the target audience combined with the analysis of strategic narratives and communication methods helps reveal the true purpose of informational influence. Once an understanding of who the target audience is and why it must be influenced is achieved, it will be easier to make a balanced assessment of what the goal of the informational influence is. This, in turn, will help identify the appropriate countermeasures.

Techniques of informational influence employed by Russia

In most cases, techniques are neutral by nature, meaning that they are neither good nor bad. They can be used in open and acceptable ways as a natural part of the democratic dialogue, or with deceitful and criminal intent as part of an informational influence campaign. The use of either of these techniques is not in every instance a sign of targeted (let alone hostile) informational influence. The enemy is adept at using influencing techniques and disguises them as a natural part of the democratic dialogue led by society.

Although the enemy uses a wide variety of techniques and their combinations in building its campaigns, this manual aims to cover only the most important ones.

The main techniques of informational influence employed by Russia



Social and cognitive hacking

- Subliminal advertising
- The effect of the winning side
- Spiral of silence
- Echo chambers and filter bubbles (information bubbles)

Malicious use of technology

- Bots
- Virtual/sock puppet accounts
- Deepfakes
- Phishing

Manipulation of rhetoric

- Actions targeting specific individuals/Ad hominem
- Whataboutism
- Gish's gallop
- Substitution of theses/Strawman
- Interception



Use of false identities

- Straw men
- Impostors and fraudsters
- Forgery
- Potemkin villages
- Fake media

Disinformation

- Falsification
- Manipulation
- Misappropriation
- Satire and parody

Symbolic actions

- Information/data leaks
- Hacking
- Public demonstrations



HOSTILE RESOURCES AND HOW TO TRACK THEM



1. Twitter

No other resources or tools are usually required to identify an inauthentic Twitter account. Twitter has enough data to enable a complete analysis of a page, in particular:

1) Date of creation

This data can be used to determine whether the page was created recently or in advance for an information operation.

2) Profile avatar

Usually, the profile picture is downloaded directly from the Internet to create bots and fake profiles. This makes it possible to verify the image through image recognition algorithms, such as:

1. <https://images.google.com/>



2. <https://pimeyes.com/en> or a free-of-charge alternative <https://tineye.com/>. These tools are designed to recognize faces by parsing all photos available on the Internet.



3. Once all of the above analysis resources have been exhausted, one can **use <https://yandex.ru/images/>** for an in-depth search on the Russian Internet via a VPN.



4. To analyze fake photos, we recommend using **<https://fotoforensics.com/>**. By compressing the photo, this tool shows which areas of the photo have been altered or faked: if the color is white, it means that the photo was not faked, and pronounced rainbows mean that the area was faked.



3) Profile name

There are two profile names on Twitter that can be used to conduct a more detailed analysis. A nickname is a name that the author can change without much effort. A username is a name that cannot be changed quickly and is prefixed with the “@” in search. Usually, bots and fake profiles use either the most trivial combinations of first and last names that are typical for the region or a set of characters without a specific meaning. It is not uncommon for bots with Chinese or American names to attack the comment sections of Ukrainian channels, which can be immediately noticed even without additional checks.

4) Activity

The profile activity section provides analysts with a lot of information. In particular, it is the number of publications over a certain period of time that is meaningful. Typically, numerous posts per day indicate that the profile is not authentic.

5) Interaction with other profiles

When analyzing a profile, it is important to review its interaction with other users. In the case the given user is actively reposting information from other users who appear to be bots or information obtained from suspicious resources, it is highly likely that the profile is engaging in inauthentic behavior.

6) Language

By analyzing the language and spelling used in the profile's posts, one can understand whether machine translation was used to write a post.

7) General profile information

In the profile header, ordinary users sometimes publish useful information about themselves. Inauthentic profiles, in turn, either do not publish any information or use falsified information.



2. Media resources

1) URL links

When conducting its information operations, the enemy can create numerous fake resources that require careful checking. It is important to start by checking the link to the resource because the enemy can create resources that imitate the original ones.

It should be noted that the link protocol has to be examined carefully. Sometimes fake media resources use the HTTP protocol, which is not secure. The thing is that data is transmitted over HTTP in clear text. Such transmission poses a risk of disclosing confidential information if the traffic is intercepted. HTTP protocols solve this problem by adding a data encryption functionality to the original protocol. Furthermore, careful attention should be paid to the ending of the link. For example, the original BBC website has the link <https://www.bbc.com/>, while fake ones may look like this: <http://www.bbc.com.co/>.

2) Headline

The main task of the headline lies in attracting interest and encourage the user to visit the resource page. Therefore, it is crucial for an analyst to pay attention to the headline and understand what emotions it can evoke in the reader.

3) Author

Usually, fake media resources do not have an author, which is also an indicator that the information is fake. If a questionable article has an author, it is important to check their identity and verify which articles have also been authored by this person. Authors of articles are active on social media, so one can check other content produced by them, apart from the article concerned.

4) Sources

Regardless whether or not a given article is authentic, sources cited in it are extremely important. By analyzing the sources used by the author, it is possible to understand where the author got the underlying information and which objectives the author in fact pursued. Therefore, it is important to check all the sources listed, and in their absence, draw the correct conclusions.

5) Content

When reading the text, one can make a logical summary of the goals and ideas inherent in the article. One needs to understand and distinguish between an informative and an argumentative article. An analysis has to cover the style of the article, its underlying principles, or facts. Therefore, it is important to read the article carefully, even several times, and identify the main points prioritized by the author.

6) Images

The author may use images in the text of the article that also require careful checking to understand the objectives pursued by the author. The authenticity of the image can be verified by using the online resources mentioned above.

7) Comments and activity on the article page

Most media resources have a separate comments section. Since the enemy can fill it with fake comments and correspondence between users to make the article look more truthful, it is also important to include it in the scope of the analysis.

Moreover, the enemy can use links to fake media resources to give the article an appearance of popularity as part of its information operations.

8) Other information

When analyzing media resources, careful attention should be paid to the information indicated at the end of the page. It is common practice for companies to provide information that may be required by the user, in particular the company's registered address, links to its social media accounts, official contact details, email address, registration information, information about copyright, privacy policy, etc.



3. Telegram

Telegram, by its nature, does not contain much data suitable for analysis, but one can use some built-in functions to verify the authenticity of the information. Open comments that can be found in channels sometimes can provide additional information. The number of subscribers to the channel and the number of people who viewed the post should also be considered. A channel that has less than 20 % views of the total number of subscribers is definitely frequented by bots. It is also worth checking the authenticity of the channel's link, as the enemy can always create a fake page that imitates the original one. The channel description may contain additional information provided by the author, such as maps, contact details, administrator usernames, crypto wallets, links to other websites, etc.

For an in-depth analysis of Telegram resources, it is recommended to use on-line analytical tools that use the social media's API, such as <https://tgstat.ru/>.

The following tools can be used to analyze Telegram statistics:

1) Channel statistics

On this site, one can enter the channel name or a link to it in the search field. Once the channel has been located, the channel statistics can be reviewed to obtain the following information: the date when the channel was created, the citation index, the average number of views, the number of followers over the time period, the percentage of publications

viewed, and the average number of publications per day. All of the above information may be used to analyze a Telegram channel.

2) Read the channel

This section resembles a regular Telegram feed but has several additional features that may be useful for an in-depth analysis.

- The posts filter has a function that allows viewing deleted posts, as well as a drop-down window where one can select the year and month of the channel's publications.
- The number of views, shares, and reposts can be found under individual publications. By clicking on the views, one can see detailed information about the total views the post has had, and the reposts show the channels and chats where the post was shared.

It is worth mentioning that this section allows viewing posts from channels that are blocked in our region (for example, Rybar).

3) Citation

In this section, one can find a graph with the channels that most actively repost the given channel, as well as the channels most frequently reposted by it. This graph shows the likely network of channels where the channel operates and publishes its content.

4) Publication schedule

This section shows a detailed publication schedule for the past month. This provides an opportunity to verify whether an allegedly "personal" channel that posts from 9:00 a.m. to 5:00 p.m. may, in fact, be operated by an organization or government agency.



4. YouTube

There is enough data available on the platform itself to analyze inauthentic YouTube videos and the pages that publish them. The number of comments, views, and subscribers is worth noting. It is important to keep in mind that bot activity in comments can be determined based on the relevance of the comments themselves. In most cases, comments posted by bots have no content or are basic in nature.

When analyzing a YouTube channel, it is important to look at its other sections. The About section contains additional links to the channel, region, date of creation, total number of views, contact details, and description. There are also the Community and Channels sections where an analyst can get additional information.

It is worth noting that with the advent of the YouTube Shorts format, a significant number of fake videos are now presented in a shortened format. This is due to the fact that such videos are easier to create on a smartphone and, due to the short format, the YouTube algorithm distributes them faster to a wider audience.

There are various tools available for an in-depth analysis of a YouTube channel, but the most affordable one is Social Blade (<https://socialblade.com/>). A link or channel username has to be entered in a search box on this site to get forwarded to the channel page. This is where more detailed information about the channel can be found. In most cases, the "Detailed Statistics" is sufficient for the purposes of analysis. This section contains information about an increase in the number of views and subscriptions to the channel over a certain period of time. This data allows identifying the irregularities in the increase in the number of views and activity on the channel.



5. Facebook

In order to recognize inauthentic behavior on Facebook profile pages and communities, one needs to pay attention to audience engagement and the ratio of likes and shares. It is also worth paying attention to the content of the page. Many fake Facebook pages lack additional information, as inauthentic profiles do not spend so much time creating a believable page.

The following sections of a Facebook page are worth noting to ensure the completeness of an analysis.

1) Information

This is probably the most important section in terms of the analysis of any social media page. It contains essential data that may be useful for the further analysis of the page, such as contact information, page or profile description, links to other social media, number of followers, number of likes, page reviews, links to other websites, and additional information about the page.

2) Photos and Videos sections

These two sections can provide additional information that may be used for analysis purposes, as some pages or communities allow their users to post photos on their pages. In this way, the analyst can scrutinize these photos and find the necessary connections and information to draw the final conclusion.

3) Communities

A community section can sometimes be found on a public Facebook page. This section can provide further information about the network that is being analyzed, as well as evidence of bot activity on the page. For example, a community may have hundreds of thousands of followers, but only 100–200 reactions to posts on the page, which is an indicator of bot activity.

4) Other

Users or administrators decide what additional sections their Facebook page will have. Therefore, it is important to carefully review other sections that may contain information about the interests of a community and topics discussed on the community page. For example, several inauthentic Facebook pages may have a YouTube section.



6. Deepfakes

Deepfake videos first appeared back in 2014, and at that time, they were quite simple and easy to recognize compared to the original video. However, in a short period of time, deepfake technology has evolved considerably. Now, there are paid tools available for creating videos that are barely distinguishable from the original.

An attacker using such videos may have the following intentions:

1. **Blackmail** (a threat to release a compromising video).
2. **Fraud** (impersonation to gain access to systems or data).
3. **Authentication** (manipulation of identification verification or authentication that uses biometric data such as voice or facial recognition patterns to gain access to systems, data, or other resources).
4. **Reputational risk** (the threat of damage to the reputation of a person or organization).

In order to address such vulnerabilities, efforts should be made to identify the deepfakes. **The following methods can prove useful:**

- Looking for unnatural eye movements.
- Paying attention to color and lighting mismatches.
- Comparing the sound quality.
- Noticing strange body shapes or movements.
- Analyzing artificial facial movements.
- Noting the unnatural positioning of facial features.
- Noticing an awkward posture or body type.
- **Real-time deepfakes can be recognized if a person turns their head. This means that a live feed of a deepfake is incapable of processing other parts of the face with 100 % accuracy.**

CASE STUDIES OF INFORMATIONAL INFLUENCE EXERTED BY THE RUSSIAN FEDERATION (THE CENTER'S PRACTICAL EXPERIENCE)



The “Mobilization in Poland” campaign aimed at discrediting Ukrainian-Polish relations



Link:

[https://t.me/
JokerDPR/123](https://t.me/JokerDPR/123)

On February 3, 2022, the website of the Russian news agency Krasnaya Vesna published information, according to which the Ministry of Foreign Affairs of Ukraine was allegedly preparing political notes requesting the return of Ukrainian citizens of military age. The news agency cited an unnamed representative of the so-called “DPR” police, and a report by the Russian news agency Regnum (the report has now been deleted).

On June 17, 2022, at 10:53 a.m., the Telegram channel Joker DPR published a message aimed at discrediting Ukrainian-Polish relations, creating a distrust of the Ukrainian authorities, and spreading a feeling of fear for their safety

among the target audience (men of military age who were forced to leave Ukraine due to the beginning of Russia's full-scale invasion, and their families).

Source:

Telegram channel Joker DPR (92K+ subscribers), part of the Russian network used for information support of hacker attacks and dissemination of the resulting data.

The publication was accompanied by a letter allegedly sent by Minister of Foreign Affairs of Ukraine Dmytro Kuleba to Minister of Foreign Affairs of the Republic of Poland Zbigniew Rau. It appeared from the letter, the Ukrainian minister allegedly asked his Polish counterpart to deport all men of enlistment age from the territory of the Republic of Poland to Ukraine for subsequent mobilization.

On the same day, Cezary Nobis, who positioned himself as a "Polish politician," published a series of documents from the diplomatic institutions of Ukraine and the Republic of Poland and claimed that an official decision had been made to search for all persons of enlistment age who evaded service in the Armed Forces of Ukraine. After that, the aforementioned Telegram channel referred to the publication of Cesar Nobis to support its previous message. The Russian media subsequently picked up this "news" and started spreading it throughout the information space.

The main narrative:

"Ukraine is preparing to mobilize men abroad".

Threat type:

An information campaign aimed at discrediting Ukrainian-Polish relations, creating a distrust of the Ukrainian authorities and spreading a feeling of fear for their safety among the target audience (men of enlistment age who were forced to leave Ukraine due to the beginning of Russia's full-scale invasion and their families).

Scope of distribution: over 100 thousand views

Considering the potentially wide scope of dissemination, the Center analyzed and identified all the elements and stages of the above operation. Thereafter, the Center sent a request to the Ministry of Foreign Affairs of Ukraine and received a confirmation that the letter mentioned above was fake.

Types of distribution sources:

A Russian disinformation network that includes both smaller (up to 100K subscribers) and larger channels (over 100K subscribers), and the Facebook page of Polish official Cezary Nobis.

Conclusion:

The disinformation campaign is destructive to the information security of Ukraine and its international partners.

A decision was made to respond at the inter-agency and intergovernmental levels.

Outcome:

The Center notified the Ministry of Foreign Affairs of Ukraine about the PSYOP.

The Center contacted forthwith the Government Center for Security of the Republic of Poland and shared with them analytical materials containing detailed information about the PSYOP.

As a result of these efforts, the Center and the Government Center for Security informed, through well-established communication channels, the public and relevant state institutions about the PSYOP conducted by the Russian Federation, and also mitigated potential negative consequences.

https://twitter.com/RCB_RP/status/1537788674754191360?s=20&t=GSQhB5Qt-1nM-laCWMAHcg



<https://t.me/CenterCounterintelligenceDisinformation/1851>

However, despite the successful elimination of the above-described enemy PSYOP, the enemy did not abandon its attempts to discredit Ukraine in the eyes of its Polish allies. Therefore, sometime later, the enemy decided to tap into the difference in the interpretation and perception of certain events in the common history of Ukraine and the Republic of Poland, choosing the conservative part of the Polish population as its target audience.

A campaign to discredit Ukraine's Euro-Atlantic aspirations



Link:

<https://tgstat.ru/channel/CXis8yPFITi5Y2Q6/15587>

On November 4, 2022, at 2:12 p.m., a video titled “Six reasons why Ukraine should not join NATO” was published on the private Telegram channel “С МЕСТА СОБЫТИЙ” (“DIRECT FROM THE SCENE”) (over 800K subscribers).

The purpose of the video was to create a false image of Ukraine and the Ukrainian people in the European information space to discredit Ukraine's integration into NATO.

The video was allegedly authored by the European Security & Defense College.

The Center contacted the European Security & Defense College and received confirmation that the organization had not been involved in the creation and distribution of this video.

Source:

Private Telegram channel “С МЕСТА СОБЫТИЙ” (DIRECT FROM THE SCENE) (800K+ subscribers), part of the Russian network.

The main narrative:

“Ukraine’s accession to NATO will have a negative impact on the welfare of member countries.”

Threat type:

An information campaign aimed at discrediting Ukraine.

Scope of distribution:

- 150 thousand views;
- five channels published the article;
- 290 reposts.

Types of distribution sources: a large Russian channel (800K+ subscribers)

Conclusion:

The disinformation campaign failed to achieve its initial goal of the widespread distribution of information on social media. However, it had the potential for further spread as it included hard-hitting messages targeting citizens of the Western states.

Outcome:

The information was shared with Ukrainian diplomatic missions in to the NATO member countries to offset any possible negative impact.



Link: <https://t.me/CenterCounteringDisinformation/3035>

The Center for Countering Disinformation also prepared a message for the Center's website and social media.

The efforts taken by the Center nipped the spread of these messages in the bud.

A campaign to discredit NATO assistance



Link:

[https://t.me/
breakingmash/39593?singl](https://t.me/breakingmash/39593?singl)

On November 3, 2022, at 10:00 a.m., the Mash Telegram channel published a post aimed at discrediting the Armed Forces of Ukraine, the Ministry of Health of Ukraine, and NATO countries.

Source:

Mash Telegram channel (1M+ subscribers), part of the Russian network.

The main narrative:

“NATO countries have been supplying Ukraine with canned blood infected with HIV, hepatitis B & C, and other infections that could lead to an epidemic among Ukrainian military personnel.”

The publication was accompanied by documents allegedly obtained with the help of the Kombatant hacker group. These documents carried the signature of Minister of Health Viktor Lyashko and contained a reference to the personal e-mail address of Prime Minister of Ukraine Denys Shmyhal.

Threat type:

An information campaign aimed at discrediting the Armed Forces of Ukraine and NATO.

Scope of distribution:

- over 1 million views;
- 252 channels posted the article;
- 20 thousand reposts.

Types of distribution sources:

A Russian disinformation network with one very large channel (1M+ subscribers).

Conclusion:

The disinformation campaign is destructive to the information security of Ukraine and its international partners.

A decision was made to respond at the inter-agency level; recommendations were prepared and sent to the Ministry of Health and the Ministry of Defense of Ukraine.

Outcome:

The Ministry of Health of Ukraine refuted the information on its official website.



Link: <https://moz.gov.ua/article/news/sprostovuemo-chergovij-rosijskij-fejk-pro-nejakisnu-krov-dlja-pacientiv>.

The Center for Countering Disinformation also prepared a message for the Center's website and social media.



Link: <https://cpd.gov.ua/warning/dezinformacziya-pro-import-ukrayinoyu-infikovanoyi-krovi/>.

As a result of the response, the threat posed by the information campaign was canceled out at the outset.

A campaign to discredit Ukrainian-Japanese relations



On August 11, 2022, a post aimed at discrediting Ukrainian refugees, Japan, and Ukrainian-Japanese relations in general was published on Twitter and Instagram.

Source:

Japanese bot accounts on Twitter and Instagram.

The main narrative:

“The world has grown tired of the war in Ukraine.”

The publication was accompanied by alleged photos of a billboard of the Sushi no midori company in Tokyo, which depicted a Japanese sushi chef covering the mouth of a Ukrainian woman, with a slogan: “Let’s change the subject – let’s talk about delicious sushi.”

Threat type:

An information campaign aimed at discrediting Ukrainian refugees, Japan, and Ukrainian-Japanese relations in general.

Scope of distribution:

Despite the large potential for dissemination, the scope of dissemination was limited to less than 10 thousand views thanks to the timely response of the Center.

Types of distribution sources:

A Russian network of coordinated inauthentic behavior involving niche Russian media.

Conclusion:

The disinformation campaign is destructive to the information security of Ukraine and its international partners.

A decision was made to respond at the inter-agency level; recommendations were prepared and sent to the Ministry of Foreign Affairs and the Embassy of Ukraine in Japan.

Outcome:

The Embassy of Ukraine in Japan contacted the management of Sushi no midori and requested explanations in connection with the provocative billboard.

The company management informed that it has zero tolerance for discrimination against any country or nationality, and the image that is being disseminated has nothing to do with the company.



Link: https://www.sushinomidori.co.jp/#modal_1329.

Moreover, a statement was filed with the Japanese police asking to open a criminal investigation into a potential offense.

Furthermore, the Center for Countering Disinformation prepared a post debunking the fake for the Center's website and social media



Link: <https://t.me/CenterCounteringDisinformation/2329>.

As a result of the response, the threat posed by the information campaign was canceled out at the outset.

RECOMMENDATIONS FOR COUNTERING HARMFUL INFORMATIONAL INFLUENCE AND COMMUNICATING WITH THE TARGET AUDIENCE



Firstly, it should be understood that there is no one-size-fits-all response to all information threats. As demonstrated above, informational influence can take many different forms. In addition, each organization has regulations that outline the framework within which it can perform its functions, and these limits lead to certain vulnerabilities. Therefore, response tools should be tailored to the specifics of the organization.

The response to an information threat should correspond to its level. Below is a generalized algorithm for responding at different levels.

Fact-based response

The first two levels are assessment and information sharing. They are key to recording and reporting.

Level 1. Assessment.

In order to understand what we are dealing with, we need to assess the situation. What is going on? Who is involved? What are the risks involved? The more information you can gather, the better you can tailor your response.

1.1. Situation analysis.

Analyze the situation and develop a comprehensive view of it. Use the information from the previous sections to determine what you are dealing with.

1.2. Fact-checking.

Conduct fact-checking to determine what is true and what is disinformation.

1.3. Comprehensiveness of the research.

Involve reliable experts to ensure a comprehensive study of the issue.

Level 2. Information sharing.

The threat assessment should be followed by information sharing. This can include both communication with the public and informing the authorities concerned to further coordinate the response to the threat.

2.1. Informing stakeholders.

All stakeholders including colleagues, other departments, and other government agencies should be informed as soon as possible, especially in the case of high-level threats that require a coordinated inter-agency response.

2.2. Official statement.

Communicate the facts of the case in a neutral manner if it is a low-level threat that requires an organization-wide response. Alternatively, prepare a statement that you are investigating the situation. This will give you time to prepare a more thorough response.

Advocacy

The third and fourth levels are about assertion and defense. These steps include activities that are appropriate in difficult situations where an informational influence campaign has been unequivocally identified.

Level 3. Assertion.

Assertion is very similar to information sharing but involves more active argumentation. It is important to keep in mind the values of the organization when formulating a response.

3.1. Narrative.

Establish a connection between the situation and a broader narrative, such as information about the organization and its values, which will help the target audience better understand the matter and form their own opinion.

3.2. Access to information.

Streamline access to information for your target audience. Organize events, meetings, or press conferences to discuss a specific issue and share the position of your organization.

3.3. Dissemination.

Involve key public relations professionals who can help spread your narrative to a wider audience.

Level 4. Defense.

Defense involves a direct response to the aggressor's actions. This step may seem more controversial and is usually only available to a limited number of government agencies.

4.1. Complaints.

If the malign informational influence results from a violation of national laws or the social media's code of conduct, law enforcement agencies or platform administrations should be contacted to have the publications removed. This tool should not be abused to avoid negative public discussions.

4.2. Blocking.

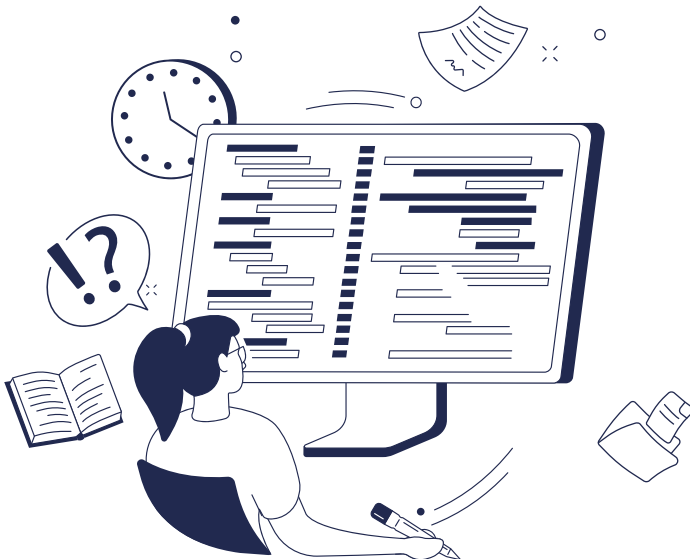
If a person or organization exerts malign informational influence, they can be blocked on the platforms. However, the reason for blocking should be clearly limited to the violation of the platforms' rules. This tool also carries certain potential risks, the main one being the popularity of the blocked person or organization and their reputation. If they have an impeccable reputation and are popular, nothing prevents them from either creating a new page and quickly regaining their audience or appealing the decision, which could lead to unwanted public discussions.

4.3. Exposure.

Exposing the true motives, goals, and affiliations of the person using malign informational influence. Disclosure of the details of the information campaigns they conduct and their coordination with a hostile actor. It is one of the most effective tools that can be used to respond to

large-scale campaigns posing a high level of threat. However, there are certain risks to avoid and to avoid them, the exposure must be supported by a comprehensive analysis that leaves no room for speculation.

The most appropriate level of response depends on the assessment of the situation. If a low level of malign informational impact has been identified, it is best to address the problem at the first and second levels, i.e., to inform stakeholders and the public in an unbiased manner. This response is based on facts. For more complex cases that involve medium and high levels of malign informational influence, the first two levels should be used in combination with the third and fourth levels, i.e., to assert the position and defend the organization affected from attacks. However, caution should be exercised at this stage, as the organization may face some mirrored risks, so such responses should be carefully prepared.



GLOSSARY



Informational influence means the targeted use of special information tools and techniques to change attitudes and beliefs of individuals, social groups, or the population (behavioral modification) in the information and technical infrastructure of the target and/or the physical condition of a person.

Hybrid warfare means a war that involves the use of a combination of conventional weapons, guerrilla warfare, terrorism, cyberwarfare, trade wars, patent wars, revanchist movements, propaganda, human rights violations, crimes against humanity, military exercises, displacement, usurpation, manipulation of public opinions, acts of censorship, and criminal behavior in order to achieve certain political goals. The main goal of the hybrid warfare pursued by the aggressor state is to create internal contradictions and conflicts in the target state that can be thereafter used to achieve the political goals of aggression that are attained through the use of conventional warfare.

Bot means a software application designed to interact with and mimic human users using the same interfaces as human users, either automatically and/or according to a fixed schedule.

Virtual/sock puppet accounts mean fraudulent accounts operated by a person who hides their intentions anonymously. These fake identities are used to join online communities and participate in debates to disseminate fake or contradictory information. Two or more virtual identities can also be used simultaneously to artificially encourage both sides of a debate.

Gish gallop means a rhetorical technique in which a person in a debate attempts to overwhelm their opponent by providing an excessive number of arguments with no regard for the accuracy, strength, or relevance of those arguments.

Disinformation means false or manipulative information that is deliberately spread to deceive people. Disinformation is the cornerstone of classical propaganda and the basis of the more modern phenomenon of fake news.

Info-alibi means information manipulation where one party preemptively accuses another party of actions that have been / will be committed by the accusing party. For example, Russia accuses the Ukrainian side of planning to shell civilians in the region that will later be shelled by Russian artillery.

Information attack means a combination of intentional actions carried out by a perpetrator to violate one of the three properties of information, i.e., its availability, integrity, or confidentiality.

Information bubbles / echo chambers mean organically created sub-groups in which people only engage with others of similar opinions and beliefs. Information bubbles can also be used to disseminate targeted information to certain groups or even manipulate such groups to restrict their access to the sources of information sources; as a result, a person ends up in a closed information circulation system.

Information threat means a potential or real adverse action or event caused by a vulnerability that leads to an undesirable impact on the information space.

Information campaign means a planned flow of information with specific goals and objectives, disseminated through various means and channels used for mass and individual information sharing, and characterized by a certain duration and intensity.

Information manipulation means accurate information that has been distorted to influence consumer behavior and judgment.

Information operation means a pre-planned and prepared act of informational influence on a targeted audience aimed at achieving certain strategic goals. Information operations are characterized by a short duration and relatively small resources available to them.

Information space means a separate sphere of human activity where information is created, changed, and transmitted. It is a historical form of coordinated and structured information resources that accumulate the results of people's communication activities. A set of databases, communication systems, and techniques for their application can be considered to constitute an information space.

Coordinated inauthentic behavior (CIB) means a malicious activity conducted with the help of programs, bots, and other tools used for conducting information operations that impersonate real persons to shape the desired public opinions and achieve certain goals.

Coordinated inauthentic behavior networks (CIBNs) mean a network of interconnected CIB tools owned by a certain organized group of persons and used to achieve their goals by exerting informational influence on users.

Message (in communications) means a separate unit of information transmitted by a source for use by a recipient or a group of recipients. A message can be delivered in a variety of ways, including a physical letter, a phone call, a post on social media, etc. Furthermore, a statement made by one of the opponents against the other can also be deemed a message.

Misappropriation means the use of content that, despite being, in fact, correct, is not related to a particular issue, to create a false conception of that issue, event, or person. For example, a fake news article may use images related to an entirely different event as evidence.

Misinformation means false information that is disseminated without criminal intent or intent to mislead. For example, journalistic errors, rumors, and gossip constitute misinformation. People usually believe this information and spread it.

Narrative means a way of presenting or understanding a situation or series of events that reflects and promotes a particular point of view or set of values.

Potemkin villages mean fake campaigns, research institutes, or think tanks created to build trust in disinformation.

Spiral of silence means a theory of mass communication that applies to a situation where people feel a growing need to hide their views if they are not supported by the majority. Before expressing their opinions on a certain phenomenon or situation, audience members tend to unconsciously check whether their views are shared by the majority.

Fake means a forgery or imitation of elements of the information space. It can exist in the form of distorted information (fake news or publication), a channel used to disseminate false information (a public page on social media, website, etc.), or a fake page of a certain person on social media created to mislead the user of the platform (bots, trolls, etc.).

Phishing is a fraudulent practice of sending emails or other messages, allegedly from reputable companies or individuals, to trick users into disclosing personal information, such as passwords and credit card numbers.

Whataboutism means a cheap rhetorical tactic in which a critical question or argument is not answered or discussed, but retorted with a critical counter-question that expresses a counter-accusation.



Kyiv
2023

