RUSSIA'S HYBRID WAR AGAINST UKRAINE

WINNING ON THE INFORMATION FRONT

Handbook

2023

CENTRE FOR STRATEGIC COMMUNICATION AND INFORMATION SECURITY

CENTRE FOR DEMOCRACY AND RULE OF LAW

Sweden Sverige

The information war waged by the Russian Federation against Ukraine is just as perilous as any direct military action. It has the potential to undermine the unity of Ukrainian society, the trust of citizens in the government and armed forces, and Ukraine's relationships with its allies. Therefore, it is vital for employees of state institutions to possess the skills to recognise and counter Russian propaganda and disinformation.

The primary objective of this manual is to familiarise readers with the fundamental aspects of countering Russian disinformation and propaganda. To achieve this, we have analysed the information component of the hybrid warfare conducted by Russia against Ukraine, identifying the main characteristics and techniques of Russian propaganda and disinformation, as well as methods for detecting and responding to Russian disinformation within the context of strategic communications. Furthermore, we have provided evaluation frameworks for communication measures.

The manual is for government officials and employees of local government bodies. The materials will be valuable to leaders, their deputies, department specialists, communications managers, social media specialists, and all individuals engaged in public communication on behalf of Ukrainian state institutions or local government bodies.

AUTHORS:
team of the Centre for Strategic Communication and Information Security

EDITED
by the team of Centre for Democracy and Rule of Law

TARGET AUDIENCE

Olga, 27 years old, SMM-specialist of the Main Department of the State Emergency Service of Ukraine in the Ternopil region*

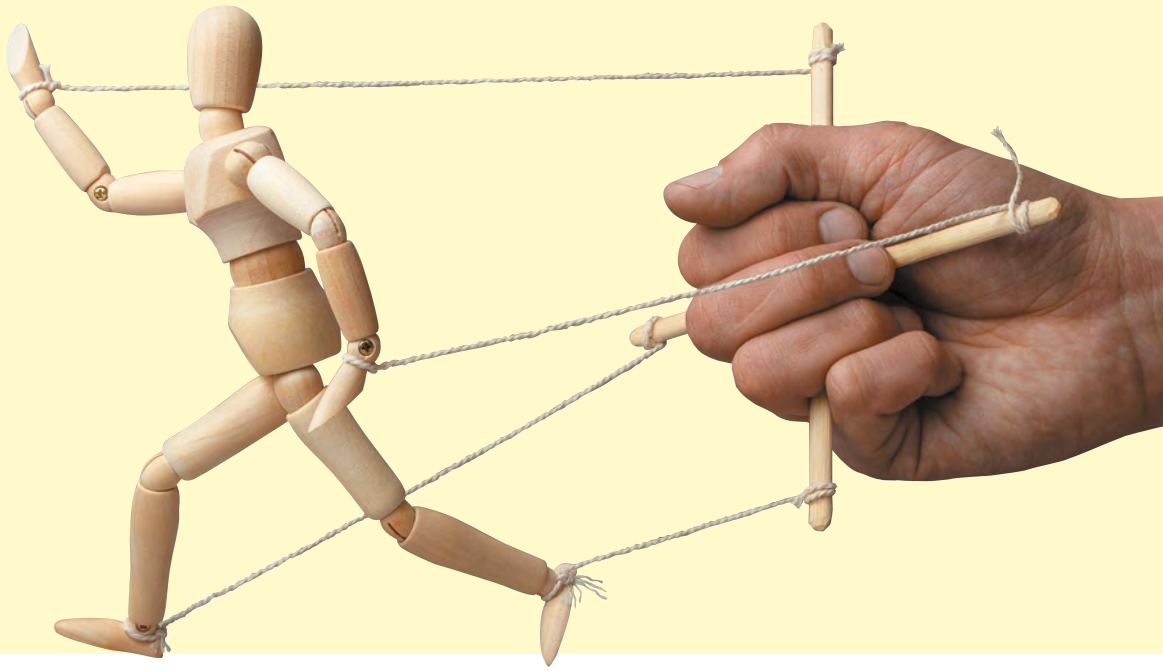
Yevhen, 32 years old, Deputy Head of the Mykolaiv Regional State Administration for Digitalization

Andriy Vasylyovych, 65 years old, head of Boromlyanska village hromada, Sumy region

*These persons and positions are fictitious

This handbook has been prepared within the framework of the core support programme of the Centre for Democracy and Rule of Law, enabled by the financial support from Sweden. The original publication is in Ukrainian, and the English version has been made possible by the support of the NATO Strategic Communications Centre of Excellence.

CONTENT



DEFINING HYBRID AND INFORMATION WARFARE.

WHAT IS RUSSIAN PROPAGANDA?

Debates regarding the concept of hybrid warfare among political and military experts gained prominence in the early 2000s. Yet, as a phenomenon, it has been prevalent since the dawn of warfare. Despite the extensive experience gathered in this field, the concept of hybrid warfare still lacks a universally accepted definition.

> This manual uses the following definition of hybrid war, as being **'a military strategy aimed at masking the role of the aggressor in the conflict. It involves sponsoring insurgencies, "false flag" military actions, and a wide range of non-military means of influencing the enemy (economic, information-psychological, cyberwarfare, etc.)'.**

The 'hybridity' arises from blending unconventional (information and economic actions) and conventional (use of armed force) methods of conducting war. Hybrid warfare also resides in the so-called grey zone of international law, where it is challenging to identify, measure, and regulate since the standard rules of the laws and customs of war are not applicable.

TRADITIONAL METHODS OF WAR

- Regular Armed Forces
- Clear state affiliation
- Diplomacy
- Economic sanctions
- Complex logistics
- Advanced technologies
- Firepower dominance
- Observance of the rules of armed conflict

NON-TRADITIONAL METHODS OF WAR

- Guerrilla methods
- Terrorism
- Incitement of uprisings
- Participation of criminal elements
- Cyber Information Warfare
- Low intensity
- Use of irregular forces
- Non-compliance with the rules of armed conflict[1]

A hybrid war is rarely formally declared, and its ending is not recorded by formal legal acts of the parties. In general, such conflicts have two main features: a blurred line between war and peace and a high level of ambiguity.

The obscuring of boundaries between war and peace presents a challenge in discerning the onset of war, which is characterised by the overt hostility of states towards one another. Rather than deploying conventional forces into the territory of another nation, it proves significantly more economical to disseminate misinformation, dispatch unauthorised militias, stir up the domestic 'fifth column' (media, political parties, church), and employ economic coercion to fulfil political objectives. A high level of ambiguity gives any state using hybrid instruments the opportunity to conceal its involvement in hostile measures targeting another state.

Hostility is veiled in different forms, like a 'special military operation' or 'aid to the brotherly republics of Donbas'. Consequently, the targeted nation must demonstrate to its citizens the reality of an external assault on it and the participation of a specific aggressor country, which is concealing itself behind a façade of non-state entities. Owing to the considerable ambiguity of hybrid warfare, tackling hybrid challenges is far more challenging than conventional military threats.

Other signs of hybrid warfare include the use of economic and diplomatic means of coercion, cyberattacks, information and psychological operations. Political scientist Yevhen Magda names among its characteristic features **THE USE OF INFORMATION WEAPONS, PARTICIPATION IN THE CONFRONTATION OF NON-STATE ACTORS, THE USE OF TERRORIST METHODS, DISREGARD FOR MILITARY LAW AND ETHICS, THE USE OF METHODS OF ECONOMIC AND PSYCHOLOGICAL PRESSURE, PROPAGANDA, ETC[2].**

[1] Brin Najžer. The Hybrid Age. International Security in the Era of Hybrid Warfare (Digital resource)

[2] Magda E. M. Hybrid war: essence and structure of the phenomenon (Digital resource)

Hybrid warfare offers numerous benefits to the state employing it, enabling the attainment of political objectives with little or no use of military force, at a comparatively lower cost, and often allows evading accountability before the international community for war crimes and other breaches of international law. In hybrid warfare, four primary domains are identifiable: economy, weaponry, non-state actors, and information.

- **ECONOMY.** Generating economic difficulties by impacting markets and obstructing the victim country's connections with allies. An instance of this is Russia's deliberate inflation of gas prices in Europe during the winter of 2021–2022.

- **WEAPONS AND COVERT OPERATIONS.** Intentional provision of arms to one or more conflict parties to prolong conflict, topple governments, or destabilize regions. Key roles are played by special services and covert operations. Examples include Iran's arming of Hezbollah in Lebanon and Russia's weapons supply to Syrian leader Bashar al-Assad.

- **NON-STATE ACTORS.** Employing proxy groups instead of regular military forces. An instance is the involvement of the Russian PMC 'Liga' (formerly 'Wagner') in conflicts in Latin America, Africa, and the Middle East.

- **INFORMATION.** Generating internal public controversies via propaganda, false news, and misinformation. ISIS, for example, uses information campaigns to recruit new members to its terrorist network.

Among these elements, the information aspect is the most critical and effective in hybrid warfare. It is the hardest to counter yet can yield desired outcomes without military engagement. This manual focuses on developing strategies to combat the primary tools of Russian information warfare – propaganda, disinformation, and manipulation.

Information warfare involves information influence methods, which can

be destructive communication forms used by foreign states or their agents. These methods aim to disrupt trust between a government and its citizens by interfering in internal affairs, advancing foreign state interests by exploiting societal vulnerabilities to cause polarization and destabilization[3].

Since the early 2000s, Russia has been actively engaging in hybrid warfare, particularly utilizing its information component, against Western nations and neighbouring countries. The doctrinal basis of this approach was shaped in 2013 when Valery Gerasimov, the Chief of the General Staff of the Russian Armed Forces, published an article titled 'The value of science in foresight.' The concepts outlined in this

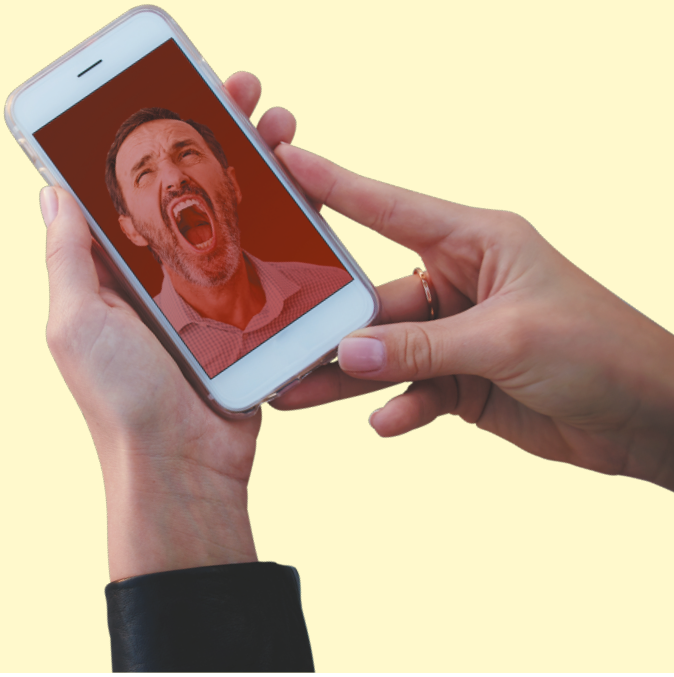
article were later termed the 'Gerasimov doctrine'. This article presented a novel perspective on warfare, the fundamental tenet being the employment of non-traditional military tactics – such as economic pressure, covert diplomacy, information warfare and the promotion of separatism – instead of directly invading another state's territory, to accomplish primary political objectives. This doctrine has been actively applied against Ukraine since 2014[4].

Russian military doctrine perceives hybrid warfare distinctively compared to other nations. In Russia's view, hybrid warfare isn't merely a collection of specific tactics; rather, it's seen as a type of conflict where all means, including military operations, are integral parts of a unified information campaign. In essence, Russia engages in warfare that targets the mindset and consciousness of the adversary.

Russian analysts consider the aim of hybrid warfare to be the capability to influence the long-term governance and strategic direction of another state. From Russia's perspective, the victors in hybrid conflicts effectively impose their world-view, values, interests, and notions of 'fair' resource distribution on the defeated. Consequently, the winning states gain power and, in the Russian view, earn the right to shape the future of the other country. This approach emphasizes the importance of psychological and informational dominance in modern conflict scenarios[5].

In light of Russia's objectives in its hybrid warfare, the primary method for achieving political ends is through information and psychological operations (IPsO), which encompass propaganda, the spread of fake news, and disinformation.

AN INFORMATION AND PSYCHOLOGICAL OPERATION (IPSO) is a series of actions designed to shape beliefs and attitudes within a broad or hostile audience. The aim is to weaken their resistance, thereby aiding the attainment of military objectives. Typically, IPsO applies psychological pressure on society, incites panic, and erodes trust in governmental institutions.



[3] Countering information influence activities. A handbook for communicators (Digital resource)

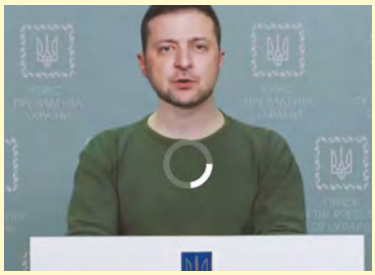
[4] Molly K. McKew. The Gerasimov Doctrine. It's Russia's new chaos theory of political warfare. And it's probably being used on you (Digital resource)

[5] Mason Clark. Russian Hybrid Warfare (Digital resource)

At the onset of the full-scale war in 2022, a notable Russian IPsO (Information and Psychological Operation) involved mass tagging and placing obscure devices on civilian infrastructure in Ukraine. Predominantly Ukrainian citizens were recruited for this, lured by Russian special service curators through messengers with offers of monetary rewards. Concurrently, Russian disinformation propagated the narrative that these tags and devices were used to guide air, missile, and artillery strikes in Ukraine and assist Russian troops in navigating the terrain.

The primary aim of this operation was to instill panic and chaos among Ukraine's civilian population. Furthermore, Russian propagandists sought to convey the impression that many in Ukraine were willing to betray their country for money, while diverting attention from real Russian saboteurs and collaborators, thus enabling them to conduct their subversive activities more freely.

In the temporarily occupied territories, Russian IPsO efforts are intense. Propagandists spread the narrative that the disconnection of Ukrainian mobile communications in the Kherson region was orchestrated by Ukrainian authorities, fostering a sense of abandonment among the remaining population.



Another example of Russian IPsO targeting the Ukrainian population was the hacking of the 'Ukraine 24' TV channel's news feed. Hackers posted a false statement purportedly from Ukrainian President Volodymyr Zelensky about the country's surrender, aiming to demoralize Ukrainians and erode their trust in the government.

To demoralize the Armed Forces of Ukraine, various IPsO tactics are employed. Soldiers' relatives receive calls providing false information about the military's status and location.

Additionally, Ukrainian soldiers often receive SMS messages with threats that Russians allegedly know their specific locations and personal data.

Traditional propaganda methods are also employed in these areas, including public surveys to gauge sentiments, support for staged 'humanitarian actions', and direct communication with locals. Information materials like leaflets and newspapers are distributed, and collaborators are recruited in coordination with FSB/GRU officers. These 'freelance employee' collaborators, paid around 70,000 rubles, are involved in organizing and participating in propaganda actions, disseminating pro-Russian content on social networks and other channels.

HOW DOES RUSSIAN PROPAGANDA WORK?

Russian propaganda began to exhibit its current characteristics following Ukraine's 'Orange Revolution' in 2004. It marked a shift where the Kremlin's propaganda efforts were no longer targeted at individual persons or entities but directed against an entire state. This approach's effectiveness was further honed during the Russian-Georgian war in 2008 and became more following the illegal annexation of Crimea and the aggression in Eastern Ukraine.

The events of February 24, 2022, catalysed a further transformation in Russian propaganda, leading it to become even more aggressive, revanchist, and radical. This change reflects an escalation in the intensity and scope of Russia's information warfare strategies.

In Ukraine, the target audience of Russia's Information and Psychological Operations (IPsO) includes the pro-Russian population across various regions, with a particular focus on Russian-speaking citizens, civil servants, the intellectual elite, and older individuals. This targeting strategy reflects a nuanced understanding of the societal and demographic landscape in Ukraine, aiming to influence specific groups that might be more receptive to Russian narratives and objectives.

Five distinctive features characterize the current model of Russian propaganda:

- **High volume and multichannel;**
- **Speed, persistence and repetition;**
- **Detachment from objective reality;**
- **Lack of consistency;**
- **Narrativisation.**

1 HIGH VOLUME AND MULTICHANNEL

The Kremlin's approach to propaganda leverages the psychological tendency of people to align with the majority view, even if it is incorrect. To exploit this, Russia has established a vast network dedicated to disseminating propaganda. This network includes television channels, news agencies, online publications, social networks, and even troll factories* and bot farms**. The sheer volume of information and the variety of channels through which it is transmitted enhance the credibility of the main propaganda narratives for the intended audience.

RT (formerly known as Russia Today) stands as one of Russia's primary multimedia news providers, operating with an annual budget exceeding $300 million. The media holding broadcasts in various languages, including English, French, German, Spanish, Russian, and several Eastern European languages. Notably popular online, RT has amassed over a billion page views on the internet, potentially making it the most popular news source on the web. Additionally, there are numerous proxy news sites that disseminate Russian propaganda while either concealing or downplaying their connection to Russia.

On February 26, 2022 the Security Service of Ukraine successfully identified and dismantled a Russian 'bot farm' responsible for war propaganda through around 7,000 accounts. In 2021, another 'bot farm', operated from the Russian Federation, was discovered. This network, consisting of over 5,000 accounts, was primarily focused on undermining the coronavirus vaccination efforts in Ukraine.

The Security Service of Ukraine (SBU) has published a list of Telegram channels disseminating Russian propaganda in Ukraine. Among them are such well-known channels as 'Legitimate', 'Resident', etc.

Also, after the start of a full-scale war, Russian propagandists created many new Telegram channels for the temporarily occupied territories (Kherson, Melitopol, Berdyansk, etc.) and cities where hostilities were or are being conducted (Kharkiv, Chernihiv), through which they conduct their IPsO and actively disseminate disinformation and fakes.

2 SPEED, PERSISTENCE, AND REPETITION

Russian news websites and television channels often quickly report on certain events. This rapid coverage is usually due to the news being fabricated or pre-scripted as per governmental guidelines. The initial information a person hears, especially if corroborated by other sources, tends to be more believable to them. Thus, even when they later encounter accurate news, they are likely to adhere to the earlier narrative they heard repeatedly.

This tendency is rooted in a psychological concept known as confirmatory bias.

CONFIRMATORY BIAS is the inclination to search for or interpret information in a way that reinforces one's pre-existing beliefs or theories, and to overlook or undervalue information that contradicts these beliefs.[7]

A sociological survey in Russia underscores the phenomenon of confirmatory bias, revealing that 89% of Russians believe the aims of the 'special military operation' are to protect Donbas's civilians, avert an attack on Russia, and 'denazify' Ukraine. This bias is also evident in the widespread belief that Western countries are instigating Ukraine into war, ignoring Russia's unprovoked and unjustifiable invasion of Ukrainian territory.

Russian propagandists are often the first to appear on the scene, which creates the illusion of 'exclusive information from the source.' In particular, this happens after shelling and explosions. This immediacy often leads to suspicions that some reports might be staged.

A prominent example of the continuity and repetitiveness in Russian propaganda is the persistent myth that 'the Ukrainian Armed Forces have been bombarding Donbas and killing children for eight years.' This narrative has deeply embedded itself in the Russian psyche over the past eight years and is now being used by Russian authorities to justify the full - scale invasion of Ukraine and the war crimes committed by the Russian military. They frame this as 'retribution for eight years of shelling of Donbas,' adhering to a tit-for-tat rationale. Russian media portrays this as a form of 'vengeance for the prolonged bombardment of Donbas.'

---

* **Troll factories** refer to groups of social media and forum users who post comments and content on various online platforms with the intent of spreading disinformation and propaganda, often for monetary compensation. These users actively participate in manipulating public opinion and discourse.

** **Bot farms,** on the other hand, involve the creation of large numbers of fake social media accounts that post thousands of comments, typically negative. These comments are aimed at discrediting individuals, events, or stirring up hatred. By flooding social media and online spaces with these orchestrated messages, they aim to skew public perception and create a false sense of consensus or widespread opinion. This multifaceted strategy is key to the effectiveness of Russian information warfare, as it targets the psychological inclination of individuals to conform to perceived popular opinion.

[6] **Christopher Paul, Miriam Matthews. The Russian «Firehose of Falsehood» Propaganda Model** (Digital resource)

[7] **Joshua Klayman and Young-Won Ha. Confirmation, Disconfirmation, and Information in Hypothesis Testing** (Digital resource)

3 DETACHMENT FROM OBJECTIVE REALITY

Russian propaganda frequently includes misinformation and falsehoods. There's no necessity for the Russian Federation to alter facts when they can easily fabricate news and present it through a credible source.

Examples of detachment from objective reality can be Russian disinformation narratives about 'war drugs used by servicemen of the Armed Forces of Ukraine for fearlessness', 'training of Satanist units for war with Russia', 'mosquitoes and migratory birds that purposefully carry dangerous diseases adapted to the Slavic ethnos in biological laboratories of Ukraine'.

Among other classic examples of Russian propaganda, one can mention fakes about the alleged canonization by the Orthodox Church of Ukraine of Stepan Bandera, who was a Greek Catholic, and the creation of a separate gay battalion 'Blue Tornado' from representatives of the LGBT community on the basis of the 80th Brigade of Air Assault Troops of the Armed Forces of Ukraine.

4 LACK OF CONSISTENCY

Inconsistency is paradoxically a key trait of Russian propaganda. Various media outlets may relay differing narratives on identical subjects. Additionally, the same Russian sources often shift their stance or message. Yet, surprisingly, this inconsistency doesn't lead to a loss of trust among consumers.

A vivid example of the inconsistency of propagandists was the very different and colorful messages about the explosion of the Russian ammunition depot in Nova Kakhovka on July 11, 2022.

5 NARRATIVISATION

Despite occasional inconsistencies in specific messages, Russian propaganda maintains steady overarching narratives. Take, for instance, the tale of a grandmother with a red flag, widely spread by Russian media and subsequently debunked by Ukraine's Centre for Strategic Communication and Information Security. The core narrative aimed to depict the Ukrainian populace as supportive of Russian invaders. However, details within this narrative varied. The grandmother was said to be from the Kyiv region in one instance, then the Donetsk region in another. After her interview denying allegiance to Russia, the propaganda narrative splintered, with claims ranging from her abduction by Ukraine's Security Service to accusations of her being a Ukrainian nationalist.

Russian propaganda often simultaneously propagates conflicting messages, further polarizing society. During Ukraine's peak COVID-19 crisis and vaccine rollout, Russian-operated bots and trolls on social media simultaneously accused the Ukrainian government of both enforcing harmful mandatory vaccinations and failing to vaccinate the population swiftly enough.

Russia's propaganda efforts extend beyond polarizing Ukrainian society to influencing the population of the European Union. In Germany, Russian support is evident for ideologically opposing parties, the ultra-right 'AfD' (Alternative for Germany) and the ultra-left 'Die Linke'. Despite their ideological differences, representatives from both parties have consistently echoed Russian propaganda narratives and justified Russian aggression against Ukraine. Notable instances include speeches made in the Bundestag by Alice Weidel, co-chairwoman of the 'AfD' parliamentary faction, and Sarah Wagenknecht, a former co-chair of the Die Linke party and a member of the Bundestag.

> Russian propaganda operates via a so-called chain of disinformation encompassing four distinct categories: **LEADERSHIP, PROXIES, DISTRIBUTION CHANNELS, AND CONSUMERS.**

THE FIRST CATEGORY in the chain – leadership – comprises the political and military elite of the Russian Federation, such as President Vladimir Putin, Chief of the General Staff of the Armed Forces Valery Gerasimov, and Foreign Minister Sergei Lavrov, among other top officials. This political-military echelon of Russia is the principal originator of disinformation campaigns, targeting not only domestic audiences but also the international community. The manipulative statements made by Russia's Permanent Representative to the United Nations, Vasily Nebenzia, during UN Security Council meetings, Vladimir Putin's remarks in calls with global leaders, and Sergei Lavrov's interviews are prime examples of the initial sources of Russian propaganda.

THE SECOND CATEGORY in the disinformation chain comprises proxies responsible for executing Russian propaganda campaigns. These organizations, depending on their relation to the Russian government, fall into three types.

1. Entities affiliated with the highest levels of Russian authority, such as the FSB and the GRU of the Russian Ministry of Defence.

2. Organizations not formally connected to the government but effectively controlled by it due to state budget financing. Prominent examples include RT (formerly Russia Today) – the Russian state television company, and the Sputnik news agency.

3. Bodies whose ties to the Russian government are concealed, like the Internet Research Agency, also known as the St. Petersburg Troll Factory. Based in St. Petersburg, it promotes disinformation primarily through social media channels.

THE THIRD CATEGORY is distribution channels, with social networks like Facebook, Twitter, and Telegram playing pivotal roles. These platforms enable Russia to spread disinformation via bots, trolls, and various online communities, channels, and groups, reaching vast audiences.

THE FOURTH AND LAST CATEGORY consists of the consumers. This group includes diverse population segments from different countries, targeted by the Russian Federation's information campaigns. They range from ordinary citizens to business people, politicians, and opinion leaders.

Russian propaganda's **PRACTICAL MECHANISMS** include a mix of direct and indirect influence forms. Experts generally categorize these into **POSITIVE** (creating a favourable image of Russian authorities) and **NEGATIVE** (spreading falsehoods, manipulating facts). In terms of content, it's divided into disorienting, defensive, and aggressive.

DISORIENTING CONTENT aims to dismantle the notion of truth, suggesting that objective reality doesn't exist, and hence, no institutions, especially governmental ones, are trustworthy. Domestically, defensive content strives to portray the Russian authorities as protectors of their people, presenting them as the sole viable option. In contrast, its external counterpart, particularly targeting Ukraine, focuses on discrediting the current establishment. Familiar narratives about an 'aggressive West' seeking to undermine a 'peaceful and prosperous Russia' fall into this category.

AGGRESSIVE content, structurally similar to defensive, contains emotionally charged messages about protecting the 'Russian world' from 'American capture', rescuing Ukraine from the clutches of the 'fascist junta', 'Soros', 'Dempartia', 'Gayropa', and similar entities.

Since 2020, these content categories have taken on a more aggressive tone. The change reflects Russian consumers' dissatisfaction with media content focused on Ukraine and America, growing grievances about rights and freedoms oppression, the deteriorating state of the healthcare and social sectors, and the declining regime rating amid the COVID crisis. This led to a shift towards a disorienting approach, suggesting the state leadership as the sole bearer of truth, urging trust only in authorities and no one else[8].

Post February 24, 2022, security and aggressive content in Russian propaganda converged with a singular aim to justify Russia's unprovoked invasion of Ukraine. The propaganda now intensifies by demonizing the West, assigning blame to Ukraine, and emphasizing the protection of Russian values.

Since that date, Russian propaganda has been pushing three key narratives that align with the military invasion of

Ukraine. The first narrative highlights **THE SUFFERING OF ORDINARY RUSSIANS DUE TO SANCTIONS,** portraying them as 'naïve and innocent' victims. This narrative aims to spark debates in Western countries about the appropriateness of sanctions.

The second narrative reframes **THE INVASION OF UKRAINE AS A 'MILITARY OPERATION' AND NOT A WAR.** Russia deliberately avoids labelling its actions in Ukraine as warfare, opting instead for 'special military operation'. This terminology is echoed in some Western media, which prefer terms like 'crisis' or 'conflict' over 'war'. This approach is an attempt by the Kremlin to sidestep international legal accountability for acts of aggression and to rationalize the war of conquest to its domestic audience.

The third narrative is one of **UKRAINOPHOBIA.** Russian media depict the Ukrainian military as neo-Nazis and war criminals and portray Ukrainian refugees as ungrateful, aggressive migrant workers. Moreover, Russian propaganda seeks to diminish Ukraine's historical and cultural heritage, casting doubt on the legitimacy of its statehood. This narrative aims to convince the West that Ukraine does not merit support as it is not a truly sovereign state, and its population is not seen as civilized[9].

---

[8] **Joshua Klayman and Young-Won Ha. Confirmation, Disconfirmation, and Information in Hypothesis Testing** (Digital resource)

[9] **Anna Romandash. Russian propaganda is affecting you more than you think** (Digital resource)

THE DETRIMENTAL IMPACT OF RUSSIAN PROPAGANDA

WHY FIGHT IT?

Russian propaganda, considering its objectives and methods, exerts a negative influence on societies abroad. Its primary impact is the **DESTABILIZATION** within other states, achieved chiefly by **EXPLOITING EXISTING SOCIETAL VULNERABILITIES.** For instance, continuously stirring debates over the dual language issue in Ukraine ultimately **WEAKENS THE UNITY OF UKRAINIAN SOCIETY, CREATING A DIVIDE** between Ukrainian and Russian speakers.

The narrative of «oppression of Russian-speaking people in Ukraine» propagated by Russian media is one of the most enduring, having been systematically spread since the early 1990s. A notable instance of this was the actions of pro-Russian activist and former Crimean president Yuri Meshkov in the 1990s. During this period, there was an initial attempt to detach Crimea from Ukraine and annex it to Russia, which ultimately did not succeed.

The tactic of artificially dividing Ukraine along linguistic and regional lines was prominently used during the contentious presidential elections of 2004-2005 and throughout Viktor Yushchenko's presidency. A prime example is the leaflet about 'three varieties of Ukrainians', allegedly authored by Russian political technologist and associate of Viktor Yanukovych, Timofey Sergeytsev. This concept was widely circulated in Ukraine during the 2004-2005 election campaign, illustrating the persistent efforts to sow division within the country.

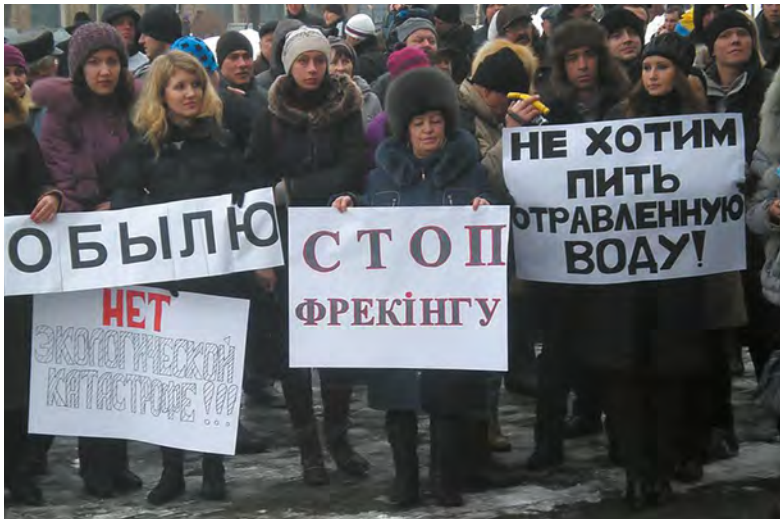
The wave of propaganda gained further momentum following several legislative developments in Ukraine. In 2017, the new 'Law of Ukraine on Education' was adopted. In 2018, the Constitutional Court of Ukraine declared the 'Kivalov-Kolesnichenko Language Law' (Law of Ukraine 'On the Principles of State Language Policy') unconstitutional. Additionally, in 2019, the 'Law of Ukraine on Ensuring the Functioning of the Ukrainian Language as the State Language' was passed. The Russian narrative on this topic continued to evolve in 2022 during the full-scale war, particularly when the Verkhovna Rada of Ukraine enacted laws restricting the distribution of Russian music in Ukraine and banned the import of books from Russia and Belarus.

The groundlessness of this propaganda theme was effectively highlighted by a sociological survey conducted in May 2022 by the Kyiv International Institute of Sociology. The survey revealed that 90% of Russian-speaking Ukrainians and 85% of ethnic Russians, who are citizens of Ukraine, affirmed that there was no oppression of the Russian language in the country.

Another method for destabilization involves eroding trust in state institutions and law enforcement agencies. The spread of falsehoods and misinformation about the actions of governmental bodies and portraying the government as deceitful undermines its legitimacy in the eyes of the populace. This strategy was executed in the territories of the so-called 'DPR' and 'LPR,' leading to strong anti-Ukrainian sentiments in the region during the events of 2014. Russian news outlets have been propagating the narrative since the late 2000s that the Kyiv authorities exploit mineral resources and extract maximum economic gains from Donbas enterprises, while deliberately keeping the living standards of the region's residents low. As a result, a belief has taken root among some people in the Donetsk and Luhansk regions that they 'feed all Ukraine', but live in poverty themselves due to exploitation by the government.

A notable instance occurred in 2013 with mass protests against shale gas extraction in the cities of the Donetsk region. Investigative journalist Hristo Grozev revealed that these protests were funded by Russian special services, with backing from Viktor Mokin, the then Consul General of the Russian Federation in Kharkiv. The political backbone of the 'anti-shale' movement included members of the Communist Party of Ukraine and Viktor Medvedchuk's 'Ukrainian Choice' organization, along with the active participation of local environmental groups. Clearly, the Russian Federation and Gazprom were heavily disadvantaged by the potential surge in Ukrainian gas production, particularly involving Western companies. Intriguingly, these same protest groups played a role in early 2014, aiding the temporary occupation of Sloviansk and the conduct of an unlawful 'referendum' on the independence of the so-called 'DPR'[10].

Russian propagandists even beyond 2013 perpetuated the narrative of a 'severe environmental threat' from shale gas extraction. Protests in the Kharkiv and Donetsk regions persisted up until the onset of the full-scale invasion in 2022. These campaigns effectively employed intimidation tactics, with propaganda primarily leveraging emotional appeals to influence public opinion[11,12,13].

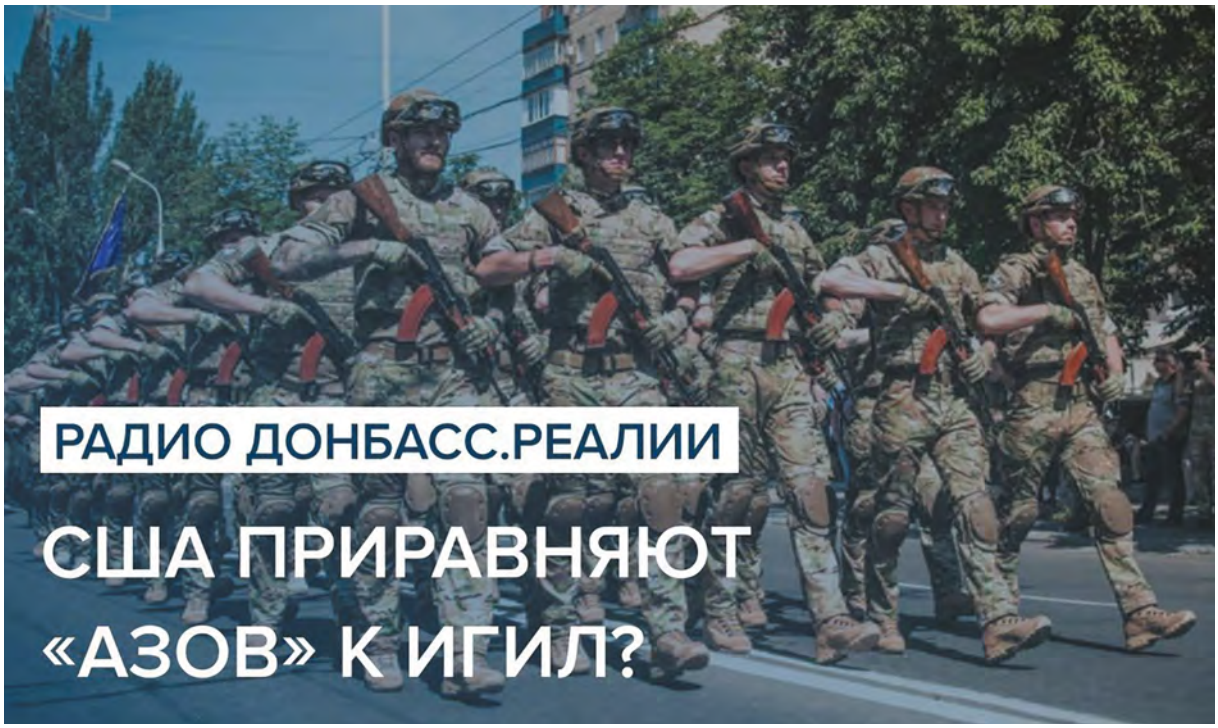


[10] Did the seizure of Sloviansk begin as protests against shale gas? (Digital resource)

[11] Ecology or treason? (Digital resource)

[12] Residents of Merefa blocked the highway for five hours in protest against shale gas extraction (Digital resource)

[13] 'Gas' protests in Donbas and inspired phobias (Digital resource)



The Russians consistently and methodically spread disinformation about the supposed atrocities and war crimes committed by the Ukrainian Armed Forces and National Guard, with a specific focus on the 'terrorist' and 'neo-nazi' connotations attributed to the Azov regiment. This is done with the aim of breeding distrust within Ukrainian society towards its own law enforcement agencies and diminishing public support for them. Such narratives are particularly prevalent in the temporarily occupied territories, disseminated through Russian-controlled media and Telegram channels. This strategy is designed to erode trust in the Ukrainian government, secure loyalty from the remaining population, and complicate the process of future reintegration.

To create a distinction within the military, Russian propaganda coined the term 'national battalions'. There's a persistent push of narratives about 'a small group of nationalist militants used as barriers against the Armed Forces of Ukraine, the National Guard, etc.' However, it is a well-established fact that all volunteer formations in Ukraine have long been integrated into the official state military structures.

The various tactics and methods of Russian propaganda underscore a key objective of Russia's information war — exerting control over the populace of another state. The Information Security Strategy of Ukraine, acknowledging the impact of Russian propaganda and disinformation, categorizes Russia's informational influence **AS A THREAT TO UKRAINE'S NATIONAL SECURITY.**

Therefore, **COMBATING AND PREVENTING RUSSIA'S INFORMATION AND PSYCHOLOGICAL OPERATIONS (IPSO) WITHIN UKRAINE IS CRUCIAL FOR ITS SOVEREIGNTY, THE EFFECTIVE FUNCTIONING OF STATE INSTITUTIONS, AND THE COHESION OF UKRAINIAN SOCIETY.**

COMBATTING RUSSIAN PROPAGANDA

The Centre for Strategic Communication and Information Security outlines a strategy to counter Russian propaganda, disinformation, and manipulation. To understand the issue better, it is essential to define disinformation, misinformation, manipulation, and fakes.

At the state level, countering hostile information influence involves several steps.

1. **BLOCKING ACCESS TO ENEMY COMMUNICATION CHANNELS.** Ukraine took this approach in 2014 by banning Russian TV channels from its cable networks. In 2017, Russian search engines (Yandex.ru) and social networks (Vkontakte, Odnoklassniki) were also prohibited. In 2021, TV channels associated with Viktor Medvedchuk, funded by Russia and echoing Russian propaganda, were shut down. These measures have proven effective, considering their potential impact had they been operational on February 24, 2022, the day of Russia's invasion of Ukraine.

2. **CREATING HIGH-QUALITY NATIONAL CONTENT.** Post-ban of Russian channels and social networks, Ukraine began supporting the development of pro-Ukrainian and Ukrainian-language media, including music, cinema, television, book publishing, and other sectors.

3. **MEDIA LITERACY.** Educating the populace to independently recognize and counteract hostile information, especially those that slip through the initial two filters.

This understanding of the importance of countering hostile information has moved from public and specialized initiatives to the state level. The Centre for Strategic Communication and Information Security, under the Ministry of Culture and Information Policy of Ukraine, was established. The fight against disinformation and hostile propaganda is a focus across all law enforcement agencies, the Cabinet of Ministers, the Office of the President, and the Verkhovna Rada of Ukraine.

- **DISINFORMATION** is the intentional spread of false information to harm an individual, organization, or state.
- **MISINFORMATION** is the spread of false information without malicious intent.
- **MANIPULATION** involves using information (true or false) to influence people.
- **A FAKE** is distorted or intentionally false information.

The Centre has devised a strategy to counter disinformation and manipulation, specifically those intended to cause harm. This strategy includes several stages: detection, prevention, strategic communications, and evaluation of implemented measures. Each of these stages is detailed in the subsequent sections.

DETECTION

To effectively counter Russian disinformation and manipulation, it is crucial to ascertain if it is indeed part of the Russian information campaign. Various methods can be employed for this purpose.

METHOD 1. IDENTIFICATION BY CHARACTERISTICS

Russian disinformation typically exhibits certain key traits, which, when identified, suggest its affiliation with the information war waged by the Russian Federation. These characteristics include.

- **PURPOSEFULNESS.** Evidence of orchestration, with clear intent.
- **ELEMENT OF FALSEHOOD.** Inherent untruthfulness in the content.
- **IMITATION.** Presentation as credible information.
- **TARGETED AUDIENCE IMPACT.** Aimed at influencing a specific group through disclosure.
- **NEGATIVE (SOCIALLY HARMFUL) OUTCOMES.** Potential to cause societal harm.
- **CONNECTION TO SIGNIFICANT EVENTS.** Often relates to socially impactful or symbolically valuable information.

EXAMPLE 1

Claims of the Ukrainian Armed Forces 'shelling' Mykolaiv in conjunction with Russian missile strikes.

PURPOSEFULNESS. The organizer is the Russian propaganda media 'Rusnext', with apparent intent.

ELEMENT OF FALSEHOOD. The report is entirely false, as the Ukrainian Armed Forces refrain from shelling cities, even those occupied, to avoid civilian casualties. Mykolaiv, under Ukrainian control, is situated 30 km from the front line.

IMITATION. Presented as factual, citing a 'source in Mykolaiv,' claiming the majority of the city's population blames the Ukrainian Armed Forces for the shelling. The article acknowledges Russian missile attacks, but claims they target only military sites.

TARGETED AUDIENCE IMPACT. Primarily aimed at Mykolaiv's residents, extending to the populations of Ukraine's controlled regions, the temporarily occupied territories, the Russian Federation, and the pseudo-republics it illegally established in former USSR countries.

NEGATIVE CONSEQUENCES. The goal is to demoralize Mykolaiv's residents and erode Ukrainian confidence in their Armed Forces and government. This aims to tarnish the image of the Ukrainian army and obscure Russian war crimes ('shifting the blame').

CONNECTION TO SIGNIFICANT INFORMATION. Regular rocket attacks on a city of 500,000 (pre-war) mainly targeting civilian infrastructure constitute socially relevant information.

EXAMPLE 2

Russian military correspondent Alexander Sladkov claims that the Ukrainian Armed Forces are discarding Western Javelins as they are vastly inferior to Russian counterparts.

PURPOSEFULNESS. The propagator is Alexander Sladkov, a Russian war correspondent, with a clear intent.

ELEMENT OF UNTRUTHFULNESS. The claim is patently false. Javelin ATGMs have been highly effective in countering Russia's full-scale military aggression, destroying numerous enemy vehicles. These weapons, in service with the US Army since 1998, are used by 19 countries, including the UK, France, Australia, South Korea, Ireland, the Czech Republic, Norway, Lithuania, etc. The Javelin has also proven effective in conflicts in Iraq, Afghanistan, and Syria.

IMITATION. Sladkov presents his assertion as factual, claiming that any reporter at the front line would witness Ukrainian soldiers abandoning Javelins on the battlefield, purportedly for enhanced credibility.

TARGETED AUDIENCE IMPACT. The primary audience is Ukrainian servicemen and civilians, aiming to demoralize them by portraying American

weaponry as inefficient and Russian arms as superior. An indirect audience includes Russian military personnel and civilians, to boost their morale. Additionally, it targets the governments and populations of Ukraine's Western allies, suggesting their weaponry and support are subpar.

NEGATIVE CONSEQUENCES. This propaganda seeks to erode the confidence of the Ukrainian Armed Forces and populace in their victory prospects and the efficacy of Western-provided weaponry, while intimating Russian weapon superiority and casting doubt on Western support for Ukraine.

CONNECTION TO SIGNIFICANT INFORMATION. Javelins symbolize the Ukrainian Armed Forces' and people's resistance, supported by Western countries, since the onset of the full-scale war. They are featured in graffiti, murals, and even inspire children's names. Russian propagandists aim to undermine this symbol.

METHOD 2. FIRST METRICS

Developed by the UK's Government Communication Service, the FIRST metrics include:

- **FABRICATION;**
- **IDENTITY;**
- **RHETORIC;**
- **SYMBOLISM;**
- **TECHNOLOGY.**

FABRICATION. Involves manipulative content, such as forged documents, image manipulation, or intentional quote distortion.

> NGO Detector Media refuted the Russian fake that the Azov regiment was allegedly going to equip its positions in residential areas and that 70% of Mariupol residents support Russia. The 'official document' in the photo contains numerous signs of forgery, spelling and stylistic errors, unnatural linguistic constructions like 'curb', which confirm its inauthenticity.

IDENTITY. Involves hidden or misleading sources, or false claims about someone else, like fake social media accounts or behaviour inconsistent with the account's presentation.

> Russian propagandists created a fake Telegram channel of the 14th mechanized brigade named after Prince Roman the Great. In addition to pro-Ukrainian narratives, the channel also publishes blatantly false information, such as 'more than 90% of Ukrainians are against the continuation of mobilization', 'the situation of the brigade is critical', 'a gay activist joined the Kyiv defense unit', thus concealing disinformation is hidden on this channel.

RHETORIC. Are onerous tones or false arguments used?

> The fact-checking initiative 'No Lies' has debunked the Russian myth about the number of Ukrainian aircraft, helicopters and UAVs shot down by the Russian army. The fact is that the Russians cited figures (186 planes and 129 helicopters) that exceed the number of air equipment in service with the Armed Forces of Ukraine before the full-scale war (134 planes and 112 helicopters), proven by statistics of international industry publications.

SYMBOLISM. This aspect examines whether data, issues, or events are employed to attain a communication objective unrelated to them. Examples include historical events taken out of context, use of irrelevant facts to support conspiracy theories, or manipulation of statistics for purposes other than their original context or significance.

> A good example of this indicator is the words of President Putin on December 23, 2021, that Ukraine was allegedly created by Bolshevik leader Vladimir Lenin. The obvious manipulation of historical examples taken out of context.

TECHNOLOGY. Are technologies used as communication measures for the purpose of misleading, for example, bots, deepfakes, spam, etc.

> Russian hackers created a deepfake of Kyiv Mayor Vitali Klitschko and held 20-minute conversations on his behalf with the mayors of five capitals of the European Union. The attackers managed to mislead the mayors of Warsaw and Vienna, but the mayors of Berlin, Madrid and Budapest identified deepfakes by some indirect features.

METHOD 3. ALIGNING TARGET AUDIENCES WITH STRATEGIC NARRATIVES

Russia's information campaigns typically comprise multiple narratives, each specifically targeted at certain population segments or society as a whole. Identifying these narratives and discerning their intended audience is crucial for understanding the nature and scope of the threat posed by Russia's harmful information activities.

The Swedish Civil Protection Agency has outlined three methods to identify strategic narratives based on the nature of their messaging.

1 POSITIVE OR CONSTRUCTIVE. 'IT'S TRUE!'

This approach seeks to craft a cohesive narrative around a particular issue, aiming to integrate, enhance, or build upon pre-existing, well-established strategic narratives. An example is the Russian disinformation narrative about the alleged presence of NATO biolaboratories on the territory of Ukraine and the creation of biological weapons in them. It complements and expands strategic narratives that Ukraine is a puppet of NATO countries and together with them threatens Russia's national security. The continuation of this narrative is the news that dangerous infectious diseases were allegedly found in the blood of Ukrainian prisoners of war, and therefore they were subjected to biological experiments.

2 NEGATIVE OR DESTRUCTIVE. 'THIS IS A LIE!'

Attempts to prevent the emergence of an opposing narrative or to refute or undermine an existing narrative.

A good example of this method of identification is the Russian disinformation narrative that the massacre in Bucha was allegedly staged by the Ukrainian authorities. This is done in order to shift responsibility for the atrocities of the Russian occupation army onto Ukraine and whitewash its reputation before the international community, which was shocked by the footage from Bucha.

3 DISTRACTION 'LOOK HERE!'

Russian propagandists actively diverted the attention of the international community from the massive theft of Ukrainian grain in the temporarily occupied territories. They employed a counter-narrative incorporating elements of a 'conspiracy theory', claiming that the United States and Poland were taking grain from Ukraine, thereby causing starvation among the population. Additionally, they propagated the narrative that Ukrainian grain exports predominantly benefited developed Western countries, rather than aiding developing nations facing food shortages. The threats to end the 'grain deal', possibly intended to restart ammonia transit through Ukraine, might also be part of this narrative strategy.

Another part of this counter-narrative involves manipulative statements by Russian high-ranking officials downplaying the share of Ukrainian grain in the global balance. They also sought to convince international audiences that the conflict in Ukraine would have negligible effects on global food security.

In essence, Russian strategic narratives serve three fundamental purposes. They either construct an alternate reality through affirmation, undermine the validity of other narratives via denial, or reduce the significance of competing narratives by shifting focus away from their core message.

Regarding the target audiences for these strategic narratives, they are categorized by their scale and scope, encompassing the following groups.

GENERAL PUBLIC: BROADEST POSSIBLE AUDIENCE

Information impact is directed at society as a whole, synchronizing messages with widely relatable narratives and shared experiences.

SOCIODEMOGRAPHIC TARGETING. TARGETING SPECIFIC GROUPS

Based on demographic factors like age, income, education level, ethnicity, etc. The messaging is then customized to resonate with the identified demographic group.

PSYCHOGRAPHIC TARGETING.

This strategy targets individuals. By analysing and classifying large sets of data, efforts are made to influence a particular individual whose behaviour is intended to be altered.

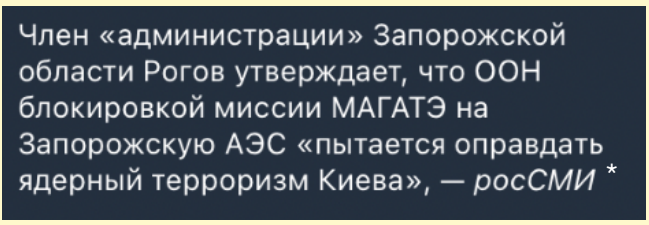
Typically, Russian disinformation is aimed at the general public as this strategy enables quick destabilization with minimal resource allocation towards audience segmentation.

To ascertain whether a piece of information is indeed Russian disinformation, it often requires a combination of the methods outlined above. While disinformation is relatively straightforward to identify, pinpointing its source can be more challenging. To confirm Russian origins, one should compare the messages and narratives against the Kremlin's main objectives discussed in prior chapters. If the disinformation or manipulation paints Russia in a positive light, denies the criminal activities of its government, or seeks to foment discord within Ukrainian society, there's a 98% likelihood that it's part of a Russian information campaign.

HOW TO DETECT A FAKE ON SOCIAL NETWORKS?

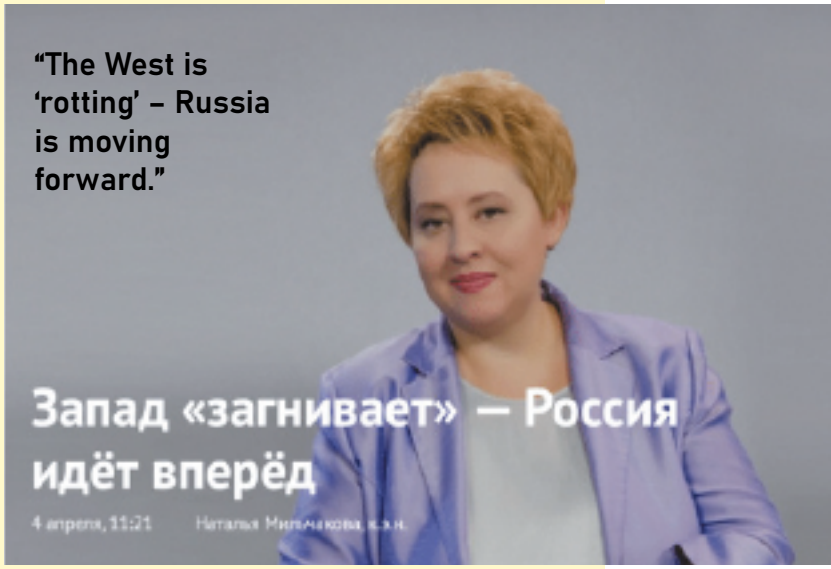
To identify a fake on social networks, consider these characteristics of the source.

SOURCE. The absence of a credible information source, anonymity, unreliability, and political bias are key indicators of potential fakery.



EXPERTISE. Fakes are often based on the words of certain experts, representatives of structures that do not really exist. If a news or post mentions an expert's opinion without mentioning the institution, whether an expert is anonymous or politically biased, then thi s is most likely a fake or manipulation.

EMOTIONS. If a news story or post evokes a strong emotion, it may indicate that the information is false or being misrepresented.



THE WAY INFORMATION IS PRESENTED. Fakes or manipulations have a characteristic way of presenting: sociological data without specifying specific figures; one-sided presentation of facts, assessments and comments, generalization; distorted presentation of news; false photos, videos used to confirm information; incorrect or distorted translation of quotations, comments from foreign sources.

*A member of the [Russian] 'administration' of the Zaporizhzhia region, Rogov, claims that the UN by blocking the IAEA mission to the Zaporizhzhia nuclear power plant 'is trying to justify Kyiv's nuclear terrorism' – Russian media.

PREVENTION

The most effective strategy to counter Russian disinformation is to prevent its spread at the initial stages of IPsO. The Centre for Strategic Communication and Information Security under the Ministry of Culture and Information Policy of Ukraine suggests several measures to inhibit the dissemination of Russian narratives among a specific organization's target audience.

DEVELOPING MEDIA LITERACY

To effectively counter Russian propaganda and disinformation, efforts should focus not just on **COMBATING THE PHENOMENON, BUT ON OBSTRUCTING THE ACHIEVEMENT OF SPECIFIC OBJECTIVES OF THE RUSSIAN INFORMATION CAMPAIGN.** This involves making the target audience 'resilient' to narratives and falsehoods propagated by Russian sources.

Campaigns aimed at enhancing media literacy and critical thinking skills in the target audience are vital in mitigating the adverse effects of disinformation. This effectiveness is supported by research from the US research institute the RAND Corporation, which indicates that post- implementation of media literacy programs, social network users have shown a reduced positive response to Russian sources, regardless of their ideological leanings.

> **MEDIA LITERACY** encompasses the capacity to employ critical thinking to assess media-produced messages, signs, and symbols.

This skill set aids in identifying, analysing, and evaluating negative or false messages distributed across various communication channels. The broader the audience equipped with media literacy skills, the more challenging it becomes for Russian propaganda narratives to infiltrate society.

THE PRIMARY METHOD FOR FOSTERING MEDIA LITERACY INVOLVES CONDUCTING EDUCATIONAL CAMPAIGNS AND TRAINING. In Ukraine, such initiatives are led by IREX (International Research and Exchanges Council), which launched the 'Learn to Discern' project in 2015. Following its success in Ukraine, the project expanded to over 12 countries worldwide. 'Learn to Discern' has trained more than 400 media literacy trainers and involved over 20,000 adults, including teachers, higher education educators, civil servants, journalists, community leaders, and public activists.

In Ukraine, the project focuses on teaching educators to incorporate infomedia literacy into their curriculum. Consequently, over 84,000 students are currently benefiting from enhanced lessons developed with the project's assistance. The project's experts have also created a free online media literacy course, Very Verified, which is available in three languages.[15]

BUILDING TRUST. Specific segments of the population often share similar preferences, interests, and values, leading to a common set of communication channels that a particular target audience frequents and trusts. In this context, for a given target audience, it is crucial to establish oneself as a credible and legitimate source, more trustworthy than other communication channels.

THE FOUNDATION FOR BUILDING TRUST LIES IN CREATING A POSITIVE IMAGE. Key elements of a positive image include having

- **A SIZABLE AUDIENCE**
- **A VERIFIED PROFILE ON SOCIAL NETWORKS**
- **AN UNBLEMISHED REPUTATION**
- **EFFICIENCY**

LARGE AUDIENCE

Users often place their trust in information sources that attract a large following. To achieve this, messages should be varied, creative, and engaging. They need to captivate, include, and make a lasting impression. The appeal of the messages is enhanced by their design. Incorporating specialized videos, stories, and interactive elements can make them more engaging. Inclusivity in messaging means reaching the broadest possible audience, irrespective of age, gender, and beliefs. This can be accomplished through a specific tone of voice, which is the unique manner a communication channel uses to relay information to its audience, and by focusing on relevant topics. Lastly, the sustainability of a message is gauged by the duration and intensity of its impact on the potential reader's memory.

VERIFIED SOCIAL MEDIA ACCOUNTS

To prevent the emergence of counterfeit duplicates and bolster trust among the target audience, the Centre for Strategic Communication and Information Security under the Ministry of Culture and Information Policy of Ukraine advises securing a 'verification badge' on social networks or featuring a link to the genuine profile on its official website. Moreover, it is important to avoid one-directional communication; instead, engaging in dialogue with the audience is crucial. This approach fosters a sense of interaction and provides the audience with opportunities to be heard and acknowledged.

MAINTAINING A CREDIBLE REPUTATION

Maintaining an unblemished reputation involves adhering to an informal code of ethics, which includes not spreading disinformation, inciting violence, or engaging in hate speech. These principles, essential for conducting a communication campaign, are detailed in the Code of Ethics for Ukrainian Journalists. Key elements of effective communication also encompass transparency, truthfulness, openness, fairness, and accuracy.

Publishing exposed fakes can significantly damage the target audience's trust and adversely impact the future reputation and operations of the organization. Even if the news is seemingly

---

[14] **Todd C. Helmus, James V. Marrone, Marek N. Posard, Danielle Schlang. Russian Propaganda Hits Its Mark. Experimentally Testing the Impact of Russian Propaganda and Counter-Interventions** (Digital resource)

[15] **Katya Vogt. What we learned about building resilience to manipulative information from Learn to Discern** (Digital resource)

positive for Ukraine, such as fabricated reports (e.g., the death of the Gauleiter of the occupied Kherson region Volodymyr Salda, premature reports of the capture of the village of Kyselivka near Kherson by Ukrainian forces, or a referendum in Russia's Belgorod region), it can be detrimental and threaten the reputation of Ukrainian state bodies and media.

A case in point is the controversy surrounding the former Commissioner for Human Rights of the Verkhovna Rada of Ukraine, Liudmyla Denisova. An independent journalistic investigation found that Lyudmila Denisova disseminated false information about the rape of Ukrainian children and women by Russian occupiers. This led to diminished public trust in the Human Rights Commissioner's office and provided Russian propaganda with new material to attempt to rehabilitate its image[16].

EFFICIENCY

In today's information landscape, the speed at which information is published is critically important. Swiftly covering an event or providing an appropriate and timely response can captivate a wide audience, thereby enhancing their trust. The battle for trust among various channels and information sources often resembles a 'zero-sum game', where an increase in trust for one source typically corresponds with a decrease in trust for another. This dynamic makes it essential to actively vie for public trust, aiming to diminish the potential scale of influence that Russian propaganda might have.

STRATEGIC COMMUNICATIONS

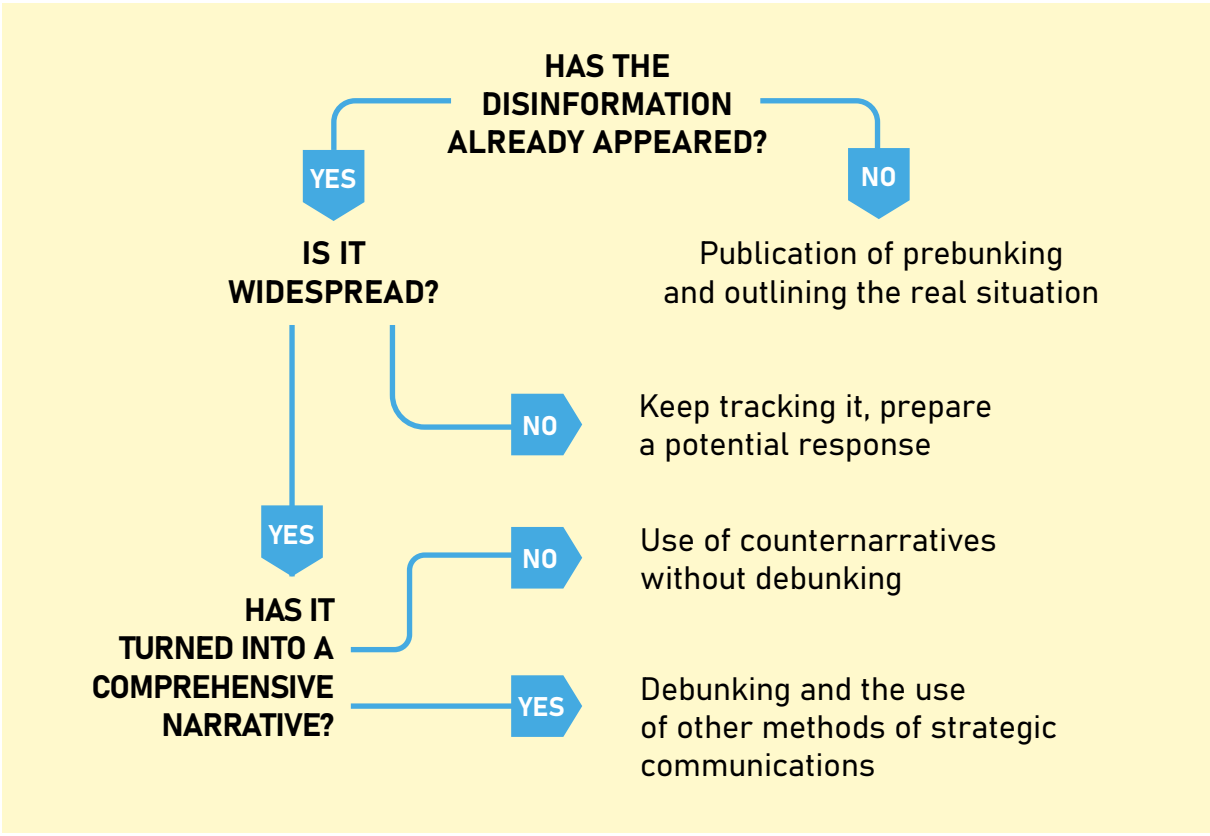
After identifying Russian disinformation, it's essential to devise methods to counteract it. A fundamental tool in this endeavour is the consistent application of strategic communication principles, methods, and channels.

Initially, it's vital to assess the need for such actions. Not all fakes or pieces of disinformation warrant a response. If the misinformation poses no significant threat to the organization's operations or its audience, addressing the fake could potentially exacerbate the situation by inadvertently reinforcing it. This is because the constant repetition of false information, even in the context of debunking, can embed it in the audience's minds as truth. This effect stems from the psychological principle that repeated information becomes familiar, and the human brain is more inclined to trust familiar information.

Therefore, it's crucial to judiciously evaluate which fakes and disinformation need addressing, based on their potential impact on the audience. The Centre for Strategic Communication and Information Security suggests a framework for determining the necessity of countering disinformation.

- If disinformation hasn't yet appeared, preemptively inform the audience about potential disinformation and clarify the actual situation.

- If disinformation has emerged but hasn't spread, continue monitoring and prepare a potential response.



▶ If disinformation has appeared and started to spread widely, but these are isolated messages that haven't formed into a narrative or align with existing general narratives, employ counter-narratives without direct refutation

▶ If disinformation has already surfaced and begun to spread broadly, and some messages have evolved into a narrative, actively refute them and utilize other strategic communication methods.

NARRATIVE. This refers to a general, simplified depiction of a particular issue that shapes a certain viewpoint for the potential reader.

MESSAGE. A fundamental component of a narrative, pertaining to a specific phenomenon, event, or situation.

The European Parliament's Research Service recognises[17] disinformation as a crucial element of hybrid threats, with strategic communications being a primary and effective countermeasure. The concept of 'strategic communications' has various definitions. In Ukraine's Military Doctrine, it's defined as **'THE COORDINATED AND APPROPRIATE USE OF THE STATE'S COMMUNICATIVE CAPABILITIES — PUBLIC DIPLOMACY, PUBLIC AFFAIRS, MILITARY PUBLIC AFFAIRS, INFORMATION AND PSYCHOLOGICAL OPERATIONS, IN SUPPORT OF FURTHERING THE STATE'S OBJECTIVES'.**

---

[16] Sonia Lukashova. Did Ombudsman Denisova Lose Her Position because of Facebook Posts? (Digital resource)

[17] Panel for theFuture of Science and Technology. Strategic communications as a key factor in countering hybrid threats (Digital resource)

KEY CHARACTERISTICS OF STRATEGIC COMMUNICATIONS:

- Implemented based on a structured and systematic plan, not merely in reaction to specific events.
- Encompass actions at strategic, operational, and tactical levels.
- Developed within a competitive environment.
- Require high-level coordination and synchronization among key stakeholders.
- Necessitate identifying the target audience.
- Involve selecting the most effective communication channels.
- Aim to inform, influence, and alter the behaviour of the target audience.
- Align with the overarching goals of the organization.
- Have short-, medium-, and long-term objectives.

BASIC PRINCIPLES:

LEADERSHIP FOCUS. Organizational leaders should be involved in the approval and oversight of strategic communication implementation.

TRUTHFULNESS. Factors like accuracy, reliability, and consistency are essential in strategic communications.

UNDERSTANDING. Efforts to comprehend the culture, vision, identity, history, attitudes, behaviours, and social norms of the target audience are crucial.

DIALOGUE. An exchange of ideas among all involved parties is important.

FLEXIBILITY. Goals and methods should swiftly adapt to changing external conditions.

CONTINUITY. It is a prolonged process involving research, information gathering, analysis, planning, implementation, evaluation, and adaptation.

PERVASIVENESS. Main messages should reach as many members of the target audience as possible.

RESULT-ORIENTED Clear objectives and means for achievement are vital.

KEY COMPONENTS.

THE EXPECTED OUTCOME, AUDIENCE, MESSAGE, COMMUNICATION METHODS AND CHANNELS, AND IMPACT ASSESSMENT.

In countering Russian disinformation, the typical aim of strategic communications is to minimize the adverse effects of Russian information operations.

Russian disinformation typically targets the **BROADEST POSSIBLE AUDIENCE** (refer to 'Prevention' earlier). However, some campaigns focus on specific demographic groups. Thus, countermeasures should be directed at similarly scaled audiences.

There are three key types of strategic communication channels. **FACE-TO-FACE COMMUNICATION, MEDIA, AND SOCIAL NETWORKS.**

CHANNEL	FORMAT	AIMS	ADVANTAGES	DISADVANTAGES
FACE-TO-FACE COMMUNICATION	■ Briefing ■ Community meeting ■ Speeches at events	■ Building trust ■ Informing about pressing issues and events ■ Making ads of special importance	■ Improves reputation of the organi-zation ■ Dialogue ■ The audience feels heard and empowered.	■ Reaches a narrow audience ■ Difficult to organize in adverse conditions
MEDIA	■ Press releases ■ Interviews ■ Comment ■ Press conference	■ Clarification of the situation ■ Image improvement ■ Narrative promotion	■ Increase trust with source ■ Implemen-tation of intermediate goals of the communication strategy ■ Resource optimization	■ Risk of target audience not receiving a message

CHANNEL	FORMAT	AIMS	ADVANTAGES	DISADVANTAGES
SOCIAL NETWORKS	■ Posts ■ Stories ■ Live streams ■ Video and audio materials	■ Informing about pressing issues and events ■ Especially important ads ■ Clarification of the situation ■ Reaction to major events ■ Promotion of messages and narrative ■ Implementation of strategic goals of communication campaigns	■ Wide audience coverage ■ Possibility of feedback ■ Informing about pressing issues and events ■ Ability to track reach and impact of communication strategy	■ Risk of attack by bots and trolls ■ The probability of hacking the profile ■ Possibility of receiving sanctions from social networks for 'hate speech' or other formal violations

Strategic communication methods can be categorized into **PROACTIVE** and **REACTIVE APPROACHES.**

PROACTIVE METHODS focus on delivering accurate and timely information to the target audience before any occurrence of information manipulation. They also aim to build resilience in the audience against false narratives.

These methods include.

- **UNDERSTANDING THE INFORMATION ENVIRONMENT;**
- **COMMUNICATION STRATEGIES;**
- **RAISING AWARENESS;**
- **PRE-BUNKING;**
- **ESTABLISHING PARTNER NETWORKS;**
- **ENHANCING THE RESILIENCE OF THE TARGET AUDIENCE.**

UNDERSTANDING THE INFORMATION ENVIRONMENT

This involves using a theoretical concept that encompasses the dynamics between information conveyors and receivers, and how the audience perceives the world based on their beliefs, values, and interests. The information environment comprises three interconnected dimensions: **COGNITIVE** (Pertains to how individuals think, understand, and make decisions), **PHYSICAL** (Involves tangible entities such as individuals and organizations) and **INFORMATIONAL** (Encompasses facts, knowledge, and information.)[18].

Analysis of the information environment is needed in order to realize

the vulnerabilities of its target audience and, in accordance with this understanding, build a communication strategy, set goals and conduct events.

> Vulnerabilities are understood as the inability to withstand destructive information influence caused by social, psychological, cultural and communication shortcomings and problems. Vulnerabilities generate weakness of state, economic, social and public institutions at all levels, which can potentially impede the effective existence of state and public life.

In Ukraine, vulnerabilities are often associated with deteriorating societal security, lack of reforms, civil unrest, distrust of the government, language and identity issues, and Russia's war against our state[19].

COMMUNICATION STRATEGY

Formulating a communication strategy becomes feasible after analyzing the information environment. When creating and implementing a communication strategy, the following seven components are crucial.

1. **TARGET AUDIENCE** Understanding its needs, interests, and values.
2. **ORGANIZATIONAL GOALS.** Defining what the organization aims to achieve.
3. **COMMUNICATION GOALS.** Determining how to use communication to achieve organizational objectives.
4. **MESSAGES.** Clarifying what the organization intends to communicate to the target audience.
5. **COMMUNICATION CHANNELS** Identifying the best ways to deliver information to the target audience.
6. **TIMEFRAME.** Establishing when the messages should reach the target audience.
7. **IMPACT ASSESSMENT.** Evaluating whether the communication strategy has attained its intended results.

Often, the combat against or prevention of Russian disinformation becomes an integral part of communication strategies aiming at broader objectives.

RAISING AWARENESS

Focuses on creating a lasting understanding of a phenomenon, event, or situation in the target audience. It can be a goal within a communication strategy, achievable through training programs, public lectures and talks, dissemination of educational content, promoting self-education, and various professional knowledge and experience exchange forms.

---

[18] **U.S. Joint Chiefs of Staff, Joint Publication 3–13:** Information Operations, incorporating change 1 (Washington D. C., 2014), 1–2.

[19] **Internews Ukraine. Taming the Hydra. How to Resist Kremlin's Information Aggression** (Digital resource)

In the context of countering Russian disinformation, raising awareness might involve educating the populace about Ukraine's statehood history, the Ukrainian people's achievements to overcome a sense of inferiority, reform implementations, the Euro-Atlantic course, and the government's actions during the war.

A good example of such communications is the website of the Deputy Prime Minister for European Integration, Olha Stefanishyna. She reports on concrete steps to deepen Ukraine's cooperation with EU countries, and work on harmonizing Ukrainian legislation with European standards. Historical matters have been effectively addressed by the Ukrainian Institute of National Remembrance. This organization is dedicated to promoting scholarly knowledge of history and opposing the Russian-Soviet historical narrative. It has notably shifted Ukrainians' perspectives on their past, leading to the public condemnation of the numerous atrocities committed by both the communist and Nazi regimes in Ukraine.

PREBUNKING involves alerting the audience about the potential emergence of a disinformation message or narrative. It stands as one of the most effective strategic communication tools in countering Russian disinformation, as it can nullify the impact of an information campaign even before it commences or becomes widely spread. Anticipating the rise of Russian disinformation is possible through risk assessment and media monitoring.

> Risk assessment entails identifying which vulnerabilities within the target audience are most susceptible to exploitation by adversaries in an information campaign.

Additionally, intelligence gathered from special services can significantly aid in prebunking. However, such intelligence is typically accessible only to the highest echelons of state structures and is often not publicly disclosed.

The Defence Intelligence of Ukraine regularly publishes warnings on its pages about new waves of Russian IPsO, manipulations, fakes and disinformation.

Thus, in August 2022, Ukrainian intelligence officers published information about Russian propagandists preparing to launch a fake website allegedly of the Volodymyr Zelensky Foundation to discredit the President of Ukraine.

The General Staff of the Armed Forces of Ukraine warned of possible provocations by Russians during the 'Army International Games — 2022' held in Belarus, in August 2022. This preemptive action may have helped avert a scenario involving sabotage and potential casualties among the military personnel of foreign countries.

ESTABLISHING A NETWORK OF PARTNERS is a critical element not only for the communication efforts of a specific organization but also for the broader state and public communication framework.

A unified stance from all governmental departments and institutions is essential for bolstering society's resilience against Russian disinformation. State bodies, in collaboration with non-governmental organizations (NGOs), should maintain a consistent communication strategy, disseminating the same messages and narratives, and fostering a cohesive brand resilient to Russian propaganda efforts. Essentially, the communication process in Ukraine should adhere to a 'one voice' policy.

Furthermore, partnerships with other government institutions, media, and NGOs serve to broaden the audience reach. The spread of information on social networks and publication in various media outlets facilitates the combat against Russian disinformation by educating a large segment of the population about specific disinformation narratives and their untruthfulness.

INFLUENCERS — such as bloggers, public activists, and cultural figures - play a significant role in the modern information space. Their involvement in the communication process can significantly enhance the quality and speed of disseminating key messages and narratives, thereby effectively countering the influence of Russian disinformation.

An instance of disjointed and uncoordinated communications was evident in the case involving the order from the General Staff of the Armed Forces of Ukraine, which initially barred men from leaving their regions without permission from military registration and enlistment offices. This decision was not synchronized with Ukraine's top political leadership, resulting in its revocation by the President of Ukraine. The order sparked widespread criticism not only among the general public but also within the Verkhovna Rada of Ukraine, where deputies even proposed a draft resolution to annul the order.

Additionally, there was a lack of consensus within the General Staff itself and the Ministry of Defense of Ukraine regarding the interpretation of this new rule. While the Commander - in-Chief of the Armed Forces of Ukraine, Valerii Zaluzhnyi, and the spokesperson of the Ministry of Defense of Ukraine, Oleksandr Motuzyanyk, affirmed the movement restrictions for men within Ukraine, Zaluzhnyi's legal adviser Yevhenia Ryabeka **said that men liable for military service could move around Ukraine without any permits.**

Such scenarios can significantly damage the reputation of both the state and the Armed Forces of Ukraine. This particular incident played into the hands of Russian propaganda.

BUILDING RESILIENCE involves enhancing the target audience's ability to resist destructive information influences. More details on this can be found in the 'Prevention' section.

REACTIVE METHODS
of strategic communications are employed after the emergence of disinformation messages and narratives, aiming to deny and mitigate their impact.

These methods include

- **NAMING-AND-SHAMING;**
- **REFUTATION;**
- **COUNTER NARRATIVE;**
- **CRISIS COMMUNICATIONS.**

'NAMING-AND-SHAMING'
is a technique that publicly exposes and accuses individuals or organizations of spreading disinformation. In countering Russian disinformation, revealing the identities of media or social media accounts propagating Russian disinformation narratives can diminish audience trust in these channels and counteract the adverse effects of Russian propaganda.

The Security Service of Ukraine periodically publish and update lists of Telegram channels promoting hostile propaganda, as their numbers are consistently growing.

REFUTATION
involves debunking disinformation, which is a crucial and effective aspect of strategic communications against Russian disinformation.

REFUTATION
specifically exposes false information and provides accurate counterarguments, aiming to lessen the negative effects of disinformation.

While often accompanied by fact-checking, refutation and fact-checking are distinct tools. Fact-checking is a broader concept, whereas refutation is targeted at a specific issue.

THE PROCESS OF REFUTATION starts with identifying the information needing counteraction, based on an evaluation of its intent and impact.

Furthermore, **REFUTATION** is a strategic approach. Unlike fact-checking, which seeks truth irrespective of the disinformation's nature, refutation is applied only to disinformation that could potentially harm the interests and objectives of a specific organization.

FACT-CHECKING is a lengthy and resource-intensive process, often outsourced to specialized organizations. Several fact-checking groups in Ukraine, listed in the Appendices, can be approached for assistance or partnership in jointly tackling Russian disinformation.

An organization can conduct a rebuttal independently but should use a standard model, in order to reduce the risk of confirmatory bias or a backlash effect.

---

[20] **James Pamment, Anneli Kimber Lindwall. Fact-checking and debunking. A best practice guide to dealing with disinformation. NATO Strategic Communications Centre of Excellence.**

A COMMON APPROACH FOR DEBUNKING DISINFORMATION:

1 ■ FACT
The text should commence with a clear, straightforward, and comprehensible fact to establish a firm understanding of the issue in the potential consumer's mind.

2 ■ MYTH-BUSTING
It's essential to explain what type of disinformation is being propagated. The false information should be described only once and succinctly.

3 ■ JUSTIFICATION OF FALSITY
Offer robust arguments to demonstrate the falseness and manipulative character of the disinformation being disseminated.

4 ■ FACT Reiterate the initial fact to reinforce the correct information and dispel any lingering doubts created by the disinformation.

EXAMPLE

■ **FACT.** Ukraine does NOT produce biological weapons.

■ **MYTH-BUSTING.**
Russian propaganda machine claims the opposite

Even before Russia's full-scale invasion of Ukraine, Russian media circulated false claims about Western-created laboratories in Ukraine allegedly producing biological weapons. This rhetoric escalated post-February 24, 2022, to an official level. Dmitry Medvedev, for instance, claimed that Russia had evidence that the purpose of US bio laboratories in Ukraine was to develop biological weapons. Russia even convened three UN Security Council meetings on this issue, on March 11, March 18, and May 13.

■ **JUSTIFICATION OF FALSITY.**
However, at all three meetings of the UN Security Council, Izumi Nakamitsu, UN High Representative for Disarmament, noted that the UN was not aware of the existence of any biological weapons program in Ukraine. The US State Department also denied the existence of laboratories in Ukraine capable of producing biological weapons.

In reality, the United States and Ukraine collaborate on biosecurity, not the development of biological weapons. This partnership is part of the Biological Threat Reduction Program (BTRP) under the U.S. Department of Defense's Cooperative Threat Reduction (CTR) program, operational since 2005 with the Ukrainian government. The program's objective is to support peaceful and safe research, diagnosis, and mitigation of biological threats posed by pathogens.

[21] Lewandowsky S., Cook J., Ecker U. K. H., Albarracín D., Amazeen M. A., Kendeou P., Lombardi D., Newman E. J., Pennycook G., Porter E., Rand D. G., Rapp D. N., Reifler J., Roozenbeek J., Schmid P., Seifert C. M., Sinatra G. M., Swire-Thompson B., van der Linden S., Vraga E. K., Wood T. J., Zaragoza M. S. The Debunking Handbook 2020 (Digital resource)

During the implementation of the Biological Threat Reduction Program, many laboratories of the Ministry of Health of Ukraine and the State Service of Ukraine for Food Safety and Consumer Protection were modernized. In 2019, two laboratories were built (in Kyiv and Odesa).

In addition, Ukraine is a signatory to the 1972 Biological Weapons Convention, which prohibits the development, production and stockpiling of bacteriological weapons.

FACT.
Russia's allegations about biological weapons in Ukraine are false, serving as a pretext to justify its unprovoked invasion of Ukrainian territory. Ironically, these accusations come from a country with a history of using banned chemical and biological weapons against civilians in Aleppo, Syria, and in attacks against individuals such as Alexander Litvinenko and Sergei Skripal, deemed unfavorable by the Kremlin.

A COUNTERNARRATIVE INVOLVES ADVANCING ONE'S OWN NARRATIVE IN OPPOSITION TO DISINFORMATION AND PROPAGANDA DISSEMINATED BY AN ADVERSARY. It is often employed to articulate a distinct perspective on highly sensitive and contentious issues.

Implementing a counternarrative necessitates a **WELL-COORDINATED COMMUNICATION PROCESS AMONG ALL INVOLVED PARTIES, EMPLOYING TOOLS OF REFUTATION, AND CONSISTENTLY SUBSTANTIATING ONE'S STANCE WITH FACTUAL EVIDENCE.**

In the struggle against Russian disinformation, the counternarrative is vital for cultivating a positive image of Ukraine, not only among its own populace but also within the international community. This approach helps counteract misleading narratives and reinforces Ukraine's perspective on various issues.

A notable instance of Ukraine's **STRATEGIC COUNTERNARRATIVE** is the refutation of Russia's propaganda claim that its forces are conducting a 'special military operation' in Ukraine, targeting only military sites. Ukrainian President Volodymyr Zelenskyy and other government representatives have systematically informed the world about the Russian army's deliberate war crimes against civilians, providing compelling facts and evidence.

Journalists from Hromadske and The New York Times have presented convincing photographic proof of atrocities committed by the Russian occupying forces in Bucha, against civilians and unarmed populations, acts indefensible by any military necessity. President Zelenskyy has actively communicated these atrocities to the international community.

On June 27, 2022, Russian forces launched a missile strike on the Amstor shopping center in Kremenchuk, Poltava region, where approximately 1,000 people were present. This targeted attack on civilians resulted in 21 deaths, 101 injuries, and one person missing. Bellingcat analysts have ef-

fectively debunked all Russian propagandist narratives attempting to justify this strike as military in nature. It's noteworthy that these narratives were varied and contradictory, a typical trait of the disinformers. President Zelenskyy showcased a video of the missile strike in his address.

Another attack occurred on July 14, 2022, when Russians fired missiles at the center of Vinnytsia, killing 26 people, injuring 202, and leaving eight missing. Vinnytsia's Mayor Serhiy Morhunov affirmed that there were no Ukrainian military facilities within a two-kilometer radius of the impact site. President Zelenskyy shared a video depicting the aftermath of the missile strike and labeled Russia as a terrorist country.

Decommunization is another **COUNTERNARRATIVE** by Ukraine, **COUNTERING DECADES OF RUSSIAN PROPAGANDA THAT LEVERAGED THE SOVIET PAST AND COMMUNIST SYMBOLS.** Since 2014, Ukraine has been systematically pursuing decommunization, working with declassified special service archives and conducting thorough historical research. This has led to the exposure of many crimes by the communist regime, shattering the Russian narrative of a prosperous and safe USSR and the 'friendship of fraternal peoples'.

CRISIS COMMUNICATIONS INVOLVE ENGAGING WITH THE TARGET AUDIENCE DURING A CRISIS

Such crises can range from natural disasters, corruption scandals, attacks on critical infrastructure, to the resignation of a department head.

In critical situations, the rapid spread of disinformation often occurs, making it essential for any organization to adhere to the basic principles and utilize the main tools of crisis communications.

THE PROCESS OF CRISIS COMMUNICATIONS ENCOMPASSES SEVERAL STAGES.

1 ■ IDENTIFICATION OF THREAT(S)
This initial stage requires analysing the information environment and identifying vulnerabilities to anticipate potential crisis scenarios, ranking them from most to least likely.

2 ■ PREPARATION
In this phase, the focus is on developing a strategy to address a crisis. This includes defining key messages, assigning responsibilities, and establishing primary communication channels.

3 ■ RESPONSE
The response to a crisis should be prompt and unified across all stakeholders. It should also aim to build trust and establish a connection with the target audience.

4 ■ EVALUATION. Once the crisis has subsided and the response strategy has been implemented, the effectiveness of the crisis communications plan should be assessed. This analysis informs adjustments for future crisis communication strategies.

In 2020, within the framework of the international technical assistance project 'Partnership for Urban Development', a practical manual 'Community Trust. Crisis Communications of Local Self-Government Bodies' was created. This manual offers a comprehensive explanation of how to develop and apply crisis communications.

During the war, particularly in the context of countering Russian disinformation, Ukraine frequently faces crisis situations, typically linked to Russian assaults on military and civilian targets. Employing crisis communications under these wartime conditions is crucial to prevent the spread of panic among the populace.

EVALUATING ACTIONS TAKEN

Evaluating strategic communication campaigns is the final and crucial step in the disinformation counteraction cycle. This evaluation helps identify and analyse the communication campaign's quality, assess its impact on the target audience, and pinpoint inaccuracies and errors.

ANALYSING these evaluation results enhances understanding of the audience's needs and reactions to specific communication messages and events. Successful tactics can be replicated and adapted for future scenarios. Conversely, ineffective communication strategies can be replaced or modified for improvement. This approach increases the likelihood of

significant audience engagement with the content, reducing susceptibility to misinformation. After adapting the strategy and initiating a new communication campaign, it's important to **REASSESS ITS EFFECTIVENESS.**

Basic indicators, measured at the campaign's outset, are crucial for evaluating whether the tools and channels used have met the desired objectives. It's important to note that evaluating the impact of actions should be an ongoing process.

MEASURING THE EFFECTIVENESS OF STRATEGIC COMMUNICATION

In countering Russian disinformation, evaluating carried-out activities should align with the objectives of strategic communications. Six main goals can be identified, ranging from tactical to strategic.

1 **ATTRACTING A VULNERABLE AUDIENCE.** Keeping the audience most susceptible to Russian propaganda engaged in order to prevent exposure to misinformation. Progress can be gauged through basic metrics like demographic data of social media followers, TV viewers, publication readers, and their numbers.

2 **BUILDING TRUST.** The engaged audience should view the organization as a reliable source. This can be measured by audience engagement dynamics, the frequency of referencing the organization's information, and media mentions.

3 **RAISING AWARENESS.** Disinformation thrives where there is a lack of objective knowledge. Informing the audience about specific issues reduces the chance of manipulation. This goal's success depends on audience reach and their engagement with and comprehension of the information.

4 **BUILDING RESILIENCE.** Teaching the audience to discern truth from falsehood prevents further spread of disinformation. This can be measured using surveys and questionnaires.

5 **CHANGING BELIEFS.** A strategic and challenging goal to both achieve and measure. Russian disinformation often shapes an audience's beliefs and values. If the audience rejects or denies pro-Russian beliefs, the goal is considered achieved. Measurement can be done through social surveys, focus groups, and pre/post-test designs.

6 **BEHAVIOUR CHANGE.** The most challenging goal is changing audience behaviour to act independently of Russian propaganda. Measuring this change, as it occurs beyond the information space, is difficult. Social surveys, focus groups, and pre/post-testing can provide insights into the success of these measures.

GOALS	QUESTION	MEASUREMENT METHODS
ATTRACTING VULNERABLE AUDIENCES	■ Have the messages reached the target audience? ■ What was the reaction? ■ How many people have subscribed / reacted / read? ■ Which communication channel was the most effective? ■ Have the messages spread beyond the target audience?	■ TV channel data ■ Media data ■ Minutes of the meeting ■ Meta Business Suite ■ Twitter Analytics ■ Telegram Analytics ■ YouTube Analytics ■ SimilarWeb ■ Google Analytics
BUILDING TRUST	■ How many people have subscribed / reacted / read? ■ How many shares were there? ■ How many mentions were there in other media, social networks, etc.? ■ How often does the organization appear in the information space?	■ TV channel data ■ Media data ■ Meta Business Suite ■ Twitter Analytics ■ Telegram Analytics ■ YouTube Analytics ■ SimilarWeb ■ Google Analytics ■ Content analysis
RAISING AWARENESS	■ How many people did the campaigns reach? ■ What was the reaction? ■ Has the audience learned the information? ■ Has the campaign become part of public discourse?	■ Meta Business Suite ■ Twitter Analytics ■ Telegram Analytics ■ YouTube Analytics ■ SimilarWeb ■ Google Analytics ■ Polling
BUILDING RESILIENCE	■ How many people did the campaigns reach? ■ What was the reaction? ■ Has the audience learned the information provided? ■ Has critical thinking developed?	■ Polling ■ Questioning ■ Conducting tests

GOALS	QUESTION	MEASUREMENT METHODS
CHANGE OF BELIEFS	■ Have there been changes within the community/society? ■ Has trust in Russian communication channels decreased? ■ Has the number of pro-Russian narratives within the target audience decreased? ■ Has the negative impact of Russian disinformation diminished?	■ Polling ■ Questioning ■ Social Studies ■ Focus groups ■ Before/Post-Test Design
BEHAVIOUR CHANGE	■ Has the target audience begun to act differently? ■ Has Russian propaganda lost its influence? ■ Has trust in Russian sources of information fallen? ■ Have our messages become stronger than those of Russian propaganda?	■ Polling ■ Questioning ■ Social Studies ■ Focus groups ■ Before/Post-Test Design

Modern technologies make it possible to track intermediate results of strategic communications and collect statistical data. Here are examples of such tools.

GOOGLE ANALYTICS
Provides a set of tools to measure consumer interaction with promotional materials, including behaviour on targeted websites.

META BUSINESS SUITE
Optimizes Facebook and Instagram accounts in one user-friendly dashboard. With the platform, it is possible to manage all accounts owned or administrated by a person through various tools to control the brand's social media presence much easier.

TWITTER ANALYTICS
Shows how the audience reacts to the content, which communication methods and moves work and which do not. This data is used to optimize future campaigns on Twitter and get better results.

YOUTUBE ANALYTICS
Used to better understand video and channel performance with key metrics and reports in YouTube Studio.

Note. Some data, such as geography, traffic sources, or gender, may be limited. Also, not all features work on mobile devices.

TELEGRAM ANALYTICS
One of the advantages of Telegram is its built-in analytics tools. Telegram channels have channel statistics and a feature-rich dashboard, allowing you to track the growth of a channel's audience over time.

SIMILARWEB
A tool that estimates the total amount of traffic that different websites receive. It allows you to see competitors' most popular traffic sources broken down into six main categories, including referral sites, traffic from social media, and top search keywords.

Additionally, information gleaned from various social research methods, such as **FOCUS GROUPS** and **PRE/POST-TEST DESIGN,** can be utilized.

FOCUS GROUPS, structured discussions within selected small groups, are widely used in market research and communication campaigns to elicit in-depth reactions to tested products. This format allows researchers to witness spontaneous reactions and delve deeper into respondents' thoughts, setting it apart from surveys. While surveys may be more representative, they are limited by respondents selecting from predetermined answers, capturing less nuance. Focus groups are instrumental in gathering initial feedback on various alternatives for potential communication campaign content before extending the initiative to a broader audience.

Another approach is the pre/post-test design, where participants are surveyed or tested using the same set of questions before and after their involvement in a program. For instance, in a media literacy program, participants could be tested on their ability to differentiate between real and fake news both prior to and following the program. An improvement in discerning true from false news would indicate the program's effectiveness.[22]

This represents a primary, though not exhaustive, list of goals, questions, and tools for assessing the efficacy of communication measures. Combatting Russian disinformation is a complex, non-linear process, necessitating the adaptation of strategic communication goals and measurement methods to each unique situation.

The AMEC Integrated Scoring System provides a consistent and robust approach suitable for organizations of all sizes. It can easily be adapted to specific users and tasks. With the AMEC toolkit, it is possible to measure the effectiveness of a communication campaign, including audience reactions, outputs and outcomes.

[22] **Complete Guide. Countering Disinformation** (Digital resource)

‘WHITE LISTS OF OFFICIAL AND RELIABLE SOURCES OF INFORMATION’ FROM THE CENTRE FOR STRATEGIC COMMUNICATION AND INFORMATION SECURITY UNDER THE MINISTRY OF CULTURE AND INFORMATION POLICY OF UKRAINE

For effective strategic communications and countering Russian propaganda, disinformation and fakes, the Centre for Strategic Communication and Information Security under the Ministry of Culture and Information Policy of Ukraine has developed a **‘White List of Official and Reliable Sources of Information’.**

It contains links to websites and social networks of the following categories of sources.

- Public authorities;
- Government agencies;
- Representatives of state authorities and government agencies;
- City mayors;
- Heads of regional state administrations;
- Charitable foundations;
- Media expert organizations;
- Media;
- Representatives of media and expert organizations;
- Popular bloggers, opinion leaders.

The Centre for Strategic Communication and Information Security under the Ministry of Culture and Information Policy of Ukraine has also developed a separate ‘white list’ of official and reliable YouTube channels.

This list has been approved and agreed with such NGOs in the field of combating disinformation as.

- Institute of Mass Information;
- Texty.org.ua;
- Institute of Information Security;
- Internews Ukraine;
- Detector Media.

Sources from the ‘white list’ are generally reliable, but it is important to remember that even official accounts are not immune to hacking, nor are they exempt from communication errors and misunderstandings. Therefore, we recommend always analysing, critically reflecting on, and verifying information received from these sources against other sources. This practice is crucial to prevent the spread of misinformation.

VERIFICATION OF IMAGES AND VIDEOS FOR AUTHENTICITY AND ABSENCE OF THIRD-PARTY INTERFERENCE AND EDITING

When verifying the authenticity of images and videos, and ensuring they haven't been subjected to third-party interference or editing, one effective method is to conduct an internet search. Google offers a built-in feature to examine images for originality and any signs of editing. This tool can reveal if the same images have been repurposed for different news stories, helping to ascertain their authenticity.

TOOLS you can use to check images

- RevEye Reverse Image Search — Chrome extension;
- TinEye — image verification by link;
- Image Edited? — search for traces of editing;
- FotoForensics — a site for searching for traces of editing and setting image data;
- Who stole my pictures — add-on for Mozilla Firefox.

WHEN YOU HAVE LOCATED THE ORIGINAL SOURCE OF A PHOTO, consider the following aspects.

PUBLICATION DATES. Are they the same or different?
PLACE OF PUBLICATION. Who published the photo? Is this source trustworthy?
ARTICLE TITLE AND CONTENT. Do they correspond with the photo? Ensure the image aligns with the story being told.
DIFFERENCES IN THE PHOTO. Compare the original with the photo in question. Look for cropping, added elements, or alterations.
GEOGRAPHICAL CONTEXT. Where was the photo taken? Does the location match the news story's subject?

TO ANALYSE A VIDEO

REVIEW VIDEO DETAILS. Check the publication date, channel information, and other videos by the creator.
VIEW COMMENTS. Often, commenters provide links to the original source or highlight details that suggest the video is untruthful.
TAKE SCREENSHOTS FOR IMAGE SEARCH. While watching, take screenshots to use in Google's image search for cross-verification.
OBSERVE VIDEO CHARACTERISTICS. Note any cropping, logos, and visible elements like road signs, street names, and seasonal indicators.
MATCH TITLE WITH CONTENT. Ensure the video's title accurately reflects its content. Discrepancies can indicate misleading or false information.

Detector Media and StopFake in their articles described in detail how to detect and debunk photo and video fakes, as well as how to find websites that have already been deleted. We recommend that you familiarize yourself with them.

HOW DO I TELL THE DIFFERENCE BETWEEN A REAL SOCIAL MEDIA ACCOUNT AND A FAKE?

Russian propagandists very often use the fake profiles on the social networks of Ukrainian politicians, the military, public authorities, law enforcement agencies, etc. Fake profiles spread disinformation narratives and fakes.

THERE ARE SEVERAL MARKERS, WHICH TESTIFY TO THE AUTHENTICITY OF THE ACCOUNT

- Verification Icon. Look for a blue checkmark, which typically indicates a verified account.
- Spelling of Name and Username. Check for errors or the use of characters outside the Cyrillic or Latin alphabets, common in fake profiles.
- Number of Followers. Authentic profiles generally have a larger following.
- Number of Publications and Account Age. Assess the number of posts and how long the account has been active. Older, more active accounts are more likely to be genuine.
- Mentions in Other Sources. Real accounts are often mentioned or cited in other reliable sources.
- Appropriateness of Content. Evaluate if the content aligns with the supposed identity of the account holder. Authentic profiles typically have relevant and appropriate content.
- Number of Identical Pages. Multiple accounts with the same name and similar content can be a red flag for fake profiles. Authentic individuals or entities usually have a single official account per platform.

CHECKING CHATBOTS FOR AUTHENTICITY. WHAT ARE THE DANGERS OF FAKE CHATBOTS?

When verifying the authenticity of chatbots, it's crucial to use links from official, verified sources due to the prevalence of fake bots. Chatbots can be more hazardous than fake government agency pages because they are often designed to collect personal data. Engaging with a fraudulent chatbot can lead to becoming a victim of scammers. For individuals in temporarily occupied territories, the risks are even higher, as personal data obtained by fake chatbots could potentially end up in the hands of Russian special services, posing a serious threat to their safety and well-being.

HOW DO I REPORT FAKE ACCOUNTS AND POSTS CONTAINING FALSE INFORMATION ON SOCIAL MEDIA?

FACEBOOK
If you find content and/or Facebook accounts that share malicious content, use the links below.

- Flag a Facebook post as fake news;
- Report abuse;
- If it's an ad, go to the ad library and report it there.

Appeals may be sent to the Supervisory Board. It acts as an external appellate body in case of refusal to satisfy the initial complaint.

INSTAGRAM
To report harmful disinformation or misinformation, use the 'Reducing the spread of false information' page.

FACEBOOK MESSENGER
To complain about any ongoing exchange, you need to click the 'Report' button in the menu to the right of the dialogue. There are also options 'Ignore messages' and 'Block'. You can manage message requests from people who are not your 'friend' on Facebook in the menu in the 'Receiving message requests' section.

WHATSAPP
To report harmful content on WhatsApp, follow these instructions. It's worth noting that WhatsApp is a proprietary encrypted messaging app, so monitoring content on WhatsApp differs from other social networks and platforms listed above.

GOOGLE
Google products have differing terms of service, which contain restrictions on hate speech, deceptive behaviour, and inappropriate content, as well as different mechanisms to ways to report false information and other harmful content. However, the Google search engine is the most relevant in the case of this guide. You can find a tool for requesting removal of information from Google search on this page.

TIKTOK
To report a video, comment, user, hashtag, etc. suspected of misinformation and other harmful content, you should review the detailed instructions in the report a problem section.

TWITTER
To report tweets, lists, and private messages with malicious content, follow the instructions here. Twitter identifies harmful content in its Twitter Rules, which can help the user understand what is prohibited and can be challenged.[23]

[23] Combating Information Manipulation: A Playbook for Elections and Beyond (Digital resource)

FACT-CHECKING SERVICES IN UKRAINE AND ABROAD

THE CENTRE FOR STRATEGIC COMMUNICATION AND INFORMATION SECURITY UNDER THE MINISTRY OF CULTURE AND INFORMATION POLICY OF UKRAINE was established in March 2021. The Centre's work focuses on the counteraction to external threats, uniting the efforts of the government and civil society organizations in the fight against disinformation, rapidly responding to fakes, and promoting Ukrainian narratives. The Centre actively trains civil servants and police officers to fight against fakes and Russian disinformation, informs Ukrainian citizens and international partners of information threats and narratives of the enemy propaganda.

VOXCHECK, part of VoxUkraine since January 2016, initially focused on analyzing lies and manipulations of Ukrainian politicians. Post the full-scale war, it began refuting Russian fakes and analyzing Russian hybrid information threats.

STOPFAKE, functioning since March 2014 at the Mohyla School of Journalism, refutes fakes, publishes analytical articles, and creates educational materials on recognizing fakes. The platform operates in 13 languages.

«TEXTY.ORG.UA». a data journalism agency. Texty.org.ua was founded in 2010. Its main difference from other media is its focus on analysis, processing, and visualisation of large data sets while writing journalistic materials. It works with specific figures and facts, which makes its materials trustworthy. Texty regularly publishes digests of Russian disinformation based on machine analysis of propaganda websites. They are conveniently broken down into narratives. Another interesting tool is the database of pseudo-sociologists and hidden PR officers, which provides a quick insight into the reliability of expert opinion in the news.

The agency developed plugins for Google Chrome and Mozilla Firefox, and the "Feikogryz" chatbot on Telegram. It can identify unreliable websites and disinformation. It helps with the help of tags by users and the neural network developed by Texty experts. Effective for researchers in the field of anti-disinformation, it allows creating arrays of data and tables with false news.

DETECTOR MEDIA, an NGO initiative, maintains a database of its own refutations and other fact-checking organizations. It also analyzes Ukrainian media compliance with journalistic standards and ethics and has a 'Board of Shame' for those supporting Russian aggression. Another fascinating special project is MediaCheck, where compliance with journalistic standards and ethics by Ukrainian journalists is analysed. The journalists also created a "wall of shame" featuring politicians and media workers

who openly supported the Russian aggression against Ukraine. The website offers several other interesting special projects, most of which are dedicated to the subjects of the war and Russian disinformation. Another interesting project aimed at increasing the level of media literacy is Media Driver.

Recently, the organization launched a new project — #DISINFOCHRONICLE, which collects refutations of fakes, manipulations, and lies by Russian propaganda. Search and sorting by dates and tags are available.

'BEZBREKHNI' The BezBrekhni (No-Lies) fact-checking initiative is characterized by truly thorough, profound analysis of fakes and their detailed, high-quality refutation. In addition, the fact-checkers have created several handbooks and articles on verifying information. They have an extensive regional network of local fact-checking initiatives with which they closely cooperate.

UKRAINE CRISIS MEDIA CENTER has a hybrid threat analysis group that analyzes Russian information threats and develops countermeasures, presenting these in its analytical materials.

'HOW NOT TO BECOME A VEGETABLE' is a project by famous fact-checker Oksana Moroz, which not only refutes Russian fakes and disinformation but also aims to foster information hygiene and media literacy among Ukrainians. The project, in collaboration with the Youcontrol service, created a database of Russian propagandists.

GWARA MEDIA, a media outlet from Kharkiv, counters fakes and disinformation through digests, analytical articles, and individual fake refutations.

'EU VS DISINFORMATION' is the European Union's official project against fakes and disinformation. It includes a database of Russian disinformation debunking fakes about Ukraine, Belarus, and other Eastern Partnership countries, and offers many analytical articles and research in the field of disinformation counteraction. The site is available in 15 languages and includes interactive games and quizzes to increase the media literacy level of the EU and Eastern Partnership countries' populations.

BELLINGCAT a renowned investigative journalism agency based on open data (OSINT method), although not primarily focused on combating fakes and

disinformation, successfully addresses this area as well.

INFORMNAPALM is an international investigative community founded after the start of Russian aggression against Ukraine in 2014. It unites volunteers from over 20 countries conducting OSINT research and translating and distributing publications in foreign languages, conducting important media, diplomatic, and educational work. Community investigations have identified Russian servicemen, formations, and military equipment collected during the hybrid phase of the war (2014–2022), designed in user-friendly databases crucial in proving Russian aggression.

MYTHDETECTOR is a Georgian fact-checking service founded in 2014 by the Media Development Foundation, aimed at combating Russian fakes and disinformation, containing a fact-checking database.

START2THINK is a Polish portal offering a diverse selection of services and tools useful for checking text, audio, and video content.

POLYGRAPH is an American professional fact-checking service that refutes Russian fakes and disinformation.

For news verification, various tools using artificial intelligence are also employed. Gwara Media specialists have developed a Telegram bot 'Verification'. The team of the Centre for Strategic Communication and Information Security has created a tool for checking bots. To verify information, content is uploaded to the bot, and a response about the veracity of the information is provided within minutes.

In addition to specialized fact-checking state institutions and public initiatives, other bodies situationally engage in refuting Russian fakes and disinformation. These mainly include structures working in national security and defense. the National Security and Defense Council of Ukraine, the Security Service of Ukraine, the Ministry of Defense of Ukraine, the General Staff of the Armed Forces of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, etc. False information is also sometimes refuted by ministries, regional state administrations, and local self-government bodies (if the information is specialized for them), although generally, they have other functions and counteract disinformation only situationally when circumstances require it.

OPEN SOURCE INTELLIGENCE TOOLS (OSINT) FOR IDENTIFYING INFORMATION MANIPULATION

OSINT involves collecting and analyzing information from public or open sources, which can be instrumental in tracking and detecting misinformation.

BELLINGCAT ONLINE INVESTIGATION SUITE. This user-friendly Google document features tabs for a variety of information verification tools, including image and video checks; content and social media account verification; telephone number and closed messaging service inquiries; maps and location services; transport tracking; IP address and website analysis; international company research; environmental tools; and resources for enhancing online security, privacy, and data visualization. It also includes academic resources and additional manuals.

A GUIDE TO CHECKING MEDIA for Disinformation and Manipulation Based on Data Journalism . This book is a valuable resource for conducting OSINT research on social media accounts, detecting bots, and manipulating images. It also offers resources for online investigations, including attribution tips and tools.

GUIDE TO MEDIA MONITORING OF THE BEACON PROJECT. This guide assists in analyzing disinformation narratives and their sources using data. It is an excellent resource for researchers new to media monitoring or those wanting to ensure they are employing best practices.

CROWDTANGLE. Developed by Facebook, 'CrowdTangle' is a tool designed to identify and monitor social media trends. It tracks verified accounts, pages, and public groups, and can monitor public Instagram accounts and subreddit sections on Reddit.

LIST OF RESOURCES FOR COMBATING INFORMATION MANIPULATION 'ANNEX' This list compiles a broad array of tools for countering disinformation, media monitoring, and social media analysis from leading international organizations.

It's important to recognize that each communication campaign, organization, and country will have different contexts, requiring a mix of tools, skills, and partners. A comprehensive understanding of tools that can aid in identifying and managing current campaigns will enable an effective response and foster resilience against disinformation and manipulation.

TIPS ON INFORMATION SECURITY

SECURE BROWSERS

Secure web browsers incorporate extra security protocols to safeguard against unauthorized third-party activities online. These browsers restrict features and actions not listed in an approved whitelist (like blocking ads, and preventing tracking of browsing history).

1 **BRAVE.** A free, fast, and secure web browser for both mobile and computing devices. Brave comes with in-built ad blockers, bars tracking of web activity, optimizes battery life on mobile devices, and uses less data, resulting in faster page loading. Users can easily import bookmarks and settings from their previous browser. It's compatible with Android, iOS, Windows 10, MacOS, and Linux.

2 **VIVALDI.** Vivaldi does not track users' browsing history or data. Its tracker blocker stops ads and third-party web trackers. It includes various private search engines by default (such as DuckDuckGo, StartPage, Neeva, Qwant) and offers encrypted device synchronization. Vivaldi also provides numerous navigation and interface customization tools for a user-friendly experience. It's available on MacOS, Linux, Windows, and Android.

SECURE EMAIL

Secure email services focus on enhanced security features, offering email encryption and other privacy safeguards.

PROTONMAIL Offers end-to-end email encryption based on RSA keys unique to the user's ProtonMail account. This encryption means only the account user and the email recipient can view the messages, not even ProtonMail itself. ProtonMail's data centers are secured at the hardware level, located in a nuclear bunker with fully encrypted hard drives on each server. It can be accessed via webmail, mobile apps, and Tor, and features a user-friendly interface with anti-censorship capabilities to ensure access even under government blocking.

SECURE MESSENGERS

Secure messengers provide end-to-end encryption for communications, ensuring that only the involved parties can access the information exchanged. These platforms prevent any data tracking, even on the servers hosting the data.

1 **SIGNAL**. This open-source messaging app requires both the sender and receiver to register with a mobile phone number, which Signal neither stores nor transmits. It does not access the phone's contact lists or user registration data. Signal features an option to auto-delete all communications, including calls and messages. It also allows users to relay calls through a Signal server to conceal their IP address. The app supports group video calls with up to 40 participants and chat groups of up to 1,000 members. Signal is compatible with desktops, mobile phones, and tablets across Android, Apple, Windows, and Linux operating systems. With over 40 million active accounts, Signal boasts an active support community and is funded by its founders and other sponsors.

2 **WICKR.** This commercial messenger enables secure transmission of messages, images, videos, audio, and files. Users must have Wickr for communication, but friends can be found without syncing Wickr to the phone's contact list. Each message sent via Wickr has a unique encryption key, only accessible to the recipient and not even to Wickr. It offers extensive control over how long recipients can view or store data. Senders can set different permission levels for direct contacts compared to others considered offline. Wickr's versatile security features make it a robust choice for secure messaging.

CENTRE FOR STRATEGIC
COMMUNICATION
AND INFORMATION
SECURITY

CENTRE FOR DEMOCRACY
AND RULE OF LAW

Sweden
Sverige