CEDMO
Central European Digital
Media Observatory

Russian Disinformation Campaigns in Estonia and Ukraine – A Comparative Perspective

Latte

Luka Nikolic

1. Introduction

Nowadays few notions occupy more space within the public sphere than disinformation. Its over-inflated securitization by governments, increased academic scrutiny, and ubiquitous civil society presence guarantee that it is here to stay. One of the main challenges when writing about disinformation is to avoid identifying it with close, yet different concepts such as misinformation or communication. Limited analytical value is narrowing down its meaning to the level of fake news or a niche of mass media studies. Disinformation needs to be analysed in an all-encompassing, holistic manner, consisting of narratives, agents, operational reality, strategic environment, and beyond. In other words, disinformation is a concerted effort of state and non-state actors to coerce others into a behaviour complementary to the strategic goals of the proliferators.

Although not exclusively associated with Russia, its state apparatus has made significant efforts to refine and advance methods for spreading disinformation. It can be best seen by the inclusion of information operations in all the major strategic documents. That said, many countries and actors have been targeted by Russian campaigns, suffering certain levels of damage. In order to show that, this policy brief tackles the topic of Russian disinformation campaigns conducted in Estonia and Ukraine using a comparative perspective — the three main aims of the paper. Whole-of-society inclusion on the side of the perpetrator is demonstrated, involving the Russian government, military, intelligence, civil society, private sector, academia, and even the population as such. Moreover, it is shown that target countries are hit by disinformation campaigns in a similar, society-wide fashion. Ultimately, through the two cases, valuable lessons can be drawn about modalities of combat against disinformation. The rationale for choosing the two cases lies in their simultaneously sharply opposite and strikingly similar nature. Ukraine, being involved in a war against Russia, has been forced to make authoritarian moves to contain disinformation efforts as a flagbearer of foreign malign influence. Estonia benefits from the extended deterrence umbrella provided by its powerful allies. However, it remains one of the primary targets of Russian information warfare, prompting the country to develop tools and strategies to combat these threats effectively.

The brief continues by explicating the main disinformation narratives of both cases, followed by the structure of the Russian campaign, ending with the structure of the respective counterstrategies.

Analysing the two alongside gives a shot at measuring how efficient the responses have been. Finally, a set of recommendations is given for both state and non-state actors involved in the fight against disinformation.

2. Estonia – the first victim of disruptive disinformation

2.1 Narratives and topics

It is obvious that narratives provide a surplus source of legitimacy for disinformation campaigns. Considering the context of geographical and historical proximity, it's clear that Russia goes to great lengths to manipulate Estonia for the sake of its strategic goals. The foundational narrative present is that Estonia has always been independent, and actually, it has been a Russian state for more than ten centuries. Major topics connected to this are Russian sacrifice in Estonia during WWII, subsequent Soviet liberation of the country, and nostalgia for the time spent under the communist regime. In an institutional sense, Russia has founded a Commission to fight against the alleged tailoring of historical facts which, in their opinion, would serve the purpose of glorification of Nazism (ii). In accordance with that, every action of Estonia after regaining independence will be interpreted as anti-Russian and ultimately neo-Nazi. This has been tested on many target countries and always finds its wide audience. An interesting research shows that the Russian-speaking minority in Estonia gave almost unified answers to questions about history, indicating the success of state-based propaganda (iii).

The Russian-speaking minority is particularly receptive to alternative historical narratives. Despite many holding Russian citizenship, the majority have never been to Russia. Nonetheless, they tend to unconditionally support Russian actions while criticizing Estonia. Several factors contribute to this, with the main one being their lack of proficiency in the Estonian language.

This linguistic barrier leads to a form of self-imposed isolation, keeping them tied to the Russian information sphere (iv). As a result, this group finds itself in a grey zone: unwilling to move to Russia, where the standard of living is arguably lower, but also reluctant to fully integrate into Estonian society. Russia has exploited this deadlock through waves of disinformation, fostering a sense of insecurity among the minority, particularly by promoting narratives of alleged neo-Nazi discrimination by the Estonian government (v).

The pivotal moment in Russian-Estonian relations occurred in 2007 when the Estonian government decided to relocate the Bronze Soldier monument from central Tallinn to the city's outskirts (vi). For Russians, this monument represents the victory in WWII and the liberation of Estonia, while many Estonians view it quite differently, often holding an opposing perspective. This decision sparked intense protests both in Estonia, known as the "Bronze Night," and in Russia, where demonstrators laid siege to the Estonian Embassy in Moscow. Following the monument's relocation, Russia launched its first major cyberattack against a nation-state. These cyberattacks, combined with aggressive disinformation campaigns, targeted Estonia's government, banks, police, media, and more, severely disrupting the country's ability to function (vii). The attacks were seen as a stark warning that urgent action was needed. NATO's initial response was to establish the Cooperative Cyber Defence Centre of Excellence, which remains at the forefront of efforts to counter Russian malign influence today (viii).

2.2 Russian disinformation campaign in Estonia – main actors and influence agents

As much as disinformation campaigns can be covered by multiple layers of secrecy, its consequences are evident, enabling us to reveal the structures and agents involved, at least retrospectively. In Estonia, we can identify three main clusters of influence: media outlets, civil society, and academic institutions.

Many media outlets responsible for spreading disinformation in Estonia are directly controlled by the Kremlin and are widely accessible. These primarily include traditional TV channels like RTR Planeta, and NTV Mir, and Pervyy Baltiyskiy Kanal (First Baltic Channel or PBK), as well as various internet streaming platforms. Propaganda is often embedded within entertainment shows, covering a wide range of topics, from historical narratives to health issues (such as pandemics), and offering skewed interpretations of the global geopolitical landscape (ix). These outlets exploit existing socio-political divisions, aiming to deepen polarization and incite radicalization against the Estonian government. This tactic is considered a form of psychological manipulation, with its success measured by both the level of social disruption and the impact of technological tools used. Recently, social networks such as VKontakte, Odnoklassniki, Facebook, X, and Telegram have emerged as key platforms for rapidly disseminating disinformation. Particularly concerning are "active ideological users" who, with their extensive contact networks, can expand their reach quickly, amplifying disinformation efforts (x).

NGOs and assertive diplomatic initiatives are the second domain of influence projection within the disinformation campaigns. Organizations like the Pushkin Institute, the Baltic Youth Alliance, and the Reval Media Agency operate as NGOs tasked with engaging the Russian-speaking population and spreading disinformation within this community. Under the guise of legitimate civil society work, these groups have regular access to events across Estonia, using these opportunities to subtly promote their agenda. According to an intelligence briefing from Estonian services, the Russian Embassy in Estonia directly funds a range of festivals, such as Vivat Rossiya, and publications like Baltiskij Mir, with the aim of fostering pro-Russian sentiment and covertly spreading disinformation (xi). These events and outlets have also been linked to money-laundering schemes and, in the past, have helped craft aggressive narratives, including claims of neo-Nazi persecution of the Russian minority in Estonia.

Of uttermost importance are the policies and organizations directly linked to Russian intelligence services, such as the Russian compatriot policy and the Russian Institute for Strategic Studies (RISI). This is due to the nature of their work, being directly responsible to the highest echelon of the Kremlin administration, ensuring a stable financial and infrastructural situation. The compatriot policy aims to maintain tight control over the Russian community in Estonia, making them highly vulnerable to disinformation campaigns. This group falls under the direct oversight of the FSB, with General Dmitry Milyutin, deputy director of the Department for Operational Information, specifically tasked with managing operations related to this policy (xii). Meanwhile, RISI, a think tank under the control of the foreign intelligence agency SVR, has been a consistent source of disinformation. Led by former SVR chief Fradkov, RISI sponsors international conferences, funds research trips, and provides educational exchange opportunities between Russia and Estonia (xiii). However, these activities serve as a facade for its broader goal of exerting malign influence abroad.

Of somewhat lesser significance are traditional academic institutions and political parties. Many intelligence officers hold prominent positions within university hierarchies, particularly in international offices, where they leverage foreign exchange programs to recruit potential agents of influence abroad. Research institutions like the Institute for Baltic Civilizations have provided an academic veneer for promoting historical and other disinformation narratives. Estonia's political system prohibits direct foreign financing of political parties, which limits Russia's influence in this area, but there have been exceptions. Notably, in 2016, the Centre Party—a coalition partner in the Estonian government—promoted pro-Russian propaganda and maintained an official partnership with Putin's United Russia party (xiv). However, disinformation originating from political parties in Estonia has a far more limited impact compared to other countries.

2.3 Estonian counter-disinformation efforts

Estonia is a trailblazer when it comes to the principles to counter disinformation. Those include whole-of-society since integration is a necessary condition to maintain the composure of the system. Certain parts of the system are more prone to leakages, but they are compensated by the checks and balances system.

Since the psychological component is crucial to the effectiveness of disinformation, it is equally vital in efforts to combat it. To counteract the effects of disinformation—such as confusion and fear—and to prevent Russia from achieving its strategic goals, Estonia has implemented a series of measures aimed at raising public awareness about threats that could undermine the constitutional order and society at large. A key aspect of this effort is strategic communication (STRATCOM), which serves as a coordination tool to ensure a unified response to external hybrid threats in political, economic, and defence spheres. A critical element of STRATCOM is the ability to deliver clear and credible messages to the general public. Together, these measures function as a form of "perimeter defence," representing the first line of threat neutralization when preventive and deterrent efforts have been exhausted.

While it might seem intuitive to combat disinformation by shutting down media outlets, Estonia has taken the opposite approach. Russian channels are widely accessible across the country through major telecommunications providers. In the eastern regions, residents can watch Russian TV and listen to Russian radio without needing cable subscriptions or special equipment (xv). Rather than imposing censorship, Estonian strategists chose to offer a positive alternative by launching an Estonian TV channel in the Russian language—a neutral option to counter Kremlin-backed disinformation (xvi). This approach is seen as a long-term solution, recognizing that it will take time for the Russian-speaking minority to break free from their echo chambers and embrace new perspectives. Some might argue that allowing Russian media to operate freely makes Estonia more vulnerable to malign influence, but in practice, empowering solutions with broad societal backing have proven more effective in fostering organized systematic resistance.

The Estonian mantra claims that its values spread faster than Russian disinformation—a bold assertion given the sophisticated technological tools employed by disinformation campaigns. Regardless of the government in power, the Estonian state has been nurturing and supporting a new generation of opinion leaders with access to various communities, groups, and echo chambers (xvii). These networks have steadily grown into self-sustaining entities capable of absorbing and rejecting disinformation. While their success varies, these networks consistently promote the values of Estonia's constitutional order, the significance of liberal democracy, and the fundamental importance of human rights. Once these principles are embedded in the collective mindset, the networks initiated by opinion leaders can be seen as contributing to what is known as societal resilience (xviii). This indicates that Estonian society possesses the strength to counter disinformation without resorting to escalatory measures.

Part of this solution has already been addressed under STRATCOM, as it requires cooperation between military and civilian sectors. However, it also highlights a different aspect: reassurance policy. Various initiatives have been aimed at fostering a sense of security within the Estonian population. These range from introducing media literacy classes in elementary and high schools to fact-checking efforts and guides on navigating disinformation to symbolic actions such as deploying a small contingent of NATO forces to Estonia (the "trip-wire" mechanism) and temporarily relocating government headquarters to Narva. By addressing the psychological dimension, these counter-disinformation activities enhance the public's self-confidence, thereby making institutional responses more effective.

3. Ukraine – where disinformation turns into operational reality

3.1 Narratives and topics

Since 2014, Ukraine has experienced several phases of conflict with Russia, beginning with the illegal annexation of Crimea, followed by Russia-backed separatist movements in eastern Ukraine, and culminating in the full-scale invasion launched in February 2022. This progression was the result of long-term, systematic planning. Many experts argue that disinformation played a central role, serving as a key strategy for Russia to justify and legitimize its actions (xix). Russia's disinformation campaign in Ukraine is so intricate that fully understanding its many layers may take considerable time, as hidden agendas gradually come to light. Notably, this campaign has employed both traditional and advanced disinformation tactics, combining older "active measures" with more sophisticated, technologized methods (xx).

As with Estonia, Russia has drawn on historical narratives to claim that Ukrainian independence is an anti-Russian construct. These narratives often invoke the mythology of Kievan Rus, but even more prominently reference World War II folklore. A key narrative rooted in that history portrays modern Ukrainians as followers of Stepan Bandera. Russia uses this to further a metaphor linking Ukraine to Nazism, claiming the country is a neo-Nazi puppet state committing genocide against Russians, and that its ideology is based on Russophobiaxxi.

Another pervasive narrative romanticizes the Soviet era, framing it as a golden age for Slavic people, and posits that Russia's fight in Ukraine is a continuation of the struggle against Nazismxxii. According to this narrative, any movement by Ukraine toward the West will inevitably lead to instability. These overarching themes are often reinforced by secondary narratives, such as the "clash of civilizations," the idea of Ukraine being part of the Russian world, and the notion that divisions within the West legitimize Russia's actions. By spreading these falsehoods, Russia aims to deepen socio-political divides in Ukraine and exploit the country's vulnerabilities.

As military operations escalated, Russian disinformation increasingly emphasized the idea that Ukraine had become militarily controlled by NATOxxiii. This narrative intensified after Western nations began providing military aid to Ukraine, framing Ukraine as a NATO puppet being used to provoke Russia at its borders. Another long-running narrative, dating back to the conflict in Donbas, sought to tarnish the reputation of the Ukrainian armed forces, portraying them as criminals, rapists, and war criminals committing atrocities against civilians (xxiv). The goal of these fabrications was to weaken combat readiness, encourage defections, and lower morale. Following the 2022 invasion, Russian disinformation shifted its focus to denying or distorting war crimes, such as the Bucha massacre, spreading false claims about Ukraine acquiring biological weapons from the U.S. to destroy Russia, and alleging that NATO was setting up a military base in Odessa.

3.2 Russian disinformation campaign in Ukraine – main actors and influence agents

Arguably, media outlets have played the most pivotal role in spreading disinformation in Ukraine. Both Russian channels (RT, Pervyy Kanal, Rossiya 1, Rossiya 2, LifeNews, NTV) and pro-Russian Ukrainian outlets (Inter, Channel 17, Channel 112, Ukraina24) collaborated to create an ecosystem of fake and misleading news. During the separatist conflict in eastern Ukraine, regional channels like Lugansk24 and Novorus.info were particularly influential in spreading anti-Ukrainian army narratives. This strategy, which involved flooding the public with an overwhelming amount of information that is difficult to combat or debunk, has been referred to as the "firehose of falsehoods.xxv" Financial support for these media outlets often came from Russian oligarchs tightly controlled by the Kremlin.

Various disinformation techniques were employed. For instance, during the annexation of Crimea, the same actress appeared in multiple fabricated roles, such as a protester in Crimea, a resident of Odessa, and a grieving mother of a Ukrainian soldier. Russian state-run TV also aired a falsified video that purportedly showed the Ukrainian military using phosphorous bombs against civilians, which was later debunked as footage from the Iraq war in 2004 (xxvi).

The Ukraine conflict also marked the first time the internet was fully harnessed as a tool for disinformation. Key actors in this space included paid trolls who flooded chat rooms, comments, and forums with the Kremlin's agenda (xxvii). Fake social media accounts helped amplify disinformation, making it spread rapidly and appear more credible. As early as 2013, investigative reports revealed that Russia had organized troll farms before military actions even began. One of the most prominent troll farms was the Internet Research Agency, led by Yevgeny Prigozhin, later known for leading the Wagner Group. Trolls were often paid to post up to 100 comments a day, creating significant noise within communication channels. Another disinformation tactic was "typo-squatting," where legitimate website names were slightly misspelled, leading users to doctored content (xxviii). Many Ukrainian public institutions were targeted using this method.

Given the sensitive nature of intelligence in an ongoing conflict, it’s difficult to identify all the intelligence actors (FSB, GRU, SVR) involved in Russia’s disinformation campaign. However, evidence suggests that pro-Russian political parties in Ukraine (such as the "For Life" party), Russia-based pseudo-NGOs (e.g., Rossotrudnichestvo, Compatriots Living Abroad, Russkiy Mir), mobile network operators like MirTelecom, and even physical propaganda through loudspeakers in border regions have contributed to spreading falsehoods (xxix). However, due to wartime conditions and stricter government control, the influence of these actors remains relatively marginal on the ground.

The success of Russian disinformation campaigns can largely be attributed to weaknesses within Ukraine's socio-political infrastructure. Two primary shortcomings stand out. First, Ukraine's information space was not prepared to handle such an onslaught. Russian media and disinformation efforts were largely unregulated at the time, and by the time Ukraine moved to impose controls, these channels and narratives were already deeply entrenched (xxx). Since then, Ukraine has prioritized information security and implemented various institutional reforms. Second, until 2022, Ukraine refrained from labeling the conflict as an interstate war, instead characterizing it as an "anti-terrorist operation." (xxxi) This framing allowed Russia to exploit the situation and solidify its influence in eastern Ukraine, even though it was clear that separatists were directly funded, trained, and organized by Russia. Ukraine's hesitation to declare war provided Russia with an opportunity to entrench itself in the region.

3.3 Ukrainian counter-disinformation efforts

Ukraine's counter-disinformation mechanisms have been shaped by the wartime environment and the need for socio-political unity. These efforts revolve around four key pillars:

At its core, assertive state interventionism involves censorship, based on the idea that eliminating the source of disinformation removes its impact. Ukraine has implemented censorship in three main areas. First, in mass media: following the annexation of Crimea, Ukraine suspended many Russian TV networks, with the number reaching 73 by 2016 (xxxii). This led disinformation to shift to less regulated social networks, where Ukraine also moved to suspend accounts linked to Russian influence agents. Second, in the political sphere: pro- Russian political parties were banned, including the "Opposition Platform – For Life" in 2022, a decision upheld by Ukraine's Supreme Court (xxxiii). Third, Ukraine has taken steps against the Russia-linked Ukrainian Orthodox Church, viewing it as a foreign agent spreading malign influence. While the international community has recognized the need for Ukraine to counter disinformation aggressively, concerns have been raised about balancing these efforts with the protection of press freedom and freedom of association (xxxiv).

Recognizing that existing institutions were not equipped to handle the scale of Russian disinformation, Ukraine introduced new measures. The National Security and Defense Council (NSDC) mandated that all Ukrainian media participate in broadcasting official state news, resulting in the creation of the 24/7 "United News Marathon," aired by the country's four largest TV networks (xxxv). This significantly reduced press freedom. Additionally, the government established the Centre of Countering Disinformation (CCD), tasked with debunking disinformation, fact-checking, and disseminating the truth to the public. Another legal measure aimed at curbing Russian influence was a 2022 law that restricted the use of the Russian language in public spaces. Under this law, 90% of broadcast airtime must be in Ukrainian, and regional outlets are limited to broadcasting no more than 20% of non-Ukrainian content (xxxvi). This legislation sought to minimize Russian influence and limit the space for disinformation to spread.

While the full scope of Ukraine's disinformation efforts remains unclear due to the ongoing conflict, it is logical to assume that Ukraine has engaged in counter-campaigns to push back against Russian disinformation. Evidence of this can be seen in Ukraine's counter-propaganda efforts during the Donbas conflict, which helped prevent large-scale defections (xxxvii). A key tactic has been the distribution of flyers and leaflets containing official state messaging, a traditional Russian method now adopted by Ukraine to reach Russian-speaking populations in the eastern regions.

As part of Ukraine's institutional reforms, the lack of strategic communication (STRATCOM) became evident. To address this, the government began integrating civilian, governmental, and defence sectors to build more resilient structures. The war also forced Ukraine to rethink its crisis communication strategies. Key methods included instructing mobile network providers to offer free connections across the country and establishing emergency news broadcasts to ensure even those with limited access to media stayed informed (xxxviii). In addition, empowering NGOs has been a critical part of Ukraine's strategy. Organizations like the Ukrainian Crisis Media Centre and Information Resistance have played a pivotal role in combating disinformation.

4. Estonia and Ukraine compared

The text has already identified similarities between Russian disinformation strategies in Estonia and Ukraine, particularly in terms of the actors involved, methods used, and overarching strategic goals. While the level of Russian ambition varies significantly between the two countries, the underlying logic has remained consistent. This section will compare their approaches to combating disinformation and offer policy recommendations for future improvements.

The most notable difference between Estonia and Ukraine's approaches lies in their planning. Estonia has focused on building a long-term system to respond to disinformation campaigns. Initiatives like psychological defence and societal resilience are long-term investments, often spanning decades, but once established, these mechanisms become permanent fixtures in the defence against disinformation. On the other hand, Ukraine has adopted a short-term strategy, driven both by immediate wartime pressures and the appeal of quick results. While effective, tools like censorship and restrictions on human rights, if maintained beyond the immediate crisis, risk undermining the country's future. Policies implemented during the war will need to be reevaluated once the conflict subsides, as the transition period could pose a significant risk of regression. In short, Ukraine’s solutions work as long as they remain temporary.

Similarly, Estonia's strategy to counter disinformation is rooted in promoting the values of its constitutional order, democratic institutions, and respect for human rights. These long-term solutions allow ethical, value-driven messages to permeate society quickly. Once these values are embraced, the population gains trust in the government, which can then guide the system toward lasting stability. In Ukraine’s case, however, the approach has sometimes leaned toward creating its own disinformation or presenting an overly centralized official narrative. While this may be necessary to maintain combat readiness, it does not address the root of the problem. In fact, by avoiding direct confrontation of disinformation, Ukraine's socio-political system could become more vulnerable over time.

In the two overarching strategies of each country, we can summarize that Ukraine "fights" while Estonia "reacts." These metaphors reflect their broader approaches to countering disinformation. Ukraine has embraced all levels of escalation within its operational framework. It begins by debunking and fact-checking disinformation, but if those efforts fail, it escalates to deterrence by punishment. In cases of repeated disinformation attacks, Ukraine is prepared to weaponize its countermeasures and aggressively defend its vital interests. Estonia, by contrast, has designed its strategy without resorting to weaponization. This is evident in the near absence of any significant narrative about the Russian occupation of Estonia. The highest level of escalation in Estonia’s approach is deterrence by denial, further reinforced by the extended deterrence provided by its allies. Much of Estonia’s effort is focused on enhancing media literacy and empowering its population to navigate disinformation challenges on their own.

The two countries also differ significantly in their approach to fundamental freedoms, such as freedom of expression and press freedom. The democratic versus instrumental interpretations of these universal rights are critical here. Ukraine, facing a direct military threat from Russia, has justified limiting or even suspending certain human rights, especially press freedom, as a necessary and legitimate measure to achieve its singular strategic goal—victory in the war. In contrast, Estonia views human rights and freedoms as the cornerstone of its constitutional order. Without these freedoms, Estonia would not remain the country it is. Even harmful external influences are tolerated to some extent, based on the belief that Estonian society is resilient enough to recognize and reject such efforts. In this sense, Estonia treats human rights as ends in themselves.

Both Estonia and Ukraine rely heavily on foreign partners, though in different ways. As a member of NATO and the EU, Estonia benefits from substantial military, economic, and infrastructural support during crises. In exchange, Estonia has delegated portions of its sovereignty to supranational bodies, a trade-off seen as worthwhile. The presence of NATO's Cyber Defence Centre of Excellence in Tallinn and forward military deployments during heightened tensions highlight the seriousness with which Estonia's allies approach this partnership. Ukraine, though not a member of NATO or the EU (despite its aspirations to join both), also relies heavily on foreign aid. Whether in the form of weapon shipments, financial support, or more lenient migration policies, Ukraine has worked hard to assure its European and transatlantic partners that their support is justified and for a noble cause.

5. Policy recommendations

Central and Eastern European countries can draw many valuable lessons from the experience of Estonia and Ukraine. This is particularly important for the Czech Republic which demonstrated certain deficiencies within the state apparatus that enabled penetration of the foreign malign influence.

Strategic communications: Similarly, the two described cases, the Czech Republic should introduce strategic communications in the national documents and strategies, declaring the principles, operational guidelines, and long-term aims. In a top-bottom manner, the Office of the Government, together with ministries (aside from the Ministry of Interior which already has its taskforce) (xxxix), and other sub-state levels, should work on its unification and implementation. Strategic communications must be prescriptive, continuous, deprived of political burden (in the sense of monopoly of a certain administration over the process), solutions-oriented, and educated. Outsourcing experts from civil society is a good starting point for developing coherent communications of strategic importance.

Coordination and Synchronization Strategies: Lack of cross-sector and interagency communication has been described as a factor that often left public space in the Czech Republic prone to foreign influence and hybrid operations. Lack of coordination within the government, combined with scepticism towards external agencies, is a conjecture that has led to many deviations in public opinion (such as, very low level of trust in public media broadcasters). A unified approach is essential to strengthen responses to foreign malign influence (xl). Interagency cooperation is crucial to eliminate communication gaps or conflicts within the state apparatus, ensuring that ministries, agencies, and other entities work in harmony under official guidelines. Second, intergovernmental collaborations among like-minded countries should be encouraged on a voluntary basis, as these partnerships tend to be more durable than formal resolutions or declarations. For the Czech Republic it would be beneficial to coordinate efforts on the level of Visegrad Four since those countries have been at the forefront of the fight against disinformation. Third, the public and private sectors must collaborate effectively, with grassroots organizations and civil society playing a key role in combating disinformation and providing valuable insights.

Public support for private initiatives fosters better cooperation. Finally, civil-military cooperation is vital; democratic nations cannot afford to isolate their military institutions. Ministries of defence and military leadership should be involved in shaping strategies to counter disinformation, with civilian oversight ensuring accountability. Here, the Estonian example is crucial. Namely, their Strategic Communications Centre functioning under Estonian Defence Forces, serves as the point of contact between military and civilian institutions, offering resources and know-how.

Leveraging International Organizations: Despite challenges to their credibility, international organizations (IOs) continue to symbolize the rule-based order and peaceful conflict resolution. In disinformation campaigns, IOs should provide clear standards or guidelines for protecting societies from harmful practices. Their universal legitimacy can unite like-minded states with shared strategic goals, offering a platform for long-term cooperation. Organizations such as the UN, OSCE, and EU can play a key role in establishing these standards. For the Czech Republic it is of vital importance to rely on cooperation with the EU. First, it is a community of the most advanced countries in combating disinformation where many of them can serve as role models (Estonia certainly being one of them).

Second, the EU enabled many mechanisms through which the Czech Republic can get valuable help, be it in legal, academic/expert, or practical aspects, EDMO and CEDMO being among the most significant. The EU also provides a lot of funding in order to increase resilience of its member countries, therefore protecting the alliance as a whole against the third-party influence.

Oversight of Algorithms and Legal Provisions: While human rights and liberties must remain central to counter-disinformation strategies, some degree of oversight and control is necessary to prevent unchecked autonomy from devolving into chaos. This involves monitoring algorithms to ensure they don't foster algorithmic authoritarianism. The algorithms themselves should not be manipulated, but their guiding principles should be under scrutiny. In the legal realm, laws need to clearly define disinformation and outline the consequences for violating these norms. Governmental agencies in the Czech Republic must do a better job in implementing the already existing acts and adopting the new ones as the legal provisions follow the ever-advancing technologies of disinformation. The two most important documents to apply *in foro domestico* are "A strengthened Code of Practice on Disinformation" which offers a comprehensive guide on how to prevent the erosion of democratic practices, and "AI Act" which among other things tackles the phenomena of deepfakes as one of the strongest tools on disposal for
disinformation proliferators.

Winning Hearts and Minds through Value Promotion: Borrowed from counterinsurgency strategies, winning hearts and minds involves adopting a soft approach to resolve conflicts. Rather than mobilizing the population ideologically against disinformation, the state should offer rational, value-based explanations for its actions. The guiding principle here is *necessity*

in a democratic society. By adhering to this standard, states can legitimately engage citizens and foster public support in countering disinformation. The Czech Republic can learn here both from Estonia and Ukraine. Estonia mostly prevented and deterred major Russian intrusions by spreading the values of constitution and liberal democracy, gathering people around the common values. On the other side, Ukraine demonstrated that it is possible to turn a common enemy into a promotion of societal values. That is why the war against Russia in the Ukrainian communications strategies has been turned into a war to protect the integrity of Ukraine. The Czech Republic, as the country with an unpleasant history of relations with Russia, must determine on the strategic level adversaries and allies, tailoring the communications according to that division. Just after that, it will be possible to gather Czech people positively around the ideals of democracy and prosperity. This soft component can be crucial in maintaining the composure of the population and increase their will to participate in the process of combating disinformation which definitely requires whole-of-society engagement.

Systemic Funding for Disinformation Countermeasures: Funding for disinformation countermeasures typically focuses on basic efforts like fact-checking, debunking, and supporting NGOs or media outlets. However, it's equally important to fund institutions tasked with deterrence, such as strategic communications (STRATCOM) departments, Cyber Centres of Excellence, and joint civilian-military initiatives. Additionally, specific funds should be allocated for participation in intergovernmental efforts and initiatives led by international organizations. Adequate, sustainable funding across all levels of disinformation response is essential for long-term success. A viable strategy for the Czech Republic on how to find sufficient financial means to achieve systemic stability in combat against disinformation should come through a double-track, public and private enterprise. The Czech government can count on the financial help of the European Union but needs to increase its spending for the same purpose. Small sums from the defence and education budget would ensure intra-structural and inter-agency development and cooperation. Outsourcing already existing experts and organizations from the civil society and academic sector would build the capacity of governmental structures and provide additional systemic cohesion. Financing needs to be oriented towards a long-term, proactive, and informed combat against disinformation.

6. References

i Sazonov, V., Pakhomenko, S., Kopytin, I. (2021). *Between History and Propaganda: Estonia and Latvia in Russian Historical Narratives*. In: Mölder, H., Sazonov, V., Chochia, A., Kerikmäe, T. (eds) The Russian Federation in Global Knowledge Warfare. Contributions to International Relations. Springer, Cham.

ii Security Police of the Republic of Estonia (2010) *Annual Review 2010*, p. 13.

iii Teperik, D. et al. (2018) *Virtual Russian World in the Baltics: Psycholinguistic Analysis of Online Behaviour and Ideological Content among Russian-Speaking Social Media Users in the Baltic States*, NATO Strategic Communications Centre of Excellence, Riga, p. 7.

iv Mattiisen, M., Grajewski, P., Supinska, A. (2021) *Russia's Influence and Presence in Estonia*, New

Direction: The Foundation for European Reform, Brussels, p. 24.

v Teperik, D. (2022) *Disinformation Networks of pro-Kremlin Proxies in Estonia and Their Fostering*

of Anti-Government Sentiment among the Russian Speaking Community: The Case of Antivaccination Narratives in the Online Space, International Centre for Defence and Security, Tallinn, p. 3.

vi Details about the case can be found at: Jurvee, I., Mattisseen, M. (2020) *The Bronze Soldier Crisis of*

2007: Revisiting an Early Case of Hybrid Conflict. International Centre for Defence and Security, Tallinn.
vii Thomas, T. (2020) *Three Discussions of Russian Concepts : 1. Russian Information Weapons ; 2. Baltic*

Defenses (Estonia, Latvia, Lithuania) against Russian Propaganda; and 3. Russia's Development of Non- Lethal Weapons, The MITRE Corporation, McClean, VA, p. 33.

viii Thomas, T. (2020) *Estonia Reacts: Confronting Russian Manipulation Techniques*, The MITRE

Corporation, McClean, VA, p. 3.

ix Teperik, D. (2022) *Ibid*. p. 4.

x Teperik, D. et al. (2018) *Ibid*. p. 38.

xi Security Police of the Republic of Estonia (2010) *Ibid*. p. 9.

[xii] Estonian Foreign Intelligence Service (2023) *International Security and Estonia 2023*, Estonian Foreign Intelligence Service, Tallinn, p. 48.

[xiii] *Ibid*. p. 50.

[xiv] Mattiisen, M., Grajewski, P., Supinska, A. (2021) *Ibid*. p. 22

[xv] *Ibid*. p. 27

[xvi] Thomas, T. (2020) *Estonia Reacts*, *Ibid*. p. 5.

[xvii] Teperik, D. (2022) *Ibid*. p. 4.

[xviii] Jermalavicius, T., Tarmak, V. (2012) *Towards a Resilient Society, or Why Estonia does not Need 'Psychological Defence'*, International Centre for Defence and Security, Tallinn.

[xix] Gretskiy, I. (2022) *Russia's Propaganda War*. International Centre on Defence and Security, Russia's War in Ukraine Series no. 9, Tallinn, p. 1.

[xx] NATO Strategic Communications Centre of Excellence (2015) *Analysis of Russian Information Campaign against Ukraine: Examining Non-Military Aspects of the Crisis in Ukraine From a Strategic Communications Perspectives*, NATO StratCom Centre of Excellence, Riga, p. 6.

[xxi] Sazonov, V. et al. (2017) *Russian Information Operations against Ukrainian Armed Forces and Ukrainian Countermeasures (2014-2015)*, ENDC Occasional Papers no. 6, p. 55.

[xxii] NATO Strategic Communications Centre of Excellence (2015) *Ibid*. p. 17-21.

[xxiii] Gretskiy, I. (2022) *Ibid*. p. 2.

[xxiv] Sazonov, V. et al. (2017) *Ibid*. p. 56.

[xxv] Ferencik, A. (2022) *Putin's Disinformation & Misinformation Campaign*, Europeum Institute for European Policy, Prague, p. 4.

[xxvi] Cordesman, A. (2020) *Chronology of Possible Russian Gray Area and Hybrid Warfare Operations*, Center for Strategic and International Studies, Washington, DC.

[xxvii] Kowalski, A. (2022) *Disinformation and Russia's war of aggression against Ukraine: Threats and Governance Responses*, OECD, Paris.

[xxviii] *Ibid*. p. 3.

[xxix] Meister, S. (2015) *Isolation and Propaganda: The Roots and Instruments of Russian Disinformation Campaign*, Transatlantic Academy, 2015-2016 Paper Series no. 6, Washington, DC, p. 7-8.

[xxx] Gretskiy, I. (2022) *Ibid*. p. 1; Sazonov, V. et al. (2017) *Ibid*. p. 67.

xxxi Minzarari, T. (2023) *An Assessment of Russia's Way of War in the Wake of Its Aggression in Ukraine*, National Defense University, Washington, DC, p. 18.

xxxii Gretskiy, I. (2022) *Ibid*. p. 1.

xxxiii The Kyiv Independent News Desk (2022) *Parliament Dissolves pro-Russian Opposition Platform Faction Following Security Council Ban*, Kyiv Independent. Available at: https://kyivindependent.com/parliament-dissolves-pro-russian-opposition-platform-faction-following- security-council-ban/.

xxxiv Kowalski, A. (2022) *Ibid*. p. 2.

xxxv Guz, S. (2023) *The Battle for Journalistic Freedom in Wartime Ukraine*, OpenDemocracy. Available at: https://www.opendemocracy.net/en/odr/ukraine-journalists-media-restrictions-self-censorship/.

xxxvi Kowalski, A. (2022) *Ibid*. p. 15.

xxxvii Gretskiy, I. (2022) *Ibid*. p. 3.

xxxviii Butenko, V. (2023) *‘We are Totally Ready’: Ukraine Prepares for Fresh Russian Attacks on Energy as Winter Nears*, CNN. Available at: https://edition.cnn.com/2023/11/10/europe/ukraine-energy-grid- russian-strikes-intl-cmd/index.html.

xxxix Tkáčová, N., Šefčíková, K. (2023) *Assessment of Strategic Communication Structures and Capabilities*

in the Czech Republic, Prague Security Studies Institute, Prague, p. 7.

xl Partially adapted from Helmus, T., Keep, M. (2021) *A Compendium of Recommendations for Countering*

Russian and Other State-Sponsored Propaganda, RAND Corporation, Santa Monica, CA, p. 11.

Funded by
the European Union
NextGenerationEU

CZECH
RECOVERY
PLAN