Disruptive disinformation: countering malign Russian influence in Estonia and Ukraine

*Luka Nikolić**

Abstract

Since the aggression on Ukraine started, Russia has re-emerged as the most important security challenge on a global scale. Aside from the robust military presence, for more than a decade Russian strategic toolbox has included leaving a socio-political impact abroad, embodied in the concept of hybrid (sometimes marked as unconventional, irregular, psychological) warfare. The flagship method with the widest domain of application is disinformation. Therefore, the aim of this project is twofold, undertaking an approach to focus simultaneously on the perpetrator of disinformation and the target country.

First, the paper aims to define and analyze disinformation as a disruptive technology. Namely, every disruptive technology including disinformation permeates a state apparatus, changing its core and leaving systemic consequences. Through the process of building resilience, states can respond and adapt to new circumstances. Accordingly, a holistic approach is needed to explain the phenomena of Russian disinformation. It stretches society- wide and includes government, military, private sector, NGOs, academic institutions, and even the population as such that can be used as a proliferator of disinformation. The ultimate goal here is to describe Russian strategies and policies formed under the cloud of disruptive disinformation.

Second, through the comparative analysis of efforts to counter Russian disinformation in Ukraine and Estonia, it will be possible to determine the pros and cons of differing approaches. Well-known events in Estonia were initiated in 2014. ranging from physical propaganda at the borders to the appearance of little green men under the auspices of harsh fake news campaigns. Estonia appeared to answer in a soft manner by raising awareness campaigns, financing independent fact-checkers, and reinforcing critical infrastructure through the combination of indigenous efforts and cooperation within the NATO alliance (eg. CCDCOE in Tallinn). Ukraine being confronted with waves of disinformation during wartime provided a completely opposite approach to counter the third-party influence. Among the most prominent methods were building a counter-campaign and bandwagoning on the influence of aligned powers. This paper will determine the main tools used in both cases, describe short-term and long-term gains, concluding with recommendations on how to improve the future mitigation of malign Russian influence.

* 2023 Think Visegrad Non-V4 Expert Fellow at the Research Center of the Slovak Foreign Policy Association, Bratislava (Slovakia) and PhD candidate at Charles University Prague

This analysis was produced within the Think Visegrad Non-V4 Fellowship programme.

Introduction

Barely anyone took it seriously when the director of the East German Foreign Intelligence Department X cynically claimed: "Our friends in Moscow call it 'dezinformatsiya.' Our enemies in America call it 'active measures,' and I, dear friends, call it 'my favorite pastime.'"[1] The history of the 20th and 21st centuries has demonstrated that the importance of disinformation has been growing steadily. Enabled by many factors such as technology and mass media, disinformation evolved from an interesting hobby of lean intelligence officials to a mid-level strategy employed not solely by vivid autocracies.

Although we tend to often merge the words Russian and disinformation, it is obvious that many countries beyond the heartland of the "awaken bear" utilize and benefit from similar efforts.[2] Nevertheless, when we say Russian disinformation, we emphasize a comprehensive, strategic, systemic, and long-standing devotion of Russia to sophisticate it, consequently increasing its power projection abroad. This policy paper builds upon the two main pillars. First, it deals with Russian disinformation in a processual, disruptive manner, analyzing simultaneously the impact on target states and the very perpetrator. Second, it applies the approach to the two very different, yet somewhat similar cases of Russian disinformation campaigns in Estonia and Ukraine. The ultimate aim of the paper is to detect, enlist, and compare the strategies of the two countries to counter disinformation. Based on that, it will be possible to craft a list of recommendations on how to improve those responses.

This paper operates in specific geopolitical settings of resurgent and revisionist Russia, increasingly isolationist US, and declining European power. Strategic struggles are out of the scope of the study, but they are important because we can trace disinformation historically through the Russian state apparatus while noticing that the periods of their increased activities in the camp were reserved for the state of global political turmoil.

A legendary diplomat George Kennan in the famous Long Telegram convincingly warned about the implications of Russian presence abroad and their nascent hybrid subversive tactics. He wrote that Russia will use covert means "[t]o undermine general political and strategic potential of major western powers. Efforts will be made in such countries to disrupt national self-confidence, to hamstring measures of national defense, to increase social and industrial unrest, to stimulate all forms of disunity…[p]oor will be set against rich, black against white, young against old, newcomers against established resident, etc."[3] The recent history of Russian meddling in the domestic affairs of other countries confirms the aforementioned, starting with the conflict in Georgia in 2008, going over the annexation of Crimea and separatism in the East of Ukraine, just to end with an attempt at a full-scale invasion on Ukraine. Baltic countries, particularly Estonia,

[1] Bohnsack, G., Brehmer, H. (1992) Auftrag: Irreführung: Wie die Stasi Politik im Westen machte. Carlsen, Hamburg, p. 19.
[2] For the US utilization of disinformation strategy, look at Bittman, L. (1990) The use of disinformation by democracies. International Journal of Intelligence and Counterintelligence, 4:2, p. 243-261.
[3] Kennan, G. (1946) The Long Telegram. Available at: https://nsarchive2.gwu.edu/coldwar/documents/episode-1/kennan.htm

have been regular suspects for Russian malign influence, primarily because of their territorial proximity and large Russian-speaking minorities. All of this indicates that the study of Russian disinformation is a very relevant topic, both in policy and strategic terms.

This paper will proceed in six parts. The first part deals with the examination of the main concepts used throughout the work such as the very disinformation, but also disruption, whole-of-society, and strategic offspring. After that, traditional and technologically transformed Russian disinformation is analyzed, to discover its structures, methods, tools, and enabling factors. The third part introduces the case of Estonia, digging deeper into the background rationale for Russian disinformation campaigns, and main narratives, while putting emphasis on the counter disinformation efforts. The fourth part does the same with the case of Ukraine. The fifth part compares the two approaches qualitatively. Finally, the conclusion offers a set of recommendations of what are the foundations for a more effective approach to countering disinformation.

The study of disinformation

Although it would be intuitive to link disinformation to the period of expansion of digital technologies, globalization, and connectivity, the phenomenon has much older roots. In the most generic sense, we can claim that the appearance of disinformation corresponds to the appearance of the communication cycle. However, not before the early 20th century did organized and systematic efforts to proliferate disinformation exist in a top-bottom manner, for it to serve a designated purpose. Arguably some of the oldest examples of disinformation are Sisson documents, Operation Trest, the Tukhachevsky affair, Operation Bodyguard, and Operation INFEKTION. Here, three of them will be briefly touched upon to describe early tools used by states to achieve a plethora of goals.

Sisson documents are a set of forged papers collected by a US official, a member of the infamous Committee of Public Information, in 1918.[4] The purpose of the Committee and the very documents was to increase the enthusiasm for the US war efforts in World War I. Sisson allegedly obtained documents proving that Soviet leaders were just German puppets in financial and military terms, therefore discrediting the Russian Revolution. Papers were published in the US by almost every media outlet without questioning the content. Many decades later, it will be proven that the papers were fake. Operation Bodyguard was a disinformation effort of Allied Forces in WWII to conceal the date and location of what would later become known as Normandy landings.[5] German state apparatus believed in much of this information and was left in operational discrepancy and low combat alert when the actual landings happened. Operation INFEKTION was a campaign created by the Soviet intelligence service (KGB), trying to prove that the HIV virus had been

[4] Hamilton, J., Georgacopoulos, C. (2021) The Sisson Documents and their 'distinguished place' in the history of disinformation. Intelligence and National Security, 36:6, p. 881-897.
[5] Fallis, D. (2015) What is Disinformation. Library Trends, 63:3, p. 402.

invented by the US as a part of the biological weapons development scheme.[6] The best witness of the robustness and importance of the campaign was the fact that the US developed a whole counterstrategy, funding novel major institutional solutions. Expressions used to describe these rudimentary disinformation campaigns were propaganda, deception, distraction, counterintelligence, and many more.

Rather than trying to define it, we should stress certain constitutive elements of the notion of disinformation.

Disinformation is information

While it may sound tautological, fake, bent, doctored, or outright nonsense information is still a piece of information. The truthfulness and instrumental deliberation of information cannot negate its value.

Disinformation is misinformation

If we use misinformation for any false or inaccurate information, then disinformation is a specific case where inaccuracy is the very aim of communication. The deliberation of spreading fakes led many to claim that disinformation is essentially a 'particularly problematic' form of misinformation.[7]

Disinformation is communication

Aside from the basic fact of transmitting a message, disinformation is a part of strategic and corporate communications. Bennett and Livingston even talk about disruptive communications utilized by many actors across the societal spectrum.[8]

Disinformation is part of hybrid warfare

All of the aforementioned would lead toward the analytically shallow media or narrative analysis. As will be seen later, disinformation must be treated as a part of a larger network of concepts possibly united under the cloud of hybrid warfare. Those include cyber-attacks, hacking, information warfare, critical infrastructure protection, weapons of mass disruption, etc.[9]

Disinformation is a weapon

Every part of warfare, even in the cyber sphere, should be considered as a weapon. If we add that the aim of disinformation is often to harm others, the situation is much clearer. Historical examples

[6] Boghardt, T. (2009) Operation INFEKTION Soviet Bloc Intelligence and Its AIDS Disinformation Campaign. Studies in Intelligence, 53:4, p. 1-24.
[7] Fallis, Ibid., p. 402
[8] Bennett, W., Livingston, S. (Eds.). (2020). The Disinformation Age (SSRC Anxieties of Democracy). Cambridge: Cambridge University Press, p. 8.
[9] Alberts, D. (1996) Defensive Information Warfare. National Defence University; Gerrits, A. W. (2018). Disinformation in International Relations: How Important Is It?. Security and Human Rights, 29(1-4), p. 5.

of campaigns against Jacobo Arbenz and Salvador Allende provide many pieces of evidence for the claim of weaponized disinformation.[10]

Disinformation is strategy

Non-accidental nature, existence of purpose, robustness, and effectiveness, are all reliable indicators that disinformation is either a strategy on its own or part of more comprehensive mid-level strategies and policies.

After framing the notion, it is important to stress that the three distinctive characteristics of disinformation are deliberation, consequences, and endurance. While the first was already mentioned, consequences as both direct and indirect effects are the most precise measurement of disinformation. Among the most prominently mentioned in the literature are: political polarization, declining trust in democracy, rise of authoritarian regimes, creating confusion, spreading information paralysis, discrediting individuals, disrupting debates, weakening confidence in financial markets, and inciting fears from global conflicts.[11] The range of consequences indicates that disinformation is not just global or significant, but a concept deeply embedded within socio-political apparatuses. A corollary of such a claim is its permanent character. Namely, disinformation is not there as an isolated advancement of particular interests possible to counter on an ad hoc basis. It is rather a game in town destined to stay and be omnipresent for a long time, always engaged in innovation of its core tenets.[12] It is also possible to consider disinformation as an always-present part of the subversion process described by the Soviet dissident Yuri Bezmenov. He claimed that the impact on a nation is being left in four long phases (multiple decades) ranging from demoralization to normalization.[13] Disinformation is sown into every stage of the process and can be seen as a factor that enables an environment for ideological subversion.

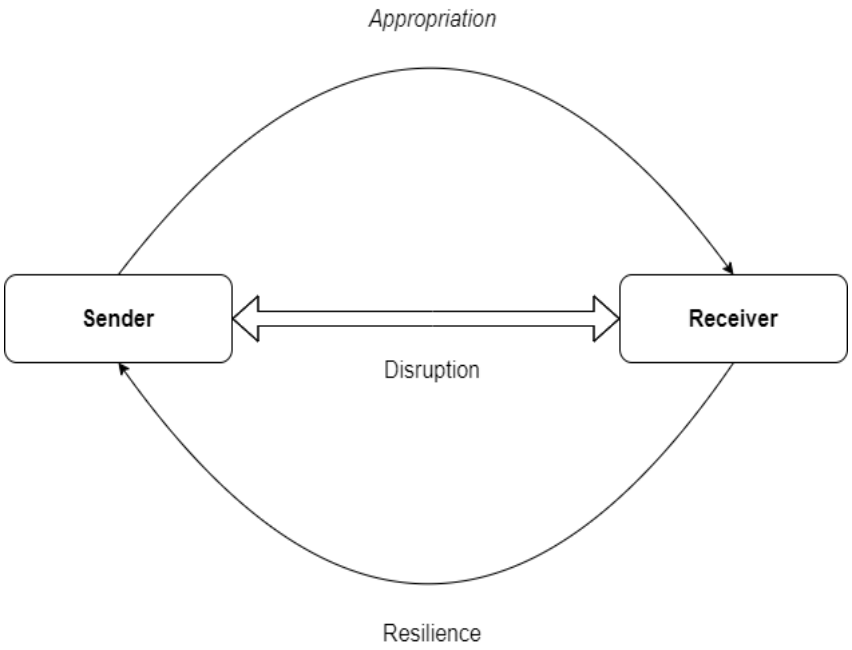
Introducing disruptive disinformation

Conflation in the usage and interpretation of a notion usually diminishes its value. Disruption has certainly been one of those that experienced resurge in recent years. Motivated by the staggering technological advancement and apparent societal impact, it has spread all over multiple domains and professions to indicate a sudden change in manifest behavior. Nevertheless, disruption is always taken as a mono-directional phenomenon. This comes from economics where the prophet of disruption Clayton Christensen described it as a purge of companies unable to achieve a

[10] For more information about those cases look at Ferreira, R. (2008) The CIA and Jacobo Arbenz: History of a Disinformation Campaign. Journal of Third World Studies, 25(2).; Carter, D. (2014). Weapons of disinformation. Index on Censorship, 43(1), p. 41-44.
[11] Gerrits, Ibid., p. 6; Bennet and Livingston, Ibid., p. 3; Thomas, T. (2020) Three Discussions on Russians Concepts. The Mitre Corporation, p. 27.
[12] Bittman, L. (1985) The KGB and Russian Disinformation. Pergamon Defense Publishers, p. 45.
[13] Charles Rivers Editors (2020) Yuri Bezmenov: The Life and Legacy of the Influential KGB Informant Who Defected to the West. Independent Publisher.

sufficient level of resilience to remain intact from the forces governed by disruptive technologies.[14] In this paper, disruption is considered a two-way process. Rather than talking about a disruptive event, antecedent, and subsequent behavior, we will read disruption as a relatively stable process in which both the disruptive and disrupted actors get changed. That is why the two pillars of the method presented in this paper are analysis conducted on multiple levels and a whole-of-society approach.

Figure 1. Disruptive disinformation process



Namely, in order to understand Russian disinformation applied to a particular country, a study needs to be simultaneously focused on the provider and the receiver. In other words, the origin and target country cannot be considered separately. Following the above-mentioned dictum, disruptive disinformation is the one that affects the target country of Russian disinformation, but through the very process, it affects Russia as well. This is mainly done through the forces of resilience. The more resilient a target country is, the more visible the backfire will be. Since disinformation cannot win a conflict or besiege a country on its own, the game of resilience is never win-lose. Therefore, the whole point is in prevailing over the other side in a relative sense. Even measuring the success of disinformation would require focusing both on the benefits for the sender and the level of misleading the receiver.

[14] Christensen, C. (1997) The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. Harvard Business School Press; Christensen, C., Horn, M. (2008) Disrupting Class: How Disruptive Innovation Will Change the Way the World Learns. McGraw-Hill.

The interplay of the two levels leads us towards the second pillar, the whole-of-society approach.[15] To consider disinformation exclusively as a matter of mass media or shadowy governmental structures definitely misses the target. If vertically we have multiple levels to analyze, then horizontally different domains demonstrate that disinformation affects many more than particular socio-political structures. The domains under observation are government (with intelligence apparatus), military, NGO, private sector, academia, and population. Each domain can legitimately serve as a proliferator of disinformation and combatant against it. While the first four domains are pretty self-explanatory, there is a need to clarify why academia and population fill in the list. As will be seen later in the text, staff and students at universities have been forming fake epistemic communities through various channels, funding and publishing pseudo-academic content, working directly for the benefit of proliferators of disinformation.[16] Not less important, academic institutions and individuals were prominent targets of malign efforts. As Timothy Thomas writes, if a government spreads fake information, then the population is prone to do the same.[17] Consequently, in the conditions of ideological homogenization and a state of exception (wars, pandemics, etc.), the whole-of-population can, even unconsciously, be turned into a sender of disinformation.

Figure 2. Disinformation across the domains

[15] Boghardt, Ibid., p. 1-2.
[16] Estonian Foreign Intelligence Service (2023) International Security and Estonia. EFIS, p. 49.
[17] Thomas, Ibid., p. 27.

Traditional and modern Russian disinformation

To compile a comprehensive list of actors, methods, tools, platforms, tactics, and strategies vital for Russian disinformation would be all but impossible due to its constantly evolving and still partially classified nature. However, it is feasible to follow the underlying logic, but also to describe its manifest evolutionary appearance. Therefore, this section will compare methods and tactics of Russian disinformation in the times of the Cold War and roughly the period after the fall of the Soviet Union. The former was an era of setting strategic aims, followed by the primary proliferation of disinformation and the development of various tools to be used for decades. The latter period is that of technological transformation of disinformation, but also careful adjustment of Russian strategic aims to a new set of geopolitical circumstances.

Thanks to numerous defectors from Soviet intelligence and politics, we have the opportunity to catch a glimpse of the modus operandi of the KGB in the sphere of disinformation. Most notably, Ladislav Bittman and Yuri Bezmenov revealed a strategic and operational umbrella under which so-called active measures were developed. While Bezmenov focused mainly on propaganda and ideological subversion, Bittman drew a complete picture from the level of actual application of an idea all the way to the state apparatus sitting behind it.[18]

If we are to start from the propaganda as the narrow form of disinformation (part of active measures) during the Cold War, it was conducted as a series of inputs from the government and intelligence to the subservient media outlets and cooperative foreign correspondents. Boghardt described the process in a couple of main phases.[19] As decision-making in the USSR was centralized, propaganda naturally started with the strategic approval of the government to ensure the alignment of further actions with the official policies. After that, agents tasked to follow the press would generate ideas on what content can be exploited as an active measure. Then it would go back to the administration where preparations, translations, and targeting take place. The usual way of doing things was to plant the content to a non-Soviet media outlet in the form of anonymous letters or tips so that a link to Moscow could be avoided. By the nature of mass media, the content is spread throughout the target audience and finally appropriated by the Soviet officials to be referenced as a non-Soviet legitimate source. The INFEKTION campaign mentioned earlier is the most prominent example of such a course of action. There were three types of propaganda: white, grey, and black. They were differentiated by the level of involvement of physical assets (such as fellow communists abroad or clandestine media organizations) in the proliferation of propaganda.

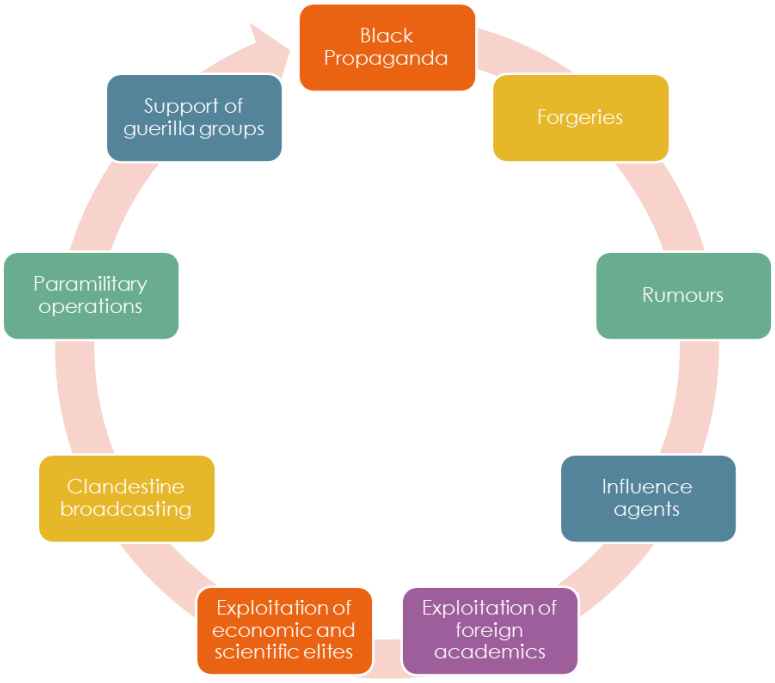
Propaganda was a prominent part of disinformation efforts labeled as active measures. Those were activities designed to promote the Soviet Union abroad and to bring the image of the

[18] Bittman, Ibid.; Griffin, G. (1984) Deception Was My Job: The Testimony of Yuri Bezmenov, Propagandist for the KGB. The Reality Zone.
[19] Boghardt, Ibid., p. 3.

Western world into doubt. Soviet state apparatus counted on a plethora of individuals outside of their country to be accomplices in fulfilling the tasks. The name given to those individuals is influence agents. As of today, they have been officials sufficiently high in the hierarchy to be able to influence public opinion in other countries. Here we talk about government officials, journalists, academics, industry leaders, or even charismatic persons from the ordinary population.[20] A very interesting feature of influence agents who would proliferate disinformation is that they did not have to be fully in agreement with Soviet policies. Lack of ideological compliance has been either compensated by financial rewards or imposed by blackmail.

Bittman diligently enlists active measures, among which we can see a: a couple of violent methods, not traditionally considered as disinformation: 'black propaganda; forgeries; rumors; use of front organizations; influence agents; exploitation of foreign academic, economic, or scientific elites; clandestine broadcasting; paramilitary operations and deception; support of guerrilla groups; and such terrorist activities as kidnappings and assassinations.'[21] This is particularly important to grasp how intertwined are the socio-political domains and that disinformation cannot be treated separately from the whole. It is a matter of fact that the advancement of technology has made these methods much more subtle and sophisticated, but the foundation of activities essentially remains the same.

Figure 3. Soviet active measures



[20] Bittman, Ibid., p. 61.
[21] Ibid, p. 43-44.

Soviet planners, similarly to their Russian counterparts of today, have never believed that disinformation alone could win the Cold or any other subsequent war. The aims of active measures were adjusted accordingly to achieve limited results and be supplementary to other strategic actions. If we take in mind that active measures were planned to last sometimes even multiple decades, the overall aims can be classified into short and long-term. Measuring the success of disinformation in the short term takes into account how much attention has been given and the dimensions of discussion provoked by a certain action.[22] Since the Cold War was marked by a very polarized political environment, a special emphasis was put on the tone of these discussions in a target country, searching for positive views on the Soviet Union and negative on the Western counterpart. On the other side, long-term effects were measured by the changes imposed by a target government to its strategies and policies. In each change, the Soviets saw a window of opportunity. An already used example of Operation INFEKTION can again serve the purpose. Namely, the US administration under the waves of Soviet active measures was forced to hold numerous congressional hearings, publish tons of announcements, form interagency investigative teams, and even engage in international cooperation so that the impact of disinformation could be mitigated. Despite all of the efforts to counter active measures, public opinion has remained largely influenced by it, to the level of a quarter of the US population believing that AIDS is a manmade laboratory product designed as a biological weapon.

Emerging and disruptive technologies enabled disinformation to travel faster than ever. Since the end of the Cold War, the physical presence of an asset has not been the necessary condition for disinformation to function properly. Wide usage of the internet, universal connectivity, and ultimately social networks, opened many niches previously unavailable to creators of disinformation campaigns. Bennet and Livingston identify characteristics of the internet that have been most significant in this sense: the scale of its reach, the microtargeting, the granular level of surveillance, and the global preeminence of US-based platforms.[23] The US dominance in internet-related technologies has been a double-edged sword. On the one side, it enables global power projection and market dominance, while on the other side, it renders the US more vulnerable to third sides with deliberation to exploit the available platforms. As can be imagined, Russia did not miss the opportunity to use the internet to render information noise.

One of the most important features of technologically transformed Russian disinformation is the inability to counter it traditionally. As with any other security threat, it is all but impossible to fight the invisible enemy. Tracing the real identity behind an army of bots, sockpuppets, and hackers is a daunting and often unrewarding task. This is especially true when their opinions are proliferated by widely available instruments of Russian propaganda such as RT and Sputnik, even more, amplified by the outlets within a target country.[24] A range of different techniques used is best described in a set of concepts: masking, repackaging, dazzling, mimicking, inventing, and

[22] Ibid., p. 56.
[23] Bennet and Livingston, Ibid., p. 169.
[24] Bennet and Livingston, Ibid., p. 7.

decoying.[25] The dimensions of socio-political impact will be demonstrated in the two cases in the next chapter.

While overall tactics of disinformation remained similar to the Cold War period, its manifestation and strategic aims are largely different. The advancement of technology has inevitably transformed democratic processes bridging the gap between political elites and the population. That generated a completely novel form of disinformation called meddling in electoral affairs. The most notable example that still produces a lot of controversy are US elections of 2016. In that case, Russian disinformation has been accused of manipulating information, publishing forged emails, and falsely attributing statements at the outset of the elections to interfere in the democratic process. This significantly reduced confidence in the US democratic order based on rules and institutions. A scholarly article considers this to be a technologically-driven art of spreading damaging information to discredit enemies.[26] Techniques utilized to achieve this information confusion went from automated bots and impersonation accounts, all the way to misuse of cutting-edge Artificial Intelligence (AI) tools to create deepfakes.[27] Aside from the obvious loss of confidence in a democratic system, Russian disinformation enriched by the technological factor aims to discredit certain political figures deemed prone to destabilization, alienate citizens from its legitimate government, and cause an overload of information within certain echo chambers, most often those on conspiracy theories or rich in other anti-mainstream narratives. Furthermore, full achievement of these aims will cause a chain reaction and provoke other, even more generic consequences. Some of the highest-order aftermaths are instigating permanent fear from global conflicts (third world war, nuclear catastrophe, hunger, natural disasters fostered by humans), loss of confidence in financial markets (financial and social insecurity as the most prominent security risks of the 21st century), and confusion of the way on how to distill propaganda and disinformation from legitimate sources of information.

Aims of Russian disinformation in the era of advanced technology fit into a series of strategic offsprings or indirect motivations.

Asymmetric balancing

Disinformation serves to leave a footprint abroad with relatively scarce resources. Asymmetry is measured as a difference in the effort to conduct a certain activity and the volume of its consequences. In the case of Russia, disinformation and hybrid tactics are used to make up for the possible lack of military power or global power projection. Therefore, strategic aims are achieved within the scope of 'high-tech poor-man tactics.'[28] To use the example of meddling in the US election of 2016, a simple forgery of an email can reverberate throughout the system and cause irreparable harm to the image of a politician. Asymmetry is obvious while balancing means that attribution of a disinformation activity will inevitably provoke a deep socio-political division and

[25] Bowyer Bell, J., Whaley, B. (1991) Cheating and Deception. Transaction Publishers.
[26] For the notion of Kompromat look at Hamilton and Georgacopoulos, Ibid., p. 893.
[27] Fried, S. (2019) Hearing on Russian Disinformation Campaigns. US Congressional Hearings, p. 3.
[28] Gerrits, Ibid., p. 10.

benefit the sender. When it comes to the inherent limitations of Russian disinformation, Pomerantsev and Weiss notably wrote: 'Moscow can generate chaos in Ukraine, destabilization in the Baltic States (part of a larger effort to influence and protect the perceived interests of Russian-speaking people in former Soviet republics), political influence in Eastern Europe, confusion in Western Europe, and distraction in the United States.'[29]

Information superiority

Through the manipulation of information space abroad, Russia seeks to gain control over the behavior of other states. In the era of the Soviet Union, it was much easier because centralized policies were distributed to near abroad, and then naturally multiplied. Nowadays, Russian ambitions are much more limited. Instead of the full grasp, there is the tendency to turn states away from their planned direction. However, knowing that many states have been building layers of resilient structures to prevent such actions in the future.

A new type of deterrence

Russian strategist Tsymbal in an official document drafted as early as 1995, states that Russia retains the right to conduct a preventive first strike against the information warfare systems of an opponent, followed by an attack against the opponent itself.[30] Other strategies mention 'strategic operation to destroy critically important facilities (SODCIT)' as yet another type of operation. Those are textbook examples of deterrence by punishment. Moreover, disinformation is proliferated in a way to leave the impression that the Russian apparatus is omnipotent and can influence whatever, wherever, and wherever it wants. Useful in both offensive and defensive terms, this modality of deterrence proves to be efficient in countries with parochial political cultures.

A playground for emerging technologies

One of the legitimate aims of Russia is to use the disinformation realm to test and operationally utilize products of disruptive technological innovation. Technologies such as quantum cryptography and psychotronic tools are among those potential silver bullets to be researched. Artificial intelligence has already found its use in Russian disinformation campaigns within the practices of big data analytics and the generation of deepfakes. Every Russian technological sophistication in this direction causes deterioration of the existing defenses of other states, relatively increasing the speed of the spread of disinformation when compared to the societal response.

[29] As quoted in Gerrits, Ibid.
[30] Tsymbal, as quoted in Thomas, Ibid., p. 10.

Rationale for the cases

The best methodological question one can ask when designing a study of two cases is: why two and why the two? Here the answer is pretty simple and lies in the simultaneous similarities and differences between them. Estonia and Ukraine have been fertile playgrounds for Russian disinformation. Nevertheless, the level of Russian ambitions within each of them varies greatly due to specific circumstances. These two cases will enable us to reflect upon the common underlying logic and also to contrast approaches when it comes to counter disinformation strategies.

There are five main similarities between the two cases. First, both countries are physically close to Russia and have robust Russian speaking minorities. While in Ukraine the minority is spread throughout the country, the biggest concentration is in the eastern flank (Donetsk, Luhansk) in the proximity of the Russian border. In Estonia, the Russian minority is mainly concentrated in the far east of the country, again near the border, in the region of Ida-Viru and its largest city Narva. As can be imagined, a Russian speaking minority represents a significant asset for any disinformation campaign launched from Kremlin. Second, both countries belonged to the so-called Russian sphere of influence. Despite regaining independence after the Cold War, both have traditionally been involved in state arrangements with Russia since the Middle Ages, with the latest one being the Soviet Union. Many Russian politicians and strategists still claim their right to those territories. Third, the countries are connected through a strong anti-Russian sentiment stemming from the fact of unequal treatment and discrimination in the Soviet Union and beyond (for example, Holodomor in Ukraine). Fourth, despite the strong sentiment, Russian media are still present and allowed to operate. Save for the period in Ukraine since the beginning of aggression in 2022, Russian outlets have been able to function and disseminate official propaganda without major restrictions. Fifth, aside from the media, Russia operates in both countries through civil society organizations, the Russian orthodox church, and many Kremlin-backed funds. All of this represents an enabling environment for disinformation campaigns.

The biggest and most obvious difference between the cases is the fact that Ukraine has been in the state of war against Russia since 2022, while in a state of limited conflict and heightened tensions since 2014. On the other side, Estonia was never seriously threatened in the traditional military sense. This difference also conditions many varieties in responses to Russian influence but does not invalidate comparative efforts which are deprived of axiological burden. Following the same line of thought, through the extended deterrence umbrella of the NATO alliance, Estonia has regularly gained allied help in terms of infrastructure and know-how. Ukraine has been deprived of that option. Moreover, the two countries differ in the levels of political culture and state of democracy. While Estonia evolved into one of the most successful European states with a digitalized administration attractive for digital nomads and beyond, Ukraine has been repeatedly described as a country of endemic corruption and hybrid democracy. Finally, Ukraine allowed Russian oligarchs to penetrate the country with their business, leaving it open for subsequent permeation of Russian influence. Estonia demonstrated a much more strict approach, partially due to the obligations stemming from the EU membership.

The pattern for both cases will be similar. In the beginning, the main Russian strategic narratives will be described. After that, the structure of disinformation campaigns will be laid out together with the main actors. In the end, a bulk of attention will be dedicated to the respective counter disinformation methods identified in each of the cases.

Estonia reacts

Strategic narratives

It is beyond a doubt that historical narratives play a significant role in seeking sources of legitimacy for disinformation campaigns. Some of the narratives present in Estonia go as far as to claim that 21st century will mark one thousand years of Russian Estonia.[31] Nevertheless, the bulk of historical considerations are connected to the Second World War, the alleged Soviet liberation of the country, and nostalgia for the subsequent life under the communist dictatorship. Russia even formed a Commission to prevent the falsification of history and put an end to the heroization of Nazism.[32] 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 witnesses that Russian speaking minority in Estonia gave almost unified answers to questions about history, indicating the success of state-based propaganda.[33]

Particularly conducive to the alternative historical narratives is Russian speaking minority. While majority of them have never been to Russia (despite many of them holding Russian citizenship), they continue to unconditionally support Russian actions and condemn Estonian. Several reasons exist for this, among which the main is the fact of not speaking Estonian language. A major consequence of such a self-imposed isolation is inextricable tie to Russian information space.[34] This turns the Russian minority into grey-zone people who do not have a wish to move to Russia due to arguably lower life standard, but also do not want to be fully incorporated into the Estonian society. This mutually hurting stalemate has been exploited by Russia through waves of disinformation that incited feeling of insecurity into Russian minority, predominantly about the allegedly neo-Nazi discriminatory treatment of Estonian government towards them.[35]

The turning point in Russian-Estonian relations happened in 2007 when Estonian administration decided to move Bronze solider monument from the centre of Tallinn to the city outskirts.[36] For

[31] 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.
[32] Security Police of the Republic of Estonia (2010) Annual Review, p. 13.
[33] Teperik et.al. (2018) Virtual Russian World in the Baltics. NATO STRATCOM, p. 7.
[34] Mattiisen et.al. (2021) Russia's Influence and Presence in Estonia. European Reform, p. 24.
[35] Teperik (2022) Disinformation networks of pro-Kremlin proxies in Estonia. International Centre on Defence and Security, p. 3.
[36] For detailed motivation and overview of events look 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.

Russians this monument is a symbol of WWII victory and liberation of Estonia, while the other side has largely different, even opposite opinion. This move provoked harsh protests both in Estonia (Bronze night) and Russia (siege of the Estonian Embassy in Moscow). In the aftermath of the monument relocation, Russia launched a first information (cyber) attack against a nation state. Coupled with aggressive disinformation, these attacks targeted government, banks, police, media, and beyond.[37] The attacks significantly crippled the ability of Estonia to deliver services and were interpreted as a warning that immediate action needs to be taken. The first reaction came from NATO embodied in the establishment of Cooperative Cyber Defense Center of Excellence, which is even today at the forefront of combating Russian malign influence[38].

The structure of Russian disinformation in Estonia

The structure of Russian disinformation campaigns in Estonia is multi-layered, complex, and challenging to fully grasp. However, most of the main actors and institutions can be identified.

Majority of media outlets tasked with spreading disinformation are under direct control of Kremlin and widely available in Estonia. Those are mainly traditional TV channels such as Perviy Baltisky Kanal (First Baltic Channel or PBK), RTR Planeta (Planet), and NTV Mir (World),[39] but also a range of media available through internet streaming. The propaganda is often hidden in entertainment shows and deals with a huge number of topics from history, over health (pandemics), all the way to providing genuine interpretations of current global geopolitical outlook. Media outlets count on deep socio-political polarization with the aim of spreading it and radicalize various groups to be more agitated against the Estonian government.[40] This is often labelled as psychological influence technique, a key for measuring success of disinformation together with level of disruption caused by software and hardware components. Recently, social networks (VKontakte, Odnoklassniki, Facebook, X, Telegram) became popular channels for quick spreading of disinformation. Particularly problematic are the so-called active ideological users who have large network of contacts and are prone to enlarge those networks in short periods of time.[41]

The second cluster is made up of NGOs and assertive diplomatic efforts. Pushkin Institute, the Baltic Youth Alliance, and the Reval Media Agency, are all NGOs tasked with gathering Russian population and spreading disinformation among them.[42] Through the legitimate civil society work, those organization have regular access to events all over Estonia, using the opportunity to diligently push for their agenda. As an intelligence briefing of Estonia services states, Russian Embassy in Estonia directly finances a plethora of festivals (Vivat Rossiya) and magazines (Baltiskij Mir), tasked with promotion of pro-Russian sentiment and spreading covert disinformation.[43]

[37] Thomas, Ibid., p. 33.
[38] Thomas, T. (2020) Estonia Reacts: Confronting Russian Manipulation Techniques. The MITRE Corporation, p. 3.
[39] Ibid., p. 5.
[40] Teperik, Ibid., p. 4.
[41] Teperik et.al., Ibid., p. 38.
[42] Thomas (2020) Ibid., p. 11.
[43] Security Police, Ibid., p. 9.

While those events and outlets can even serve as money laundering schemes, in the past they participated in created such assertive narratives such as neo-Nazi treatment of Russian minority in Estonia.

Of special importance are policies and organizations directly connected to Russian intelligence services, Russian compatriot policy and Russian Institute for Strategic Studies. The former is a policy of keeping Russian community in Estonia under granular control, therefore susceptible to every disinformation operation. Compatriots are under the direct scrutiny of the FSB. The importance of Estonia is indicated by the engagement of general Dmitry Milyutin, deputy director of the Department for Operational Information at the FSB, for overseeing the tasks regarding compatriot policy.[44] Think tank called Russian Institute for Strategic Studies has been a steady source of disinformation under the direct control of foreign intelligence agency SVR. The director of RISI is the former agency chief Fradkov.[45] RISI organizes many legitimate international conferences, finances foreign trips for researchers, opens new educational opportunities for Russian-Estonian exchange, etc. Certainly, this is all a cover for work on malign influence abroad.

Finally, somewhat less significant are traditional academic institutions and political parties. Many intelligence officers are taking high positions in the hierarchy of universities, particularly those in international offices. Through foreign exchanges they tend to recruit possible agents of influence abroad. Research institutions such as Institute for Baltic Civilizations have provided scientific cloak for historical and other disinformation narratives.[46] Political system of Estonia does not allow for parties to be directly financed from abroad, so the margin for Russia to influence this domain is significantly narrowed. However, a coalition partner in the government of Estonia in 2016 was Centre Party that spread pro-Russian propaganda and had an official partnership agreement with Putin's United Russia party.[47] It is a matter of fact that disinformation coming from the political parties in Estonia does not have even a fraction of influence as in other countries.

The structure of Estonian response

Estonia went to great length in order to formulate principles to counter disinformation. Those include whole-of-society since without integration it would be impossible to create a coherent system without domains prone to leakages. Some of the domains are more resilient than others, but the relative lack of resilience is compensated by the cross-domain protection. In this paper, four main pillars of Estonian approach to counter disinformation are identified.

Strategic communication and psychological defense

As non-physical, psychological component is essential for disinformation to function, the same goes for combating it. To mitigate effects of disinformation such as confusion and fear, but also

[44] International Security, Ibid., p. 48.
[45] Ibid., p. 50.
[46] All the research conducted by the Institute is available at: http://en.abfund.org/?page_id=155
[47] Mattiisen, Ibid., p. 22.

preclude Russia from achieving strategic aims, Estonia introduced a set of measures to raise the public awareness about those efforts threatening to undermine constitutional order and society as such.[48] The other side of the coin is strategic communication (STRATCOM) as a harmonization technique ensuring common response to external hybrid threats in political, economic, and defence spheres. They vital component of STRATCOM is the ability to communicate messages to the general population in a clear and credible manner. When considered together, those two represent sui generis 'perimeter defence,' or the primary level of threat neutralization once all the preventive and deterrent efforts failed.

Liberal media operations

While the most intuitive approach to combating disinformation in a media outlet would be to deny its operation, Estonia has been taking a completely opposite approach. Namely, throughout the country it is possible to follow Russian channels via main telecommunication operators. In the eastern part of the country, users do not have to be subscribed to a cable TV, they can follow Russian channels and listen to Russian radio without any additional equipment.[49] Since there was no wish of Estonian strategists to introduce any type of censorship, they decided to offer positive incentive by creating an Estonian TV channel in Russian language, a neutral alternative to Kremlin-backed disinformation outlets.[50] This represents a long-term solution because Russian speaking minority will need time to exit its echo chamber and accept novel solutions. Many would rush to claim that allowing Russian media to operate without barriers in Estonia means making itself more vulnerable to malign influence. However, emancipatory solutions proved to be more efficient in the conditions of organized and systematic response based on wide societal support.

Communicating values and societal resilience

Estonian mantra goes that its values travel faster than the Russian disinformation, which is a quite ambitious claim when we know a set of technological tools that disinformation campaigns utilize. Estonian state apparatus (regardless of the incumbent government) has been cultivating and supporting new generation of opinion makers and leaders with access to various communities, groups, and echo chambers.[51] The established networks have been growing steadily, turning into self-established cells with the ability to absorb and reject disinformation. More or less successful, these networks communicated values Estonian constitutional order, the importance of liberal democracy, and the paramount value of human rights. When all these principles and values are incorporated into a mindset, networks instigated by the opinion makers can be considered as a

[48] Committee on Democracy and Security (2021) Mission Report Estonia. NATO Parliamentary Assembly, p. 2; Irvee I., Jarold, U. (2021) Psychological Defence and Cyber Security: Two Integral Parts of Estonia's Comprehensive Approach for Countering Hybrid Threats. ICONO 14, Revista de comunicación y tecnologías emergentes, vol. 19, no. 1, pp. 70-94.
[49] Mattiisen, Ibid., p. 27.
[50] Thomas (2020) Ibid., p. 5.
[51] Teperik, Ibid., p. 4.

whole under the label of societal resilience.[52] This means capacity of Estonian society are sufficiently robust to counter disinformation without escalatory measures.

Civil-military cooperation

A part of this solution has already been tackled under the section of STRATCOM because it requires military and civilian sectors to cooperate. Here, it is emphasized in a different manner of reassurance policy. Namely, a range of activities have been aimed at inciting feeling of safety into the Estonian population. Starting with media literacy classes in elementary and high schools, going over fact-checking efforts and manuals on how to navigate the world of disinformation, just to end with such symbolic moves of deploying small number of NATO military forces to Estonia (trip-wire mechanism) and temporarily relocating government headquarters to the city of Narva.[53] Playing with the psychological component, this set of counter disinformation activities boost self-confidence of ordinary population, therefore making institutional responses much easier.

Ukraine fights

Strategic narratives

It is common knowledge that since 2014 Ukraine has passed through multiple stages of conflict with Russia. It started with illegal annexation of Crimea, went over Russia-sponsored separatists in the east of the country, just to end with a full-scale invasion initiated in February 2022. Beyond a doubt it took a long time and systematic planning to design such a course of action. Many authors claim that disinformation was a cornerstone as a set of strategies which would have enabled Russia to find surplus sources of legitimacy for its behavior.[54] Indeed, Russian disinformation campaign in Ukraine is so complex that untying all the knots is impossible without the extensive period over which many of the hidden agendas will be revealed. An interesting fact is that Russian campaign in Ukraine has been marked by the utilization of both traditional and technologized disinformation. In other words, active measures goes hand in hand with more sophisticated disinformation tactics.[55]

As in the case of Estonia, many historical narratives are used to claim that Ukrainian independence is a hybrid anti-Russian concept. Those narratives include centuries old Kievan Rus mythology, but much more prominently the folklore from the WWII. The main narrative stemming from that part of history are that all Ukrainians of today are followers of Stepan Bandera. Furthering the metaphors of Nazism, Russia claims that Ukraine is a neo-Nazi puppet state conducting genocide

[52] Jermalavicius, T., Tarmak, V. (2012) Towards a resilient society, or why Estonia does not need 'psychological defence'. International Center for Defence Studies, Tallinn.
[53] It is interesting to note that British soldiers deployed to Estonia have also been targeted by Russian disinformation, primarily intended to discredit their image of a professional army by staging bar brawls or involving soldiers in honey traps, just to disseminate the content via social networks. For more on this look at 2(9)
[54] Gretskiy (2022) Russia's Propaganda War. International Centre on Defence and Security, p. 1.
[55] NATO STRATCOM (2015) Analysis of Russian Information Campaign against Ukraine. Centre of Excellence, p. 6.

against Russians and that its state ideology is based on Russophobia.[56] Another omnipresent narrative is certainly the one on Soviet liberation and nostalgia for the Soviet Union as a heaven for all the Slavic people. Strategic narratives of disinformation are that Russian fight in Ukraine is a protracted fight against Nazism and any rapprochement to the West will inevitably bring instability to Ukraine.[57] Those are often supplemented with lower-order narratives of clash of civilizations, Ukraine as a part of Russian world, divisions of the West make Russian actions legitimate, etc. Through dissemination of the falsehoods, Russia has been seeking to deepen socio-political divisions in Ukraine and exploit its weaknesses.

As the military actions progressed, a bulk of narratives focused on Ukraine being military incorporated by the NATO alliance.[58] Especially after the Western countries decided to send military help to Ukraine, this storyline flourished to the level of declaring Ukraine to be a NATO puppet state used to provoke Russia at its very borders. Another militarized narrative has been present since the conflict in Donbas, focusing on tarnishing the image of Ukrainian armed forces, declaring them to be drunkards, rapists, criminals, robbers, committing war crimes against civilians.[59] The obvious deliberation of those forgeries was to diminish the level of combat readiness, encourage defections, and lower the level of morale. Finally, since the invasion of 2022, Russian disinformation focused on providing alternative facts regarding war crimes such as Bucha massacres, spreading lies about Ukraine getting biological weapons from the US to destroy Russia or NATO setting up a military base in Odessa.

The structure of Russian disinformation in Ukraine

When analyzing the annexation of Crimea, Sazonov et.al. noticed that variety of influence agents was surprisingly wide. Starting from NGOs, going over mass media, just to end with networks of traditional spies and malign actions of the Russian Orthodox Church.[60] When it comes to the structure of Russian disinformation in Ukraine, every stage of the campaign saw different actors and methods, depending on the intensity of the conflict. Here, we will formulate main clusters common to all the phases, with the special emphasize put on social networks as the most innovative disinformation aspect.

Arguably the most significant factor in spreading disinformation in Ukraine have been media outlets. Both Russian (RT, Pervyy Kanal, Rossiya 1, Rossiya 2, LifeNews, NTV) and Ukrainian pro-Russian (Inter, Channel 17, Channel 112, Ukraina24), worked together to form a bubble of harmful fake and alternative news. During the separatist outbreak in the east, regional information channels played a significant role in disseminating narratives against the regular Ukrainian army

[56] Sazonov et.al. (2017) Russian Information Operations against Ukrainian Armed Forces and Ukrainian Countermeasures (2014-2015). ENDC Occasional Papers, p. 55.
[57] NATO STRATCOM, Ibid., p. 16-21.
[58] Gretskiy, Ibid., p. 2.
[59] Sazonov, Ibid., p. 56.
[60] Ibid., p. 58.

(Lugansk24, Novorus.info). The strategy of supplying overabundant amount of information impossible to fight or debunk was labelled as firehose of falsehoods.[61] Finances for these medial outlets often came directly from the business of Russian oligarchs, which are under the tight control of Kremlin.[62] Many techniques were used to create fake news. For example, an actress has been used to play multiple roles during the Crimea annexation (protestor in Crimea, a resident of Odessa, crying mother of a Ukrainian soldier, etc.) so that fabricated stories can be released.[63] A Russian TV network run by the government once posted a video where Ukrainian military is seen using phosphorous bomb against the civilians. After debunking, it became clear that the video was in fact from the war in Iraq in 2004.[64]

For the first time, the internet as an enabling environment for disinformation could be fully grasped during the conflict in Ukraine. Main actors to spread disinformation were paid trolls, groups of people who abuse chat rooms, comments, and discussion forums in order to spread the assigned agenda.[65] Moreover, disinformation spread through fake accounts on social networks disseminated much faster due to its alleged credibility. An investigative article from 2013. Witnesses that even before the military actions, Russian was organizing trolls in the so-called troll farms.[66] Among the most prominent troll farms was Internet Research Agency owned by the later famous leader of the Wagner mercenary group, Prigozhin.[67] Trolls were often paid to post as many as 100 comments per day which certainly causes jamming within the communication channels. Another interesting strategy to proliferate disinformation is typo squatting, a deliberate misspelling in the name of legitimate websites leading a user towards a completely doctored content.[68] Many Ukrainian public institutions have been hit with this disinformation method.

Having in mind sensitive nature of the data in the ongoing conflict, it is impossible to get to know all the intelligence actors (FSB, GRU, SVR) participating in the disinformation campaign. From the available data, certain impact has been made by the pro-Russian political parties in Ukraine (For Life), Russia-based pseudo NGOs (Rossotrudnichestvo, Compatriots Living Abroad, Russkiy Mir), mobile network operators (MirTelecom), and physical propaganda coming from loudspeakers in the border regions.[69] However, influence of these factors is rarely at the level higher than marginal because of the wartime conditions and much stricter governmental control over direct Russian influence on the ground.

[61] Ferencik, A. (2022) Putin's Disinformation & Misinformation Campaign. Europeaum Centre, p. 4.
[62] Sazonov, Ibid., p. 61.
[63] Cordesman, A. (2020) Chronology of Possible Russian Gray Area and Hybrid Warfare Operations. Center for International and Strategic Studies.
[64] Ibid.
[65] Kowalski (2022) Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses. OECD>
[66] As quoted in NATO STRATCOM, Ibid., p. 22.
[67] https://edition.cnn.com/2023/02/14/europe/russia-yevgeny-prigozhin-internet-research-agency-intl/index.html
[68] Kowalski, Ibid., p. 3.
[69] Meister, S. (2015) Isolation and Propaganda: The roots and Instruments of Russian Disinformation Campaign. Transatlantic Academy, p. 7-8.

It is important to stress that majority of the disinformation campaigns were possible because Russians exploited inherent weakness of the Ukrainian socio-political apparatus. Two were the major shortcomings. First, the information space was not prepared for impact. Russian media and other factors were acting without any control and at the times when Ukraine put efforts to regulate the environment, disinformation channels and narratives were already well established.[70] Since then, information security has become a priority of Ukrainian administration, and a range of institutional solutions has been imposed. Second, not until 2022 had Ukraine started labelling the conflict as interstate war. Russian disinformation strategy was successful during the Donbas campaign because Ukraine reacted narrowly by declaring an anti-terrorist operation, leaving the conflict at the level of civil one.[71] It is obvious that separatists were directly financed, trained, and organized by Russia. Therefore, there were sufficient reasons to declare a war against Russia even then. Since Ukraine was not ready to do so, Russia exploited the situation and set down the foot firmly in the eastern Ukraine.

The structure of Ukrainian response

A set of counter disinformation mechanisms formulated by Ukraine has been dictated by the wartime settings and the general level of socio-political unity. The evolve around the four main pillars.

Aggressive and assertive action

In its basic form, this method of countering disinformation means censorship. If there is no sender of disinformation, its influence is non-existent. Ukraine has gone to lengths to impose censorship in three areas. First and the most logical domain is mass media. Immediately at the outset of Crimea annexation many Russian TV networks were suspended, while in 2016 that number reached 73.[72] After that, disinformation rapidly moved to the much less regulated social networks because traditional media space in Ukraine became largely centralized. Even on social networks, accounts of proven Russian influence agents were suspended. Second domain is the political one. Certain pro-Russian political parties were banned from operation. In 2022, Opposition Platform – For Life was banned and the ban was confirmed by the Ukrainian judiciary, ultimately by the Supreme Court.[73] Third domain is the ban on Russia-linked Ukrainian Ortodox Church which is considered to be a foreign agent network tasked with spreading malign Russian influence.[74] While international community recognized the need to fight against the imminent disinformation threat, Ukraine has

[70] Gretskiy, Ibid., p. 1; Sazonov, Ibid., p. 67.
[71] Minzarari (2023) An Assessment of Russia's Way of War in the Wake of Its Aggression in Ukraine. National Defence University, p. 18.
[72] Gretskiy, Ibid., p. 1.
[73] https://kyivindependent.com/parliament-dissolves-pro-russian-opposition-platform-faction-following-security-council-ban/
[74] https://www.theguardian.com/world/2023/oct/20/ukrainian-parliament-votes-to-ban-orthodox-church-over-alleged-links-with-russia

been warned to progressively introduce a balanced solution where freedom of press and freedom of association will be respected against the necessity of aggressive counter campaigns.[75]

Institutional redesign

As it became clear that institutions are not tuned to respond to robustness of Russian disinformation, new solutions followed the exact measures to censor persons, media and organizations. Namely, National Security and Defence Council (NSDC) introduced the obligation for Ukrainian media to join the broadcast of official state news. The established practice was 24/7 United News Marathon conducted jointly by the four biggest TV networks.[76] Freedom of the press was therefore significantly diminished. More tightly connected to the disinformation was establishment of the Centre of Countering Disinformation (CCD), a governmental body tasked with debunking disinformation, fact-checking, and communicating the results with the general population.[77] Prior to the invasion of 2022, Ukrainian parliament passed a discriminatory law which pushed back against the use of the Russian language in the public sphere. According to the law, at least 90 percent of airtime must be in Ukrainian language, while regional outlets are not allowed to broadcast more than 20 percent of non-Ukrainian content.[78] This legal solution aimed at scaling down Russian influence in the public sphere, narrowing down a niche for disinformation.

Ukrainian disinformation campaign

Although the dimensions of Ukrainian disinformation efforts are still unknown due to the ongoing conflict, it is rational and expected that Russian disinformation has partially been fought back with a counter campaign. Traces of this we can see in the counter propaganda campaign during the Donbas conflict which precluded a significant number of defections.[79] Disseminating flyers and leaflets containing official state propaganda is one of the traditional Russian methods now used by Ukrainians to reach the otherwise hardly reachable Russian speaking areas in the east.

STRATCOM, crisis communication, and soft solutions

It could already be seen in institutional redesign that Ukraine was confronted by the complete lack of strategic communication. Networking of governmental, civilian and defense domains is a first step towards building more resilient structures. Wartime conditions forced Ukraine to rethink its approach to crisis communication. Some of the main methods were tasking mobile network providers to give free connections to anyone in Ukraine, but also establishing emergency news broadcasts so that people in the state of diminished readiness to follow media can also remain informed.[80] Empowerment of the NGO sector in the domain of disinformation has also been

[75] Kowalski, Ibid., p. 2.
[76] https://www.opendemocracy.net/en/odr/ukraine-journalists-media-restrictions-self-censorship/
[77] Kowalski, Ibid., p. 14.
[78] Ibid., p. 15.
[79] Gretskiy, Ibid., 3.
[80] https://edition.cnn.com/2023/11/10/europe/ukraine-energy-grid-russian-strikes-intl-cmd/index.html

among the prominent strategies. The Ukrainian Crisis Media Centre and Information Resistance are the most famous and effective NGOs when it comes to combating disinformation.[81]

Comparison and Recommendations

Comparative perspective

Similarities between Russian disinformation in Estonia and Ukraine have already been identified within the text. They are mainly connected with the actors, methods, and strategic aims. Levels of Russian ambition vary greatly, but underlying logic has been consistent throughout. This section will compare the two approaches to combat disinformation and give policy recommendations on how to improve future attempts.

The most obvious difference between the two approaches to fight Russian disinformation is in the domain of planning. Namely, Estonia engaged in building a system that will be able to respond to disinformation campaigns at mid to long-term. Processes such as psychological defense and societal resilience are time consuming efforts, often spanning in multiple decades. The fact is that once established, those mechanisms to counter disinformation are to permanently stay. On the opposite side Ukraine adopted a short-term approach partially forced by the circumstances, but in part motivated by the quick benefits of the process. Oppressing human rights, censorship and other tools are extremely efficient, but threaten to turn the country towards the bad side of the process if adopted after the immediate danger is gone. Practices established by Ukraine during the war will need to be revised afterwards. There will exist a great risk of backsliding during the transition period. In other words, solutions taken by Ukraine are good as long as they are of temporary character.

Alike the previous point, Estonia decides to fight disinformation by mechanisms for promotion of values of its constitutional order, democratic institutions, and respect for human rights. Based on long-term solutions, a quick travel of those soft, ethically responsible appeals throughout the society is enabled. When the adoption of values has taken place, population believes in the government, which again has all the tools to lead the system towards permanent stability. In the case of Ukraine, instead of communicating values, it often resorts to creating its own disinformation reality, or at best exceptionally centralized official version of truth. Again, being necessary to avoid a drop in the level of combat readiness, this does not preclude disinformation from permeating the socio-political apparatus. In fact, it is rendered more and more vulnerable by hiding from the disinformation rather than confronting it.

Embodied in the two mantras of respective chapters, we can claim that Ukraine fights and Estonia (re)acts. Those two are metaphors for the 'grand strategy' of countering disinformation. Ukraine introduced all the levels of escalation in their operational reality. Namely, they are tackling disinformation at the basic level of debunking and fact checking. If that fails to stop penetration

[81] Sazonov, Ibid., p. 69-74.

they introduce methods of deterrence by punishment, while in the case of a repeated failure Ukraine is ready to weaponize and fight disinformation, defending its vital interests. Estonia established such a set of practices that weaponization is not a part of it. This is best seen by the almost non-existent narrative of Russian occupation of the country. The maximum level of escalation that Estonia includes in its strategy is deterrence by denial further protected by the extended deterrence umbrella of its allied partners. However, a great deal of Estonian effort to counter disinformation is at the basic level of increasing media literacy and equipping the population to navigate through the challenges of disinformation.

The two countries differ in their basic attitude towards liberties such as freedom of expression and freedom of the press. Democratic and instrumental interpretation of those universal provisions are of key importance here. Ukraine draws legitimacy from the Russian military threat to limit or even completely cease certain human rights and freedoms. This is particularly obvious in the case of freedom of the press. Limitations are seen as a legal, legitimate, and a necessary instrument to achieve one and only strategic goal, that being victory in the war. Estonia interprets human rights and freedom as the sanctuary and bedrock of its constitutional order. Without these freedoms, it would not be the same country. Precisely because of that even malign influence is allowed under the auspices that society itself is sufficiently resilient to read and despise those third-party efforts. In other words, human rights are interpreted as an end on its own.

Finally, reliance on foreign partners is a strategy adopted by both Estonia and Ukraine. As a NATO and EU member, Estonia counts on robust military, economic, and infrastructural help in the case of any emergency. As a compensation for that it delegated bits and pieces of its sovereignty to supranational decision-making bodies. Good bargain, one could claim. Cyber Excellence Centre in Tallinn and forward military deployments in the times of increased tensions are sufficient evidence how serious balancing is perceived in the partner countries. Ukraine as an outsider from both Western security architecture and European community (with aspirations to join the both, indeed), still heavily relies on the foreign aid. Whether it is shipment of weapons, protection of financial assets, or loose migration policy, Ukraine invested much of its efforts to reassure European and transatlantic partners that they are fighting for a good cause.

Policy recommendations

There are five main recommendations for the more efficient counter disinformation campaigns in the future.

Coordination and synchronization strategies

A range of concerted efforts should be achieved in order to solidify any response to foreign malign influence[82]. First, interagency cooperation should ensure that state apparatus does not contain any

[82] Partially adapted from Helmus, T., Keep, M. (2021) A Compendium of Recommendations for Countering Russian and Other State-Sponsored Propaganda. RAND Corporation, p. 11.

communication noise or jamming. Various ministries, cabinets, institutes, and agencies working together under the officially promulgated principles. Second, intergovernmental initiatives are significant for alignment of like-minded countries. Particularly on voluntarily basis, those alignments tend to become more durable than any other resolution or declaration. Third, public and private domains need to act accordingly both in top-bottom and bottom-up activities. It is beyond a doubt that grassroots and civil society organizations are often at the forefront of fighting against disinformation and therefore can provide useful insights to the public structures. Public support for private initiatives is always a sign of good will for fruitful cooperation. Fourth, civil military cooperation is of crucial importance since modern democracies cannot allow for a complete isolation of military structures. Aside from the citizen control of the sector, ministries of defence and military ranks should participate and enrich the strategies to combat disinformation.

Including international organizations as the lowest common denominator

Although we live in times of endangered image of international organizations (IOs), they still remain a symbol of rule-based order and dynamics of peaceful conflict resolution. When it comes to counter disinformation campaigns, IOs should set golden standards or provide detailed manuals on how societies should protect themselves from harmful practices. The importance of IOs comes from the sometimes universal legitimacy. Here, states that decide to hinge upon the provisions of IOs will join a like-minded family of countries with the same strategic aims. Being the foundation, this practice can serve as a platform for striking future cooperation. Some of the organizations that can serve as guarantee are the UN, OSCE, EU, etc.

Imposing certain control over algorithms and in legal provisions

Aforementioned was that human rights and liberties are the unprecedented guidelines for formulating counter disinformation strategies. Nevertheless, a certain level of oversight or limited control needs to exist so that autonomy does not dissolve itself into an anarchic environment. The phrase oversight and limited control means that for example algorithms should be monitored in order to avoid algorithmic authoritarianism. In other words, the vert algorithms are not doctored, but their underlying principles are monitored. In the legal domain, laws should be clear in defining what disinformation is and how the violation of the norms will be sanctioned. AI act to be adopted in the EU provides a relatively useful guidelines on how to balance the necessity of legal regulation and respect for the basic freedoms.

Winning hearts and minds through value promotion

As a notion borrowed from counterinsurgency studies, winning hearts and minds means undertaking a soft rather than hard approach to resolve a conflict. Instead of ideological mobilization of population over the issue of countering disinformation, a state provides a rational and value-based explanation on the importance of taking certain actions. The highest standard (taken from legal jargon) here is necessity in democratic society. If this standard is respected, we can legitimately approach people in a way to win its hearts and minds.

Systemic funding for all the phases of countering disinformation

Usually just the basic level of countering disinformation is heavily financed. Those are the subventions for fact-checkers, debunking organizations, various NGOs, and media outlets. However, there is a need to also finance institutions and actors tasked with deterrent function of the system. Among others, it is important to provide funding for STRATCOM departments, Cyber Centres of Excellence, and joint military civilian initiatives. Finally, there should always be a specific fund available for meaningful participation in intergovernmental initiatives, as well as those coming from the international organizations.