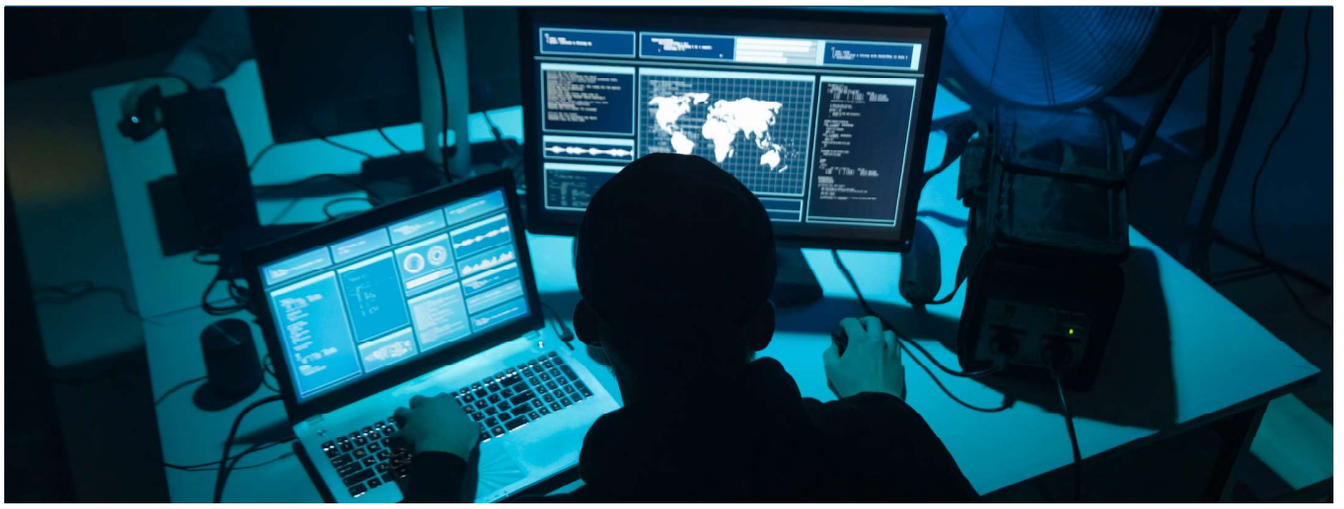
Policy Paper



January 2022

The Role of Cyber "Elves" Against Russian Information Operations

Adéla Klečková

ReThink.CEE Fellowship

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

Summary

Guerrillas of brave elves taking down hordes of dark trolls in an ideological conflict over the future of humanity. This is not the beginning of a fantasy novel but a somewhat accurate description of everyday realities in cyberspace across Europe. The "elves"—a group of cyber activists fighting pro-Kremlin propaganda and disinformation campaigns—are a growing yet little-known phenomenon. Having started in 2014 as less than 20 individuals in Lithuania, the movement expanded to 13 Central and Eastern European countries, and it counted about 4,000 volunteers by 2021. Given the size and the pace of growth of the elves, together with their successful yet unadvertised missions, it would be unwise to overlook or underestimate this movement.

Russian information operations against the Western democracies will grow in number, scale, and sophistication in the coming years. This is partially caused by the worsening state of relations between the West and Russia, partially by the global trend of the gradual shift of social and public life from the analog to the digital world. Already short of capacity to effectively counter pro-Kremlin information operations, Western stakeholders must seek and support innovative means to counter Russian information war. Cyber activism is one of them.

This paper explains how the elves have played and will play an essential role in countering Russian information operations, and it provides Western stakeholders with recommendations for how to enhance the activities of the elves. The data for this paper were collected for over a year, including through semi-structured interviews with the elves, visiting their cyber world and working with the data they have gathered, and attending their biggest international event—the Elves Academy. This paper provides a unique and comprehensive insight into the elves' cyber realm and activities.

The elves operate anonymously and focus on fighting hybrid threats conducted primarily by the Kremlin and its proxies. Their work is voluntary, unpaid, and independent from states and governments. Their activities are strictly legal—they strongly denounce any form of criminal activity such as hacking or cyber espionage, and they mostly limit themselves to monitoring Russian disinformation and its perpetrators, such as the trolls. Most of the data they generate is shared with the public, either as media outputs produced by the elves or through articles by local media.

The elves across Europe have developed functioning international cooperation, mainly consisting of intelligence and information sharing. The Elves Academy is the best evidence of continuous and robust international cooperation. This project, established by the Lithuanian elves in 2018, has trained hundreds of elves over its three editions so far. The collaboration of the elves should be further cultivated and encouraged. Joined together under a common cause, the elves represent a group of several thousand experts on countering information operations—a force that plays and will play an undeniable role in the defense of democracies against Russian hybrid warfare.

The most important recommendation for how to support the elves is to initiate a dialogue with them to learn about their needs directly from them as the needs of the chapters differentiate significantly across Europe. Each chapter can be reached through its official channels—either social media, official email, or website—or in some cases through its official spokespersons who have stepped out of anonymity. Finally, the very least everyone can do for the elves is to acknowledge their activities, read their media outputs, show public appreciation of their work, and help them spread their message.

Introduction

Guerillas of brave elves taking down dark hordes of repulsive trolls in an ideological conflict over the future of humanity? This is not the beginning of a fantasy novel but a somewhat accurate description of everyday realities in cyberspace space across Europe. The "elves"—a group of individual volunteers established to counter Kremlin-sponsored online propaganda and disinformation campaigns—are a growing, though little-known, phenomenon. Having started in 2014 as a group of less than 20 individuals in Lithuania, the movement had expanded to 13 countries and counted about 4,000 volunteers by 2021. Given the size and the pace of growth of the elves, together with their many successful if yet unadvertised missions, it would be unwise to overlook or underestimate this movement as it may (and in many cases does) play a crucial role against Russian information operations against Western democracies, which will grow in number, scale, and sophistication in the coming years. Already short of capacity to effectively to do so, Western stakeholders must look for innovative ways to counter Russian information war. Cyber activism is one of them.

With reference to the movie "Fight Club," the elves never fail to say that "The first rule of the elves is that the elves do not exist." Given the nature of their activities, anonymity is paramount for them. As a result, very little has been written (especially in English) about the movement and its operations, and there is a significant gap in the body of knowledge regarding the use of such forms of civic activism to tackle hostile information operations. There is no agreed definition for this movement. Here, the elves are defined as a specific type of cyber civic activists operating anonymously in semi-closed communities, primarily in the Central and Eastern European (CEE) countries, monitoring and countering Russia-led information and cyber operations.

This paper introduces the elves, explains how they have played and will play an important role in countering Russian information warfare, and why it is in the interests of Western stakeholders to enhance such cyber activism. Over one year, the research for this paper consisted of semi-structured interviews with the elves, visiting their cyber world and working with the data they have gathered, and attending their biggest international meeting—the Elves Academy. This generated unique insight allowing for a greater understanding of this phenomenon.

Western stakeholders must look for innovative ways to counter Russian information war.

The first section sets out the threat posed by Russian information operations, with "trolls" as one of the key non-state actors involved. It explains the main motives, principles, and actors of Russian information warfare, and it then details the trolls and examples of their successful operations. The first section concludes with a consideration of what role could emerging advanced technology such as artificial intelligence and big data play in the future of trolling. The second section focuses on three chapters of the elves considered to be among the most established and functioning ones: the original Lithuanian group founded in 2014, the Czech group founded in 2018, and the Slovak group founded in 2019, which at the time of the start of the research was one of the newest. These are very different on several levels and operate in different environments, and thus they offer a very comprehensive picture of the movement and challenges they face. This section places the elves within the broader concept of cyber activism—a phenomenon that, given the technological-social developments of the last decade, is gradually becoming part of daily life—and it argues the importance of the elves in countering Russian information operations. The section describes the history, activities, and operations of the elves. It concludes by providing examples of international cooperation among the elves, which should be further fostered and encouraged. The paper concludes by offering recommendations for Western stakeholders and members

of the expert community who might want to become involved in enhancing the activities of the elves.

Hybrid Warfare Principles, Weapons, and Actors

Russia is currently waging against the West something that is generally referred to as "hybrid warfare." The Latvian analyst Jānis Bērziņš came to the conclusion that "hybrid warfare is an appealing concept as it represents a mixture of everything and nothing."[1] But, however fitting, this observation might be too abstract. This paper regards hybrid warfare as Russia's response to its current perception and understanding of its security environment in the 21st century. This is employed to confuse enemies and to create a false perception that Russia is more capable and more powerful than the West. Broadly speaking, it can be described as involving a multiplicity of strategies, methods, and actors employed by illiberal powers seeking to paralyze liberal states by attacking their open societies.

The Russian view of modern warfare is based on the idea that the main battle space is the mind of the civilian population. Thus, hybrid warfare is dominated by information operations in which reducing the necessity of deploying hard military power and encouraging an opponent's military and population to support the attacker to the detriment of their government and country is regarded as one primary goal.[2]

With its problems related to the attribution of actions and its fuzzy boundaries, cyberspace is the perfect environment for conducting all manner of information operations.[3] By using information operations to attack the centers of gravity and critical vulnerabilities of adversaries, it is possible to win militarily as well as politically at a relatively low cost. Cyberspace provides weaker states with opportunities previously unheard of. Furthermore, the distance, commitment of forces, risk of exposure, and attribution limits involved in operations in cyberspace level the playing field for all actors, with no regard for their size, geographical location, or conventional military maturity.[4] Exploiting this, Russia's offensive cyber operations are a growing threat; for example, whether through the collection and leaking of sensitive information or through damage done by malicious software (malware) on physical infrastructure. Alongside military and non-military means, Russia uses offensive operations in cyberspace to pursue its strategic objectives.

The Russian view of modern warfare is based on the idea that the main battle space is the mind of the civilian population.

Russian actors have a holistic understanding of cyberspace. They tend to conceptualize it as the intersection between hardware, software, infrastructure, and content. By contrast, in the West these are seen as separate elements and rarely regarded as a part of a broader whole. Thus, the term "cyber" in Russian is used solely to speak about Western threats and activities, whereas in the West it is used in a more general sense. Russian actors also use the broader, more fitting term "information," and operations can be subsequently categorized as information-technological and information-psychological.[5] In the first category, electronic warfare or the distribution of malicious software is used to cause physical damage to infrastructure, to destroy or degrade adversaries' electronic capabilities, or to gather sensitive data. The

1 Jānis Bērziņš, "The West Is Russia's Main Adversary, and the Answer Is New Generation Warfare," Sicherheit und Frieden (S+F) / Security and Peace, 2016.

2 Adéla Klečková, "Does the Russian Intervention in Crimea in 2014 Demonstrate a New Way of War?" Strife Journal, 2021.

3 Daniel Bagge, Unmasking Maskirovka: Russia´s Cyber Influence Operations, Defense Press, 2019.

4 Matthias Schulze, Cyber in War, 2020 12th International Conference on Cyber Conflict, 2020.

5 Janne, Hakala and Jazly Melnychuk, Russia's Strategy in Cyberspace, Riga: NATO Strategic Communications Centre of Excellence, 2021.

second category usually consists of influence operations, such as the spread of disinformation or the application of psychological pressure, to attack the perception and morale of state or non-state actors.[6] While the main subject of analysis of this paper is information-psychological operations, understanding the more holistic conceptualization of cyberspace by Russian actors is of crucial importance to anyone wishing to study the principles, strategies, and actors of Russian cyber or information war and warfare.

This approach has also wider implications in terms of which actors Russia uses to conduct its information operations. The main ones are the three intelligence agencies: the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), and the military intelligence Main Directorate of the General Staff (GRU). Not only are these agencies not transparent, they are also newly prohibited by law to publish reports of their activities.[7] Thus, very little is known about them. Nevertheless, it is known that the GRU is the mother agency to Unit 5477 (also known as the 72nd Special Service Center), which is responsible for the agency's psychological operations, including interference in the 2016 US presidential election.[8]

Professional trolls are the most important group in the context of information and cyber war.

Like other government entities in Russia, its intelligence agencies face challenges in recruiting qualified personnel as they have to compete for talent not only among each other but also with the private sector. Thus, the intelligence agencies have to outsource operations to non-governmental actors, either cyber criminals (primarily professional "black hat" hackers), nationalistic/patriotic hackers, or professional trolls.[9] This has several benefits: these actors are cheaper as, unlike regular state employees, they are usually summoned only when necessary or some even work for free for ideological reasons, and they provide plausible deniability as they usually cannot be linked directly to the Kremlin.

The agreement between the Kremlin and cyber criminals is simple and mutually beneficial—as long as the latter do not meddle with Russian interests, they are allowed to operate freely and they are even protected from the reach of the Western law-enforcement agencies. Usually, they are used for more sophisticated operations such as attacking foreign banks, multinational companies, and other commercial websites.

Nationalistic/patriotic hackers act based on their attachment to the Russian state. As they are usually less skilled and experienced, they are primarily used to conduct more basic campaigns such as "distributed denial of service" attacks, stealing and leaking emails, and hacking into news outlets to modify what they publish or to deny access to specific stories.

Professional trolls are the most important group in the context of information and cyber war. They are creatures of chaos who prey on the frustration and anger of others . They do it by deliberately disrupting, attacking, or generally causing trouble on social networks or other user-generated-content platforms by posting comments, photos, videos, GIFs, or other forms of unwanted online content. According to one investigation, an average troll in Russia was paid about €400 a month in 2017, an above-average reward for a comfortable "office" job in the country. As one former troll describes, he was paid to write about 135 online commentaries per day, primarily about the conflict in Ukraine.[10]

With hybrid war becoming more frequent, perhaps it is not shocking that the Russian state is using paid, organized aggressive armies of online accounts to

6 Adéla Klečková, Cyber Warfare: Drivers of Change Behind the Machinery, King´s College London, 2021.

7 Aric Toler, "Russia´s 'Anti-Selfie Soldier Law': Greatest Hits and Implications," Bellingcat, February 20, 2019.

8 Congressional Research Service, Russian Cyber Units, 2021.

9 Sandor Fabian, "The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy," Defense & Security Analysis, 2019.

10 Simon Shuster and Sandra Ifraimova, "A Former Russian Troll Explains How to Spread Fake News," Time, February 21, 2018.

spread its propaganda. Nevertheless, revelations about the trolls' activities in 2014—when little was known about hybrid warfare (at least publicly) very and the role of the internet and social networks in it—were groundbreaking. They also gave birth to the elves—the internet warriors dedicated to countering the activities of trolls.[11]

Russian information operations are expected to grow in number and scale in the coming years. At the same time, the role of non-state actors is expected to grow further as it is cheaper and more convenient to outsource some aspects of the information operations to external suppliers. And so will the role of those who attempt to counter such operations and to protect the values of democracy and freedom. Thus, it is in the interest of Western governments to be aware of the movements countering trolls and other hostile cyber actors as well as to learn how to foster them and how to create an environment contributing to the enlargement of those that already exist and the establishment of new ones.

Typology of Actors

In this context, the term troll is generally applied to any type of anonymous account in the service of the Kremlin. However, with the most recent technologies and machine learning, hybrid operations are getting more sophisticated. Therefore, three types of actors can be distinguished.

Trolls refers to human-operated, non-automatized accounts that can be either created anonymously or under a made up or real identity engaging in targeted harassment. Their objective is to dissuade or dismay the target. Their methods include bad-faith arguments, logical fallacies, doxing (publicly revealing private information about an individual or organization, usually through the internet), and rude behavior. Trolls usually congregate around topics or individuals and usually have a disproportionate level of engagements.

Bots (an abbreviation of robots) are fully automated accounts engaging in certain behavior based on a set of instructions (scripts). Just like any technological tool, bots are neither inherently good nor bad—they do what they are programmed to do. The most problematic type of bots in the context of information warfare is the social bots (those operating on social networks). Using normally accessible software, in theory, a user can create an infinite number of social bots that can then engage in different kinds of activities. Thanks to their ability to tweet or post hundreds of times a day and night, they are used for amplification and to create information chaos.[12] They are also very cheap and easy to use. However, spotting bots is quite easy as they usually adhere to a pre-programmed and thus predictable scheduling, and the automation of the actions concerned is evident from timestamps.

Cyborgs combine automated and human control.[13] Automated actions such retweets can be segregated while the human user periodically takes over to respond to other users and to post original content. As a result, cyborgs are more difficult to detect than bots but are also more expensive and time-consuming to operate. Similar to bots, they are used for amplification and obfuscation.

Activities of Trolls

Russia has employed its cyber actors in different types of information-psychological operations. They have destroyed the private lives of opponents of the Kremlin, influenced the political situation in Western democracies, or threatened safety of NATO troops based in countries bordering Russia.

The first example of a large, coordinated personal attack by pro-Kremlin trolls was the one starting in 2014 against the Finnish journalist Jessikka Aro, who first discovered the existence of "troll factories": office

11 Adéla Klečková, How Czech Elves Are Fighting Russian Disinformation, Friedrich Naumann Foundation, 2019.

12 Voice of America News, "Cyborgs, Trolls, and Bots: A Guide to Online Misinformation," February 8, 2020.

13 Ibid.

buildings where the trolls create their toxic content.[14] She provided the first evidence of Russian trolls being not only very well organized but also connected to the Kremlin as an integral part of its information warfare. As an act of revenge, the trolls launched an intensive harassment campaign against Aro, effectively forcing her out of the virtual and for some time public space. Besides making rape and death threats, the trolls called her and pretending to be her dead father.[15]

Elections in Western countries are also the focus of the Kremlin and its proxies. The effort of pro-Kremlin trolls to manipulate US public opinion during the 2016 elections resulted in a vast coordinated campaign that was very successful at pushing out and amplifying messages designed in part to help Donald Trump get elected president. A similar situation occurred during Germany's parliamentary elections and France's presidential election in 2017.[16] In France, Emmanuel Macron's campaign was heavily targeted by pro-Kremlin trolls. Dozens of fake Facebook accounts were created to conduct surveillance of his social-media campaign. Some trolls tried to lure Macron's associates and supporters into sharing personal information or downloading malware that would give them access to their social network accounts, thus enabling further spying.[17]

Two more recent malicious campaigns that have targeted NATO and its troops were the Ghostwriter and the Secondary Infection operations.

The Ghostwriter operation ran from 2017 through at least May 2020 to disseminate falsified narratives surrounding Lithuania, Latvia, and Poland and their relations with NATO allies.[18] It combined an information-technological operation with an information-psychological one. The former was used to penetrate news and governmental websites to provide a credible dissemination platform for the operation's false narratives. Consequently, armies of trolls, bots, and cyborgs employed their various social-network profiles, blogs, and other sites allowing user-generated content to amplify and further disseminate these narratives. The ultimate goal was to seed tension between allies and to damage the public image of NATO troops stationed in the Baltic countries by "revealing" their alleged wrongdoings.[19]

Uncovered in 2019, Secondary Infection was a large-scale information operation spanning nine languages, 30 social networks and blogging platforms, and scores of fake user-profiles and identities.[20] Some of its stories were calculated to inflame tensions between NATO allies, especially Germany and the United States or the United Kingdom and the United States. Others appeared designed to stoke racial, religious, or political hatred, especially in Northern Ireland. Few posts gained traction, but one anti-immigrant story penetrated Germany's far right and continues to circulate online.

The Future of Trolling

The above are just a few examples of Russia's many information operations conducted against Western countries and their political systems in the last couple of years. As well as because of the growing role social media plays in daily life, the deteriorating relations between the Kremlin and the West will also cause their number to grow. Russia sees this a providing more

14 Jessikka Aro, "Yle Kioski Traces the Origins of Russian Social Media Propaganda – Never-before-seen Material from the Troll Factory," Kioski News, 2015.

15 Jessikka Aro, "My Year as a Pro-Russia Troll Magnet: International Shaming Campaign and SMS from Dead Father," Kioski News, 2015.

16 Marius Laurinavičius, A Guide to the Russian Tool Box of Election Meddling, International Elections Study Center, December 2018.

17 Damien Sharkov, "Russian spies used Facebook to trick Macron allies: Report," Newsweek, July 27, 2017 .

18 Morgan Demboski, Joey Fitzpatrick, and Peter Rydzynski, "Russian cyber attack campaigns and actors," IronNet, October 25, 2021.

19 Lee Foster et al, " 'Ghostwriter' Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned with Russian Security Interests," FireEye, 2020.

20 The DRF Lab Team, Operation "Secondary Infektion," Atlantic Council, 2019.

reasons to take "reciprocal steps" against Western countries to "punish" them for their hostile behavior, such as the EU and US sanctions against the Kremlin. Furthermore, feeling itself geopolitically cornered, it is becoming more aggressive as it feels it has less to lose. This is clear from operations against countries that the Kremlin has historically tried to have good economic relations with—such as France or Germany—as well as from the limited attempts by the Russian intelligence services to hide their operations—as in the case of the recent massive SolarWinds information-technological attack.

Thanks to digital personalization, users can be targeted with propaganda that is most likely to resonate with them.

Another important variable for the future of trolling and Russian information operations in general is the existence of new and increasingly sophisticated technologies for personalizing, targeting, and scaling up online content to maximize its impact.[21] Trolls usually work in 12-hour shifts and are required to meet quotas in terms of producing comments, blog posts, or page views.[22] This work can get tedious and writing new content about the same topics—for example, elevating the image of Russia or increasing division or confusion in the European political landscape—has its challenges. However, artificial intelligence can help overcome these creativity obstacles.

Advanced technologies can be used to generate, target, and disseminate disinformation. With the help of text-prediction tools, untold amounts of fake news and falsified information can be produced. Artificial intelligence, in the form of deep learning, can generate deepfake videos that are increasingly impossible to distinguish with the human eye from non-fabricated videos. New and accessible software and applications allows unskilled people to make deepfakes with a handful of photos. They can even create convincing but entirely fake photos from scratch. Audio can be taken too to create "voice skins" or "voice clones." Thousands of robotic accounts can then disperse this fabricated and harmful content into the virtual space daily.

Thanks to digital personalization, users can be targeted with propaganda that is most likely to resonate with them.[23] This is done through sophisticated algorithms for personalizing and targeting content by utilizing big data about the personal interests of millions of users of social networks. As a result, more and more precisely targeted disinformation campaigns can be expected. The world already witnessed this during the US presidential election and the Brexit referendum in 2016. In the case of Facebook, the use of personalization and targeting tools to spread propaganda and disinformation was recently confirmed by the revelations of the whistleblower Frances Haugen.[24]

The objective is not necessarily to change people's views about politics and policy, but rather to confuse or polarize. The more disinformation proliferates online, the more lost in the "fog" of political news the average reader gets. To prevent the future of Western democracies becoming the Kremlin's video game, politicians and other stakeholders must look for innovative ways to counter information operations. Cyber activism in the form of the elves is one of them.

Cyber Activism and the Elves

Cyber activism refers to the use of internet-based socializing and communication as well other information technologies to create, operate, and manage activism of any type. As much of daily and social life has gradually shifted from the analog world to the social networks, it was only a matter of time before

21 Antonio Missiroli, "Game of Drones? How new technologies affect deterrence, defence, and security," NATO Review, 2020.

22 Sarah Kreps, The Role of Technology in Online Misinformation, Brookings Institution, 2020.

23 Ibid.

24 Olivia Solon and Teaganne Finn, "Facebook whistleblower tells Congress social network is 'accountable to no one'," NBC News, October 5, 2021.

different actors decided to use this new virtual public space to promote messages or causes. Cyber activism applies to any individual or organization using online tools to reach and gather followers, broadcast messages, and advance a cause or movement. It can be used for various purposes—such as awareness creation or initiating reactions. In the case of the elves, it serves to counter pro-Kremlin information operations and to fight disinformation.[25] Cyber activism will keep growing in importance and it will soon become an integral part of daily life (if this has not already happened). It is a trend that has been amplified during the coronavirus pandemic with information technologies playing an ever more important role in life and more activities moving into the cyber realm.

The emergence of information technologies and consequently the internet and social networks triggered a small revolution, providing activists with previously unthinkable possibilities for disseminating information or mobilizing audiences. First, the role of "gatekeepers" has been diminished or even eliminated—social media enable activists to report, document, or write about their cause without the need for traditional media reporting. Second, growing connectivity enables activists to reach thousands or millions of people at no or relatively low cost. Third, the anonymity of the internet (especially the layers of the internet called the "deep web") allows activists to work in relative safety without the risk of being exposed and prosecuted. The last factor is fundamental for the elves.

Cyber activism will keep growing in importance and it will soon become an integral part of daily life.

Faced with the continuing growth of pro-Kremlin information operations and in their impact, the state agencies in the West—just like Russian ones—compete with the private sector and struggle to find suitable staff in suitable numbers to counter them. The situation is made worse in CEE countries by the problem of brain drain. Since, unlike Russian state agencies, Western ones cannot and should not turn to paid professionals, cybercriminals, or abuse of modern technologies in form of robotic accounts, cyber activism in the form of the elves can play a decisive role in the coming years in information wars with any hostile entities. It is in the interest of all democratic governments to know how to foster and enhance the activities of such movements as well as how to nurture an environment where they can be founded and successfully operate.

The Elves

The story of the elves starts in Lithuania in 2014. In the beginning, it concerned a group of less than 20 enthusiasts worried by Russia's aggression against Ukraine and the increasing number of information operations conducted by pro-Kremlin forces in Central and Eastern Europe. The group started calling itself "the elves" because it was founded as a counterforce to pro-Kremlin trolls. The movement eventually spread to Estonia and Latvia, and then to other countries, including the Czech Republic, Finland, Slovakia, and Ukraine.[26] In 2021, the first Western European chapter was founded in Germany. With a network this large, the movement has created a stable structure of thousands of volunteers across Europe.

The elves operate anonymously and focus on fighting hybrid threats conducted primarily by the Kremlin and its proxies. Their work is voluntary, unpaid, and independent from states and governments. Their activities are strictly legal—they strongly denounce any form of criminal activity such as hacking or cyber espionage, and they mostly limit themselves to monitoring Russian disinformation and its perpetrators such as the trolls. Most of the data

25 Frontline Defenders, #Cyber-Activism, 2016.

26 At their request, more specific information on the geographic location of the elves cannot be provided. As the chapters are at different stages of establishment, with some still rather new and small, the unwanted attention of trolls might hinder their successful development.

they generate is shared with the public, either as media outputs produced by the elves or through articles by local media.

While the elves currently focus on Russian information operations—as Kremlin proxies are still most active in the cyberspace of the CEE countries, and as geographical proximity means Russia poses the biggest security threat—with the gradual increase of similar hostile behavior from China and its local proxies and "useful idiots" (see below), they have started to discuss expanding their activities to cover Chinese operations in cyberspace.

Typology of Elves

The modus operandi of the elves slightly varies across countries. Among the ones in the Czech Republic, Lithuania, and Slovakia, one can find primarily "cyber scouts and double agents," "elves in suits," and "memetic warriors."

Cyber Scouts and Double Agents

Among all the elves communities, intelligence cells—cyber scouts—form the biggest one. As the elves reject hacking and other illegal activities, the vast majority of their data comes from open-source intelligence—information collected from published or otherwise publicly accessible sources by using advanced techniques to gather, analyze, and categorize large amounts of data. It is estimated that open-source data may account for as much as 80–90 percent of the overall intelligence decision-making is based upon.[27] The elves usually collect such data from social networks, chain emails, or other user-generated content platforms.

Their main area of focus is Facebook and Twitter. On Twitter, they gather information on new trends in disinformation or about the activities of the known networks of trolls, cyborgs, and bots. They also identify and debunk trolls or robotic accounts posing as real users.

On Facebook, the elves gather data from the public profiles of prominent pro-Kremlin sympathizers and their political movements or from "secret" troll closed groups. Unfortunately for the trolls, such groups are usually neither secret nor private enough to prevent the elves from penetrating most of them. The elves act as double agents, which enables them to monitor discussions in these groups and to collect highly relevant intelligence. Some of them go even further by engaging in counter-information operations, spreading alarm among trolls by suggesting that "an elf might have penetrated the group." Such covert actions are rare, though, since the elves are generally wary of unnecessary radicalization and further escalation of the tension between the trolls and themselves.

On Facebook, the elves gather data from the public profiles of prominent pro-Kremlin sympathizers and their political movements or from "secret" troll closed groups.

Chain emails are a communication channel—especially popular in CEE countries—heavily employed to spread pro-Kremlin propaganda, primarily among the elderly. Unlike typical scams, unsolicited emails containing false information are used to scare, intimidate, or deceive their recipients. Disinformation chain emails are an important amplifier of pro-Kremlin propaganda disseminating fear and distrust. The elves have also discovered chain emails including instructions for recipients on how they can be forwarded to all their contacts. The main problem connected to this dissemination channel is its lack of transparency—as chain emails are regarded as private communications, there are no tools that would allow outsiders to see and to respond to disinformation are people are exposed to. Nonetheless, the Czech elves have created, and shared with their Slovak colleagues,

27 Nihad Hassan and Rami Hijazi, Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence, Apress Media, 2018.

a database storing thousands of such emails.[28] Using various methods, they analyze hundreds of new chain emails that are added to the database every month to identify new trends and prevailing narratives in pro-Kremlin disinformation.

The conclusions derived from the data gathered by the cyber scouts and double agents are used to produce reports that are circulated through various channels to politicians, media outlets, or security services. The Czech elves publish monthly a several-page media product that is distributed and promoted through their website, social media, and two of their official spokespersons. These reports are highly regarded in the Czech expert community as they provide priceless insights into the pro-Kremlin underworld and make the work of analysts, journalists, and policymakers easier.

Elves in Suits

Some of the elves chapters have their own "legal department." These "elves in suits" use legal tools to put pressure on those who break the law in the cyber realm in pursuit of the interests of the Kremlin. They form a rather specific group within the elves communities as at least some of them have to step out from under the protection of anonymity to file legal suits. Thus, unlike with their other activities, the elves never publicly claim that they are behind these lawsuits and activities of this particular department is one of their most carefully protected secrets.

The legal suits brought by the elves typically involve hate speech, the spread of serious hoaxes, threats to national security, or violence or death threats. Usually, such crimes have been identified by the cyber scouts. Legal suits normally do not target trolls, who cannot be tracked down due to their anonymity, but rather the owners or authors of major disinformation portals or "useful idiots" among politicians, journalists, or celebrities. The term "useful idiot" originally referred to people from non-communist countries sympathetic to communism, who were regarded by the communists as naive and susceptible to manipulation for propaganda or other purposes.[29] Today, it refers to people who unknowingly support a foreign duplicitous and dangerous regime while attacking those who criticize it, against the interests of their own country.

The legal suits brought by the elves typically involve hate speech, the spread of serious hoaxes, threats to national security, or violence or death threats.

Securing a court ruling again criminal activities they identify is of secondary importance for the elves. They perceive instead legal suits as an efficient tool of deterrence. A combination of public, media, and legal instruments make up a strong pressure tool that can prevent some from actively engaging with pro-Kremlin narratives and activities, and it poses an obstacle for those who already do so.

Memetic Warriors

To promote their activities and to counter toxic pro-Kremlin narratives with their own positive messaging on social media, the elves have their "communication department." Contrary to common belief, they rarely engage in open combat with internet trolls. As the elves are significantly outnumbered by trolls, who also are supported by robotic accounts, they know that they must employ a better strategy than trying to outshout the trolls in the virtual space. Thus, besides promoting the work of their colleagues and commenting on daily events and new trends in disinformation, the elves' "communication department" is trained to be

28 The author was granted access to these databases and was allowed to work with them, to monitor the work of the elves, and to read the gathered chain emails.

29 Trey Hoffman, "The "useful idiots" are back," The Citizen, May 27, 2021.

actively involved in the emerging trend in strategic communication known as memetic warfare.[30]

This is a new and rising element of information warfare, which is being considered by US and NATO security experts an integral part of the future of strategic communication addressing hostile information operations. Employing memes—images or videos that portray a particular concept or idea that are then usually spread through online social platforms—as a psycho-political conflict tool has proven to be increasingly successful.

The power of humor is great as no public personality, and especially no politician, wants to look foolish in the eyes of the people. Using memetic warfare seems to be perfect a perfect strategy when it comes to addressing citizens of the CEE countries, who are known for their cynical dark humor and tendency to ridicule everything, starting with public figures and politicians. Thus, elves "memetic warriors" create memes, caricatures, or ironic remarks and comments to make their messages more appealing and therefore easier to comprehend and resonate within the public. Such content is published either through the official communication channels of the elves or with the help of allied social-media celebrities, influencers, Facebook groups, or parody news webpages. These kinds of posts are usually among the most successful ones from the elves' communication department, reaching hundreds of thousands of people. Thus, memetic warfare is among the most powerful weapons in the elves' quiver.

Activities of the Elves

As noted above, the outnumbered elves rarely engage in direct combat with the pro-Kremlin trolls and know attempts to be "louder" in cyberspace would be self-defeating. Instead, they focus on strategically more important activities from a long-term perspective for countering Kremlin information operations or for building a positive pro-democratic, pro-EU, and pro-NATO narrative.

A good example of such a large-scale, international operation of the elves was the Apple Maps campaign initiated and coordinated by the Baltic elves. In late 2019, giving in to the pressure from the Kremlin, Apple begun showing Crimea as a part of Russia in its Maps app.[31] In response, the Baltic elves and their Ukrainian partners coordinated a critical campaign on social media to put public and media pressure on the company to persuade it to display Crimea correctly in accordance to international law. The campaign took off and Apple was heavily criticized by its users worldwide for pandering to and normalizing Russia's aggression while ignoring the international community's recognition of Crimea as a part of Ukraine.[32] Even though Apple eventually decided not to change its decision, the campaign was one of the first examples of an international coordinated effort of cyber activists to counter pro-Kremlin activities.

The outnumbered elves rarely engage in direct combat with the pro-Kremlin trolls and know attempts to be "louder" in cyberspace would be self-defeating.

Another example comes from the Czech Republic where the elves played an important role in the "Konev affair." When the authorities in Prague decided in 2020 to remove the statue of Soviet Marshal Ivan Konev, who is regarded as a hero in Russia, the Kremlin opposed this fiercely and employed multiple means to prevent it. This included a disinformation campaign, massive protests by Czech right-wing and left-wing extremists orchestrated by the Russian embassy in Prague, attacks on the Czech embassy in Moscow, and

30 Tom Ascott, How memes are becoming the new frontier of information warfare, The Australian Strategic Policy Institute, 2020.

31 Alyssa Newcomb, "Apple Now Recognizes Crimea as Part of Russia in Its Apps, Bucking U.S. and International Policies," The Fortune, November 27, 2019.

32 Alastair Jamieson, "Apple "looking at how it handles borders" after Crimea map controversy," Euronews, November 30, 2019.

new legislation enabling Russia to bring citizens of any state under unprecedented extraterritorial jurisdiction.[33] The elves kept close track of these developments and monitored all related narratives on social media, comparing media reporting about the affair in Czech-language and Russian-language media. This proved helpful to the journalists and state agencies following Russia's operation and was essential for later holding it accountable for meddling in the domestic affairs of the Czech Republic.[34]

International Cooperation Among Elves

International cooperation among the elves movements is on a loose yet functioning basis. Most of it consists of intelligence and information sharing and of the Elves Academy.

For instance, in the early days of the elves in the Czech Republic, the leadership of the Baltic ones visited the country on several occasions and was consulted on the establishment of the elves there. Given the difference in the environments in which they operate, with the Baltic elves not having to fear persecution by either the state or society, the Czech elves developed their own structures and operating methods. They also sought to develop cooperation with the Slovak elves and, to some extent, provided them with the same kind of counsel as the Baltic elves did for them. These attempts bore fruits with new channels of communication and cooperation established among the Czech and Slovak elves—and by the extension between the Czech and Slovak security communities as some of the two countries' elves are member of their NGO, academic and security circles—resulting into even more productive sharing of intelligence and best practice on countering hybrid operations in cyberspace.

The Elves Academy is the best evidence of continuous and strong international cooperation. This project, established by the Lithuanian elves in 2018, has trained hundreds of elves over its three editions so far. Each winter, the capital city of Lithuania, Vilnius, becomes for several days home to about 100 volunteers who travel there in their free time and on their own funds to learn new skills and abilities to enhance their elves activities in their home countries.[35] This presents an ideal opportunity for the elves from all over Europe to get to know each other and to create new international networks of like-minded people.

The Elves Academy is the best evidence of continuous and strong international cooperation.

The content of the Elves Academy is different each year, depending on the availability of speakers, current trends in the security sphere, and the needs of the elves. The theoretical part usually teaches the elves all that needs to be known about Russian hybrid warfare and information operations, with examples of such activities from Central and Eastern Europe, how to best counter it, and how to build a general resilience against it in their own home countries. During the practical workshops of the 2020 edition, the elves were taught new ways of identifying a fake (robotic or cyborg) account on social media using new software and computer programs. Another item was advanced methods of open-source intelligence to gather more information about the agents working in the name of the Kremlin in the online and offline worlds. As the elves are highly likely to become a target of an information-technological operation, another workshop focused on raising their level of cybersecurity, teaching them how to protect hardware and software from threat actors as well as how to spot and protect themselves from the most common types of cyberattacks.

Such international networking and capacity building for the elves should be encouraged by

33 Adéla Klečková, Russia Targeting the Czech Republic over Statue Calls for International Reaction, May 1, 2020, The German Marshall Fund of the United States, 2020.

34 The Czech Elves, Special Report: Removal of the Konev Statue, 2020.

35 In 2020, due to the coronavirus pandemic and connected travelling restrictions, the academy was a fully online event.

international actors, especially as the elves chapters, now in 13 countries, are at different stages of development, with the Baltic, Czech, and Slovak ones the most established ones

Policy Recommendations

There are good reasons to believe that Russian information operations against the Western democracies will continue to grow in scale, number, and aggressivity—and that the role of non-state actors in these will become increasingly important. Thus, Western stakeholders must look for innovative ways to effectively counter such operations. The work of cyber activists like the elves is one of them. Below are recommendations for how policymakers and members of the expert community can enhance the activities of the elves and create an environment favorable to the establishment of such movements.

Each elves chapter has a different way of operating, different obstacles to overcome, and different issues it struggles with. This is due partly to the size and type of Russian information operations they face and partly to the different operational environments shaped by the political culture in their respective countries. Thus, perhaps the most important overall recommendation is that there is no one-size-fits-all solution that will help all elves in their mission. The best way for finding out how to help would be to ask them. Each chapter can be reached through its official channels—either social media, official email, or website—or in some cases through their official spokespersons who have stepped out of anonymity. Having said that, below are several general recommendations worth considering and discussing with the elves.

Operational Environment

The operational environment for the elves in CEE countries could not be more different in quite a few aspects as Russia and hybrid warfare are regarded with different level of caution across the region. For instance, in the Baltic states Russia is regarded as a clear security threat and thus countering its information operations is viewed as a noble and positive thing that is highly appreciated by the majority of the public and the political class. Thus, it is easier for the Baltic elves to promote their work and develop working relationships with the state. They organize public events and stakeholders are not hesitant in openly showing support for their work. This has a positive impact on the public image of the elves as well as their morale and motivation to join the movement or to continue in their work.

Each elves chapter has a different way of operating, different obstacles to overcome, and different issues it struggles with.

In Central Europe, the situation is more difficult for the elves. In the Czech Republic and Slovakia, the debate on Russia and its hostile operations is more divisive. Though some politicians and members of academia and civil society see growing Russian aggression as a problem that needs to be tackled, other politicians and the broad public are less convinced or even openly favor Russia. In both countries, the latter part of the political class has a stronger voice and has been represented by the president, part of the parliamentary membership, and state institutions, which negatively affects the work of the elves. In both countries, the elves thus have to hold tight to their anonymity out of fear of either losing their jobs or for their reputation and safety. This prevents them from developing functioning cooperation with the state or from publicly receiving credit for their work, which harms their morale and motivation to continue in their work.

Politicians and other stakeholders should work toward creating a safer and inviting environment for the elves. They should show public support for the activities of elves either through the media or through their communication channels. Policymakers might even consider establishing regular briefings with the official representatives of the elves and encourage

representatives of state security institutions to follow their lead. Most importantly, the elves' fear of negative repercussions in their professional career for performing what is a public service must be addressed; otherwise, a healthy and active civic society can never be properly built.

Funding

There is no consensus among the elves on the question financial support to enhance cyber activism. Some are dismissive of such an idea, claiming that this would weaken their narrative. The idea of the elves working for free because of their belief in their cause is strong—especially in opposition to the armies of trolls paid by the Kremlin—is in their mind a powerful one.

Others take the view that the chances of long-term survival for the elves are limited without funds to compensate them for their time and efforts. "A group of volunteers with bare hands cannot win the information war," they say. Thus, they strongly advocate financial support by the state, international organizations, or private donors. In this regard too, the needs of the elves chapters can differ and it is crucially important for those who wish to help them financially to open a direct communication channel with the movement. All elves tend to agree that at some point it starts getting harder to maintain motivation. And the majority agree that having their time and effort valued or rewarded would be beneficial.

A solution could be support in non-financial form—for example, by providing elves paid premium versions of software they use so they have better anti-virus, data clouds, or computer programs for either coordination and division of work or for their open-source investigations. Policymakers can fund some of those tools for the elves or help to initiate meetings between the elves and representatives of IT companies or other actors that might be able to support them in this regard. Policymakers and representatives of NGOs and political foundations should also engage in dialogue with the elves to discuss what forms of direct financial support would be manageable without the elves risking their safety by publicly exposing too much information. The elves could then decide whether such help would or would not be beneficial to their cause.

Media Support

The motivation of the elves tends to decrease over time—an inevitable trend caused by the nature of their work. The majority is tasked with analytical work that sometimes gets monotonous. The elves usually do not engage with the trolls in an active conflict, and they do not get the excitement of seeing their work having an impact, due partly to the secretive character of their work and partly to the operational environment. As put by one of them, "it feels like playing tennis against the wall." Thus, the more senior elves are always looking for new ways to lift the spirit of their colleagues and to make them feel more appreciated for their work.

Public recognition of the importance of the work the elves do is another way to enhance their activities that has wide support within the movement. This can have multiple forms. Public figures can promote the elves using their communication channels. The media should cover the work of the elves or credit them if their work was one of the sources of an investigative report. Think tanks can invite their official representatives into public discussions. But perhaps the most important part must be played by members of the broader public, who should read the reports and articles published by the elves, follow them on social media, and share or like their posts or from time to time write an appreciative comment. The internet and social media are the realm of the elves and these are very likely to be read by some of them. Thus, when asked how to aid the elves, the answer is clear: acknowledge their work and help them to spread their message.

International Support

The elves have reached a threshold many activist groups strive to achieve but only a fraction of them

does—they have become an international movement functioning in 13 European countries with further potential to grow. The fact that the elves are not a country-specific movement but can evolve and survive in different operational environments raises the hope that they can play an important role in countering information operations targeting democracies across the world. Thus, the international ambitions of the elves should be further encouraged by domestic stakeholders among politicians, academics, and representatives of NGOs.

These stakeholders should try to promote the movement when talking to their foreign counterparts or attending international conferences. International actors such as the EU and NATO as well as think tanks and political foundations should invite the elves to participate in their events and projects. First, because the elves with their unique background and experiences can make a valuable contribution. Second, because sending the elves abroad is another form of non-financial support that can help maintain their motivation. Strengthening international cooperation among the elves and between them and international organizations is another important step in increasing resilience against Russian information operations.

Conclusion

The activities of trolls—one of the key executors of Russian information operations—in the virtual realm of internet pose a severe security threat to Western democracies. The elves have real potential to successfully stand up to trolls. The conflict between them is part of an information war that is part of the broader hybrid war waged against the West by the Kremlin. Given the nature of cyberspace, Russian information operations are expected to grow in number, aggressivity, and sophistication. Furthermore, with Russian intelligence agencies already short of employees, the role of non-state actors such as trolls is expected to increase.

To prevent the rather dystopian picture of the future of trolling and other information operations due to the newest technologies from becoming reality, Western stakeholders must look for innovative ways to counter information operations. This is especially the case since hiring an army of paid professionals, employing cyber criminals, or building armies of zombie or robotic networks is not an option for them. Cyber activism undoubtedly is, however.

The elves display a very good understanding of the global security environment and a great ability to adjust and face important new and emerging trends.

Thanks to the growing role of information technologies and social networks in daily life, which allows activists to disseminate information and mobilize audiences on a previously unthinkable scale, cyber activism is on the rise. The elves present a specific type of cyber activism, operating anonymously in semi-closed communities in the CEE countries devoted to monitoring and countering Russian information and cyber operations. The movement started as a group of less than 20 enthusiasts in Lithuania in 2014 and slowly expanded, first to the other Baltic states and eventually 13 European countries overall, effectively creating a stable network of thousands of volunteers.

The elves have managed to develop international cooperation among individual chapters across Europe, based on sharing information and best practices as well as occasional visits by representatives of each chapter. This cooperation is capped each year by the Elves Academy—an international congress at which about 100 volunteers learn under the leading elves new and valuable skills to protect and enhance their activities.

The elves display a very good understanding of the global security environment and a great ability to adjust and face important new and emerging trends. Even though, given proximity to their countries, Russia will most likely be always the primary target of the elves, with China's growing aggressive behavior

and increasing information operations in CEE cyberspace, the elves are starting to expand their focus to include countering actions from Beijing. This might be highly relevant for Western stakeholders and could play an important role in the future of the elves. The elves are discussing with members of civil society in Taiwan the establishment of the first Asian chapter.

When it comes to how to enhance the activities of the elves or to create conditions in which such movements are more likely to be founded and to blossom, perhaps the most important is that there is no one-size-fits all solution and that it is important to initiate the dialogue with the elves to learn about their needs directly from them. An equally crucial lesson is that the work of the elves is difficult, monotonous, time-consuming, and yet unpaid, and therefore that it is often difficult for the elves to keep their motivation. Thus, the least that can be done for the elves is to acknowledge their activities, read their media outputs, show public appreciation of their work, and help them spread their message.

Ultimately, the journey to a strong civic society that is resilient to information operations and other kinds of hybrid warfare by Russia or any other actor starts with every single citizen. We are the internet. We are social networks. We all need to assess online content critically, be careful with our personal data, respect "netiquette," and avoid hateful and aggressive behavior under any circumstances. And, perhaps most importantly, we must think before we share. Our future is our own responsibility; let us not make it someone else's video game.

This work represents solely the opinion of the author(s) and any opinion expressed herein should not be taken to represent an official position of the institution to which the author is affiliated.

About the Author(s)

Adéla Klečková focuses on hybrid and cyber warfare and related resilience and capacity building. She is a senior consultant for the Cyber Risk Advisory department at Deloitte. She graduated summa cum laude from the War Studies Department at the King´s College London. She is a member of the Digital Sherlocks Network founded by the Atlantic Council, specializing in advanced methods of open-source investigation. For her research activities in the field of cyber warfare, she was named to be one of the "35 under 35" young leaders in techno-politics by to the Spanish governmental think tank CIDOB.

About the ReThink.CEE Fellowship

As Central and Eastern Europe faces mounting challenges to its democracy, security, and prosperity, fresh intellectual and practical impulses are urgently needed in the region and in the West broadly. For this reason, GMF established the ReThink.CEE Fellowship that supports next-generation policy analysts and civic activists from this critical part of Europe. Through conducting and presenting an original piece of policy research, fellows contribute to better understanding of regional dynamics and to effective policy responses by the transatlantic community.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of World War II, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

G | M | F

Ankara • Belgrade • Berlin • Brussels • Bucharest
Paris • Warsaw • Washington, DC

www.gmfus.org