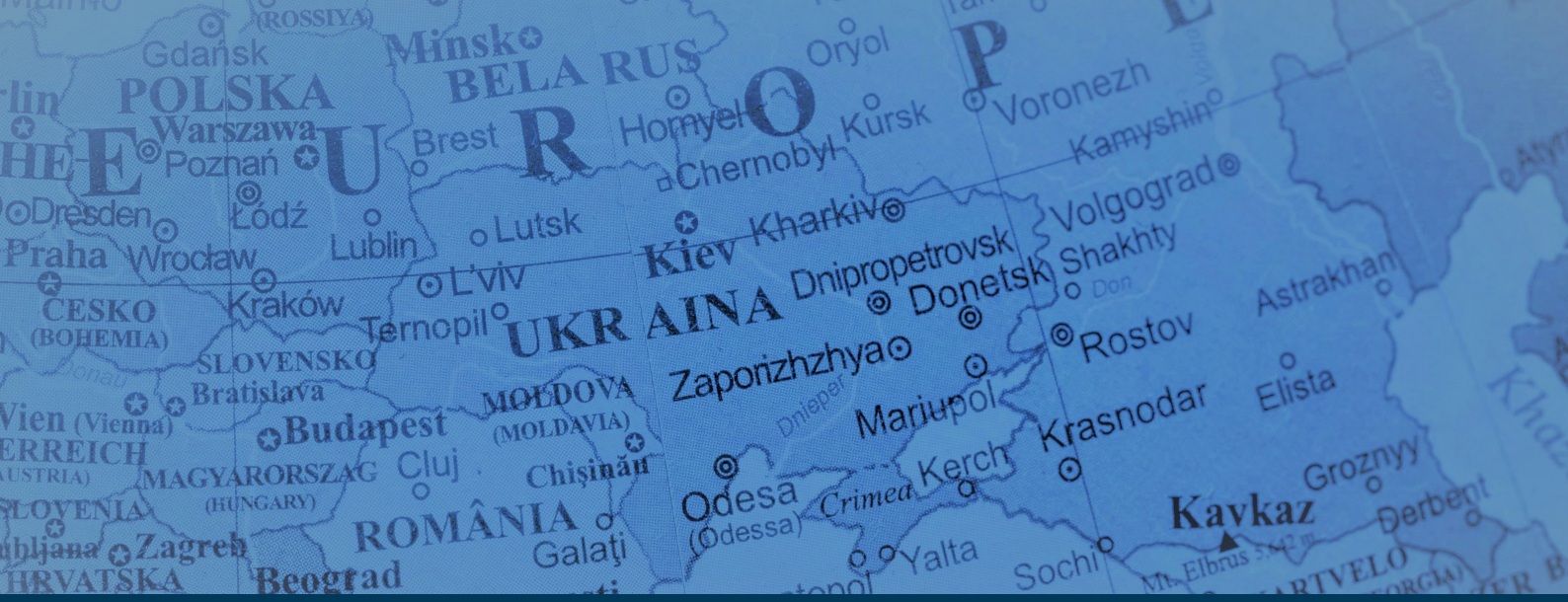


G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Policy Paper

June 2019 | No. 15

RUSSIAN INFORMATION WARFARE IN CENTRAL AND EASTERN EUROPE: STRATEGIES, IMPACT, COUNTERMEASURES

MICHAL BOKŠA

Rethink.CEE Fellowship

Please direct inquiries to:

The German Marshall Fund of the United States
1744 R Street, NW
Washington, DC 20009
T 1 202 683 2650
F 1 202 265 1662
E info@gmfus.org

This publication can be downloaded for free at http://www.gmfus.org/listings/research/type/publication.

Cover photo credit: Victor Maschek / Shutterstock.com

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF contributes research and analysis and convenes leaders on transatlantic issues relevant to policymakers. GMF offers rising leaders opportunities to develop their skills and networks through transatlantic exchange, and supports civil society in the Balkans and Black Sea regions by fostering democratic initiatives, rule of law, and regional cooperation. Founded in 1972 as a non-partisan, non-profit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

About the 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 the Author

Michal Bokša is a lecturer at the University of Economics in Prague, where he teaches European security and international institutions within the Central and East European Studies Program. He specializes in international security, with research and analytical experience from the Organization for Security and Co-operation in Europe, the NATO Defense College, and most recently NATO Supreme Headquarters Allied Powers Europe where he worked within the Civil-Military Analysis Branch. He also carries out research projects on issues of democratic governance, digitalization, and e-governance in Central Europe. He holds an MPhil in international relations and politics from the University of Cambridge.

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

Executive Summary

Information warfare operates in a fast-paced and quickly changing environment. Partly as a result, it is more opportunistic than strategic. The dynamism of Russia's information warfare is best illustrated by the fact that over the last decade it underwent at least two strategic shifts—after the Russian-Georgian war in 2008 and in 2014 when Russia went from being risk-averse and stealthy to increasingly aggressive and risk-taking. Effective countermeasures, especially those applied in Central and Eastern Europe, must reflect this reality by being highly adaptable and agile—a factor that local anti-information-warfare capacities often lack.

Central and Eastern Europe is a unique space within the Euro-Atlantic area. It can be perceived as intrinsically more vulnerable to disinformation campaigns, especially because of the wider range of narratives that Russia can exploit there for such a purpose. Simultaneously, the region faces numerous deleterious trends that are favorable to information warfare tactics. The most evident one is the continuous decline in citizens' trust in traditional media platforms, which are the least likely to be polluted with disinformation. The inherent risks in such a trend have been exacerbated by increasing trust in online media platforms and reliance on social media networks for news, both of which are far more susceptible to disinformation and misinformation.

Nonetheless, there are also positives. Concerns about the effect of Russia's information-warfare capabilities are vastly exaggerated. Disinformation campaigns have an impact, often particularly evident during periods of societal tensions. However, their effects begin to fade away relatively quickly once such a period subsides. Likewise Russia's information warfare has so far proved unable to change the geopolitical orientation of targeted societies in the region as feared especially during the European migration crisis. Moreover, although information echo chambers are a real problem that should be tackled, it is worth noting that its actual scale and ramifications in the countries of Central and Eastern Europe remains to be determined, as is the number of people actually "caught" within them.

When compared with the rest of the EU, the societies of Central and Eastern Europe face the paradox of demonstrating a very high awareness of the issue of disinformation and fake news while showing only moderate concern for their potential implications. At the same time, these societies often view the authorities as responsible for taking the lead in tackling disinformation. This is auspicious as it provides governments with maneuvering space for implementing necessary regulations or establishing appropriate institutions.

Social media platforms could considerably further aggravate the implications information warfare might have. This is especially due to the still emerging field of computational propaganda or rapidly expanding technologies such as "deep fake" video and audio doctoring. Therefore, the platforms still contain unutilized potential for disinformation, unlike the disinformation portals that boomed in the region, particularly in 2015, but have become largely stagnant and unable to expand beyond their initial base.

One of the key challenges for the Euro-Atlantic area in general and Central and Eastern Europe in particular will be escaping from the circular debates surrounding information warfare that repeat—often vaguely defined—recommendations such as improving critical thinking, strengthening civil society, and reforming education. Similarly, there is still a lack of reliable and quantifiable data that would give more substance to the ongoing discussions and could play a considerable role in furthering the advancement of research.

One fact remains strikingly clear: information warfare and disinformation are inevitable. Consequently, governments and societies in Central and Eastern Europe will ultimately have to learn to live with them.

Russian Information Warfare in Central and Eastern Europe: Strategies, Impact, Countermeasures

MICHAL BOKŠA

The recent renewed interest in information warfare emerged as a result of the development of information technologies that in an increasingly digital media landscape can significantly affect and modify how it can be pursued. Although the modern era creates new opportunities for information warfare, a significant number of Cold war strategies still form its cornerstone. This is most evident in the case of Russia, which has not significantly changed its disinformation strategies since the Soviet times.[1] Instead, it tailored them for present-day application.

Russia began considerably reinvigorating its Soviet information warfare playbook after its war against Georgia in 2008. Although winning the war itself proved to be an undemanding task, Russia suffered a tremendous defeat in the information and media sphere that surrounded the conflict. In particular, it utterly failed in spreading its narrative for legitimizing its invasion in the eyes of the international community. This would have provided Russia with a greater degree of flexibility in diplomatic maneuvering.[2] After the war numerous Russian experts increasingly voiced the need for improved information warfare capabilities.[3]

Russia's information capabilities and tactics are bound together by only a general and rather uncoordinated strategy. Overarching goals can be broadly described as exploiting divisions within targeted societies, disrupting the unity of Euro-Atlantic structures, undermining liberal values, and promoting the notion that finding objective truth on any issue is virtually impossible.[4] However, such a broad range of goals, accompanied by lack of coordination, often merely translates into ad hoc campaigns. Russian information warfare as currently pursued is thus far more opportunistic rather than strategic.

Nevertheless, some societies have higher degree of vulnerability to Russian information warfare, with those of Central and Eastern Europe (CEE) among the best examples. A commonly cited reason for this is the relative weakness of local civil society, media, and political structures, which lower resilience against foreign influence campaigns.[5] Yet, their increased vulnerability similarly stems from the ethno-linguistic, regional, and historic realities, which provide additional platforms that can be exploited by information and influence operations.

Russian Narratives, CEE Vulnerabilities

It is important to first unravel the structure of Russian information campaigns, particularly the nexus between narratives used and the number of platforms that can be effectively targeted within a society. Russian information warfare can be understood as a system of cascading narratives, along which the intensity of influence operations and the number of platforms suitable for exploitation varies. Hence, societies with more platforms are inevitably at a higher risk due to the broader diversity of narratives that can be used to reach a larger audience.

The cascading narratives of Russian information warfare messaging can be categorized as the Russian World,

1 Keir Giles, Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power, Chatham House, March 21, 2016.

2 Anton Shekhovtsov, "Conventional bedfellows: The Russian propaganda machine and the western far right," Eurozine, October 27, 2017.

3 Anatoly Tsyganok, "Informational Warfare - a Geopolitical Reality," Russia Beyond, November 5, 2018.

4 Edward Lucas and Peter Pomeranzev, Winning the Information War Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe, Legatum Institute, August 2016.

5 Vulnerability Index, Political Capital, April 11, 2017.

Slavic unity, Ostalgia,[6] "anti" rhetoric, and alternative information narratives (see Figure 1). Importantly, they are closely interlinked—if one narrative category can be applied, all subsequent ones can be typically exploited as well. As a result, interpreting Russian interference through such an approach helps to identify the number of narrative categories that can be effectively exploited within a targeted society and, thus, assess its vulnerability potential.

To a large extent the applicability of parts of this structure also corresponds with geographical proximity to Russia itself, with societies that can be targeted directly by the Russian World narratives being geographically the closest while further away Slavic unity and Ostalgia narratives can be applied, and alternative information narratives used furthest from Russia.

Russian World (*Russkiy Mir*) narratives particularly target countries with significant Russian-speaking minorities. They focus on forging and deepening the bond between these communities and Russia by addressing them as Russian compatriots—in practice encouraging the self-identification of foreign nationals with Russia.[7] Countries such as Latvia, Estonia, Ukraine, Lithuania, and Moldova where Russian-speaking communities represent between 4 and 25 percent of the population fall into this category.[8]

Slavic unity narratives focus on establishing a sense of togetherness and common identity between Slavic people via a common ethno-linguistic background. They try to exploit and further fuel pan-Slavic tendencies, and promote the concept of Slavic brotherhood. These narratives commonly appear in Slavic-dominated CEE countries, such as the Czech Republic, Slovakia, and Poland, but they also surface in the Western Balkans, particularly in Serbia, Macedonia and Republika Srpska in Bosnia and Herzegovina.[9]

6 Ostalgia is a German term based on the combination of words Ost (in German "east") and Nostalgia. The term is used in Germany and sometimes in the CEE countries to describe a positive outlook on the pre-1989 communist past.

7 Andis Kudors and Robert Orttung, Russian Public Relations Activities and Soft Power, ETH Zurich, June 16, 2016.

8 "Russians In The Ex-U.S.S.R.: Then And Now," Radio Free Europe/Radio Liberty, June 12, 2018.

9 Jarosław Wiśniewski, "Russia has a years-long plot to influence Balkan politics. The U.S. can learn a lot from it," Washington Post, September 19, 2016.

Figure 1. Russia's Cascading Narratives.

Ostalgia narratives principally aim to invigorate a nostalgic link to the Soviet Union and the period before 1989 among societies of the former communist bloc. They also strive to challenge the U.S.-dominated international capitalist order. Narratives that fall within this category also aspire to support left-wing parties with pro-Russian tendencies, such as the Czech Republic's Komunustická strana Čech a Moravy, or Germany's Die Linke.[10] Although Ostalgia narratives mainly focus on Eastern European societies, support for left-wing parties also applies to the wider European arena; for example, to Greece's Syriza and Spain's Podemos. By capitalizing on its socialist past, Russia attempts to promote itself among such parties to gain further political influence abroad.

"Anti" rhetoric narratives strive to foment sentiments of opposition toward such targets as the EU, NATO, the United States, immigration, or liberalism. Although they appear throughout the Euro-Atlantic area, they are most discernible in EU member states, and they are typically accompanied by subtle and overt Russian efforts to bolster far-right parties. Furthermore, Russia's

10 Fredrik Wesslau, "Putin's friends in Europe," European Council on Foreign Relations, October 19, 2016.

ubiquitous and continuous push for conservative values and a nationalist agenda to a large extent represents the epitome of modern Russian self-advertisement, which resonates particularly well with nationalistic parties across Europe.[11]

Alternative-information narratives embody the attempts to propagate the notion that learning the objective truth is virtually impossible, reinforcing the opinion that neither governments nor the mainstream media provide a neutral account of reality. This is typically buttressed by spreading multiple narratives regarding particular events, making the explanation backed by facts to appear as only one among many possibilities.[12] For instance, in the month following the poisoning of Sergei and Yulia Skripal in the United Kingdom in 2018, Russia's propaganda network produced up to 24 separate stories as possible explanations for what happened.[13] Supporting conspiracy theories, foreign alternative media portals, disinformation websites, and utilizing Internet trolls are all strategies particularly linked to, but not exclusively, this category.

CEE countries are clearly vulnerable to the cascading narratives, not only due to weaknesses in their civil society, media, and political structures, but also because of the relatively high number of platforms and narrative categories that can be used in their case. The region's circumstances make it particularly appealing and suitable for Russian information and psychological operations. Furthermore, Russia is not ideologically restricted when applying information warfare tactics. It has demonstrated its ability to side simultaneously with parties across the entire political spectrum without undermining its links to any one of them.[14] This deepens vulnerability in CEE countries as their communist past often allowed residual post-communist parties or pre-1989 sentiments to endure while the current European security environment and the refugee crisis considerably fueled extreme right-wing parties.

11 Matt Bradley, "Europe's Far-Right Enjoys Backing from Russia's Putin," NBC News, February 10, 2017.

12 "Disinformation Review Issue 42," EEAS East StratCom Task Force, October 4, 2016.

13 David Omand, "Undercurrents: Episode 9 - Digital Subversion in Cyberspace, and Oleg Sentsov's Hunger Strike," Chatham House, June 1, 2018.

14 "In the Kremlin's pocket, Who backs Putin, and why," Economist, February 12, 2015.

The Amplification pyramid

Russia's effort to maximize the ramifications of its information warfare operations in the CEE countries has two intrinsic aims. First, the narratives disseminated need to be viewed as realistic and credible, ideally by a great majority of those who are exposed to them. Second, they must reach the widest possible audience, preferably becoming viral via social media and disinformation online platforms. A situation in which a narrative spreads without any direct Russian support is among the most desired conditions. Russia's ability to pursue these two aims largely determines the amplification effect of an information operation.

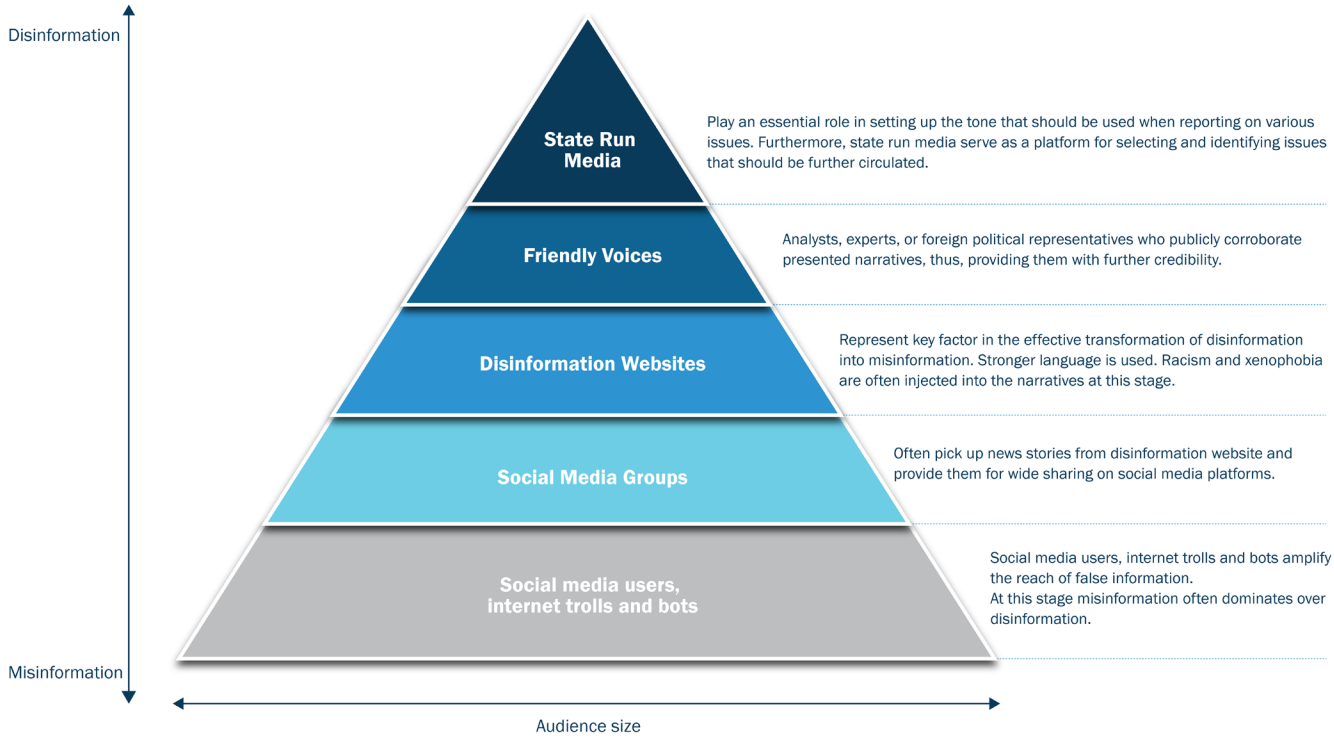
Disinformation (information known to be false and spread deliberately) becomes most effective when successfully transformed into misinformation (information not known to be false and spread unwittingly). Misinformation is rather easily replicated and diffused as the individuals sharing it are genuinely convinced of its veracity. Establishing a functioning structure (using state-run media, websites, and social networks) that can effectively transform initial disinformation into misinformation therefore plays an essential role in amplifying the effects of information operations.

Such a structure or process can be defined as an amplification pyramid (see Figure 2). Although transforming disinformation into misinformation is the ultimate aim, in practical terms such a process is never fully complete as both are circulated simultaneously. Hence, the transformation is perhaps better understood as a perpetually changing ratio between disinformation and misinformation circulating on a selected issue—from a situation where disinformation dominates to one where misinformation is increasingly present.

State-run Media and Friendly Voices

The launch-pad for disinformation or purposefully inaccurate stories is often Russian state-run or state-funded media channels such as RT (formerly Russia

Figure 2. The Amplification Pyramid.



Today), TASS, and Sputnik.[15] These play a crucial role in identifying issues and events that should be circulated while serving as an indication of the preferred Russian viewpoint. However, the direct impact of these channels is often greatly exaggerated as the size of their Western and CEE audiences is limited.[16] Nevertheless, they have an indirect impact either as a source of "alternative" information for CEE disinformation websites or by providing a platform for "friendly voices." The latter being domestic or foreign political interlocutors who are deliberately sought out in order to corroborate presented narratives.[17]

Disinformation Websites

Disinformation websites are another essential element in transforming disinformation into misinformation by allowing incorrect and/or misleading information to be circulated more independently. Numerous such websites have emerged in the CEE region relatively recently, often with opaque structures, anonymous ownership and non-transparent financial backing. They typically follow the worldview of Russia's state-controlled media, spread conspiracy theories, and tend to inject narratives with further xenophobia, fear-mongering, and alarming language. Likewise, they increase the reach of Russian disinformation by translating its content directly from Russian-language websites into CEE languages.[18] Such websites often cross-reference each other or tend to

15 Neil MacFarquhar, "A powerful Russian Weapon: The Spread of False Stories," New York Times, August 28, 2016.

16 Alexey Kovalev, "Hacking, Disinformation, and a New Cold War with Russia," ASPEN—IDEAS Festival, July 7, 2017.

17 Mark Galeotti, "Controlling Chaos: How Russia Manages its Political War in Europe," European Council on Foreing Relations, August 2017.

18 Dalibor Rohac, "Cranks, Trolls, and Useful Idiots, Russia's information warriors set their sight on Central Europe," Foreign Policy, March 12, 2015.

recycle the same content.[19] It is difficult to establish their number in each CEE country, particularly due to the blurred line between what actually constitutes a disinformation website and what does not. Nonetheless, the number of platforms that propagate Kremlin-inspired narratives in the Czech Republic, Slovakia, and Hungary is generally estimated to range from 50 to 100.

The three initial stages in the amplification pyramid—Russian state-controlled media (overt or 'white' influence), friendly voices, and disinformation websites (more opaque or 'grey' influence) are closely interlinked.[20] They depend on each other for mutual corroboration while also striving to spread the notion that the perceptions they disseminate are widespread among the public and expert or academic circles. Although Russia's state-controlled media is usually the initiator of the disinformation process, in some cases the dynamic might be reversed and Russian "white" media might recycle material from foreign channels that could be regarded as dubious, misleading, or conspiratorial.[21] In such an instance the initiator would be the disinformation channel rather than the state-run media. This further demonstrates the opportunistic nature of such an apparatus and its flexibility to react and adapt to an ever-changing environment.

Social Media Groups and Users, Trolls and Bots

While at times fulfilling similar roles as disinformation websites, social media groups have several additional features. Although they use the same alarming language and fear-mongering, by their intrinsic virtue they create a connection and network between like-minded social media users more effectively. This allows for the reinforcing of users' views and the further radicalization of individual opinions. Most importantly, social media groups, due to their network-building nature, have a considerably higher mobilization potential. Numerous protests, rallies, and demonstrations congruent with Russian narratives that have taken place in the CEE region have been organized via social media groups.[22] Harnessing the pro-Kremlin mobilization potential abroad is one of the key goals of Russian information campaigns.[23] Furthermore, such a goal is pursued for domestic and foreign policy purposes alike as pro-Russia protests abroad are used in the Russian media to shore up the public's approval of Russia's policies beyond its own borders. Although in that regard larger events are preferred, the size of the gathering and its direct effects are not always as relevant as the fact that a protest took place and can be reported on.

> *"Although the most common path for a disinformation or crafted narrative from its initial disseminator to the targeted audience can be identified, by no means is the process rigidly established.*

Social media users, Internet trolls, and bots represent the final level within the amplification pyramid. For a majority of ordinary social media users, the misleading or false information they share at this point can be within the cycle identified as misinformation—those who share it online genuinely believe in the content. Additional activities of Internet trolls ("professional" social media users and article commentators) and bots (automated scripts established to operate over major social networking applications) provide a relatively solid bedrock of misleading information by continuously recycling the information or by cross-referencing it. Consequently, even if users conduct a quick search to verify a story or piece of information, numerous corroborating disinformation portals or "friendly voices" are encountered, making the story appear more reliable and trustworthy. Hence, strengthening the users' perception that the shared content is genuine.

19 Ivana Smoleňová et al., United we stand divided we fall: The Kremlin's Leverage in the Visegrad Countries, Prague Security Studies Institute, November 2017.

20 Clint Watts, Disinformation: A Primer In Russian Active Measures And Influence Campaigns, U.S. Senate Select Committee on Intelligence hearing, March 30, 2017.

21 Alexey Kovalev, "Hacking, Disinformation, and a New Cold War with Russia."

22 For instance, Jan Martinek, "Na sociálních sítích se houfují odpůrci amerického konvoje," Novinky, March 18, 2018.

23 Michael Kofman et al., Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation, 2017.

Ultimately, the amplification pyramid is a very complex and multi-layered process. Although the most common path for a disinformation or crafted narrative from its initial disseminator to the targeted audience can be identified, by no means is the process rigidly established. As mentioned above, particularly during the early stages of the cycle, disinformation might originate from varying sources such as state-run media, friendly voices, disinformation portals, or even from an individual social media user. Nonetheless, to increase the effectiveness of misleading or false information the process is applied to allow initial disinformation to be transformed into misinformation– ideally reaching a point where misinformation begins to be spread independently by genuine social media users who are convinced about its veracity. Under such conditions the original disinformation reaches vast audiences while maintaining perceived authenticity.

Impact of Russian Information Warfare on CEE Societies

When it comes to Russian information warfare in CEE countries, it is important to highlight, that its actual impact has proved to be somewhat limited. Russia's efforts to penetrate the region's digital media and social networks landscape are certainly acute. The existence of dozens of disinformation portals and news channels, the increasing activity of Internet trolls and bots, and the considerable number of friendly voices in the region demonstrate that the threat is present and considerable. However, on various occasions the capacity of Russia's information warfare to undermine democratic governance in the CEE countries has been exaggerated.

This is illustrated by the recent example of European migration crisis, which became a commonly exploited topic by disinformation portals particularly during its peak in 2015 and in months that have subsequently followed well into 2016.[24] Throughout this period, pro-EU sentiments within the CEE countries typically showed a gradual decline, especially due to local opposition to accepting refugees in general and against EU refugee relocation quotas in particular. The Visegrad 4 countries (the Czech Republic, Hungary, Poland, and Slovakia) took a unified and rejectionist approach at the EU level.[25] The gradual decline in pro-EU sentiments was reflected in polls: from spring 2015 to autumn 2015 the positive image of the EU in CEE countries dropped by 10 percentage points in the Czech Republic, 7 in Bulgaria, 5 in Romania, 4 in Hungary, and 4 in Slovakia. Poland was in this period the exception as the image of the EU within Polish society improved by 2 percentage points.[26] However, in the following period the EU's image in Poland fell similarly by 8 percentage points.[27]

The heightened activity of Russia's disinformation has been often regarded as one of the key factors contributing to the EU's eroding image within the CEE region. This perception was strengthened by the fact that since 2014, especially following the annexation of Crimea, Russia's information warfare entered into another, perhaps even more aggressive, phase while also becoming mainstream within Russian military thought.[28] A once careful, risk-averse, and stealthy actor underwent a tactical shift in 2014, becoming more careless and risk-taking.[29] Therefore, the EU's eroding image in the region throughout 2015 and 2016 coincided with new and increasingly aggressive Russian information warfare tactics, leading to the belief that there was a causal effect between the two.

This was also a period when information warfare received very high public attention, leading to dozens of national, international, and civil-society initiatives and projects for countering information warfare activities. The EU's East StratCom Task Force, which runs the 'EU versus Disinformation' campaign, was set up in 2015.[30] The European Centre of Excellence for Countering Hybrid Threats was endorsed by the Council of the

24 "The pro-Kremlin narrative about migrants," EU vs Disinfo, May 16, 2017.

25 "Illiberal central Europe, Big, bad Visegrad," Economist, January 28, 2016.

26 "Standard Eurobarometr 84," European Commission, December 2015.

27 "Standard Eurobarometr 85," European Commission, July 2016.

28 Keir Giles, The Next Phase Of Russian Information Warfare, Nato Strategic Communications Centre of Excellence, May 20, 2016.

29 Thomas Rid, "Disinformation: A Primer In Russian Active Measures And Influence Campaigns," Select Committee On Intelligence, United States Senate March 30, 2017.

30 "Questions and Answers about the East StratCom Task Force," European External Action Service, August 11, 2017.

EU and the North Atlantic Council in December 2016.[31] Although such initiatives ultimately play a very positive role in combating information warfare and in raising public awareness, their swift emergence between 2014 and 2017 further encouraged the notion that Russia possessed alarming and far-reaching capabilities.

Russian disinformation campaigns played a role in increasing tensions and anti-immigration sentiments within Central European societies and thus contributed to the considerable decline of the EU's image in the region between 2015 and 2017. Nevertheless, ascribing this deterioration predominantly to Russian efforts is inaccurate and an overstatement. Although the form and intensity of Russia's information warfare have remained virtually unchanged since it entered its more aggressive phase in 2014, pro-EU sentiments in the CEE region and in the EU at large began to rise again. In May 2018 Eurobarometer even indicated record support for the EU since its surveys began in 1983.[32] The improvement was particularly substantial in Romania (+8 points), Hungary (+8 points), the Czech Republic (+5 points) or Bulgaria (+5 points).

> *"On various occasions the capacity of Russia's information warfare to undermine democratic governance in the CEE countries has been exaggerated.*

Although Russian disinformation campaigns have been systematically applied in the CEE region, and more aggressively so since 2014, they have not diminished pro-EU sentiments in the long run. This stems from the limits that are inherently imbedded in the opportunist nature of current Russian tactics. As a result, these campaigns typically have a wider impact on a targeted society in times of tensions, which they exacerbate. Nonetheless, once tensions or crisis situations subside, the ability of the Russian efforts to have a notable impact in a targeted country—for example, on public sentiments toward its geopolitical orientation—fades away relatively quickly.

The limitations of Russian disinformation can be also seen in the local support for other Western organizations, such as NATO, which similarly as the EU, is a common target for disinformation portals and for Russian-inspired fake news. In spite of NATO being targeted on a daily basis, public opinion in the region has remained favorable to the alliance.[33]

Limitations and Public Awareness

There are other aspects that indicate that Russia's information warfare has in many respects reached its limits in the region. Russian state-led media channels, such as RT, TASS, or Sputnik, often do not enter the CEE media landscape directly. In fact, virtually none are widely consumed by local populations. None of them are among the most followed media platforms (including television, radio, print, and online) in any of the CEE countries. Their first-hand local audience is marginal, represented by a single digit weekly usage percentage point. For example, within online platforms, the Czech version of Sputnik has only 2 percent weekly usage as opposed to the three most-followed brands–Seznam, iDnes, Aktuálně, which have 52 percent, 40 percent, and 32 percent weekly usage rates, respectively.[34]

As a result, and as indicated in the discussion of the amplification pyramid, such channels are often dependent on local disinformation portals and social media groups to reach CEE audiences. Yet, the disinformation portals have reached their maximum potential and will not be able to significantly expand the influence base they have managed to acquire in the CEE region over the past

31 "About us," The European Centre of Excellence for Countering Hybrid Threats.

32 "Public Opinion survey finds record support for EU, despite Brexit backdrop," European Parliament, May 23, 2018; "Standard Eurobarometer 85," European Commission, July, 2016; "Standard Eurobarometer 89," European Commission, June, 2018.

33 Barbora Maronkova, "NATO in an Era of Fake News and Disinformation," USC Center on Public Diplomacy, February 1, 2017. The exception being Bulgaria. Michael Smith, "Most NATO Members in Eastern Europe See It as Protection," Gallup, February 10, 2017.

34 Nic Newman et al., Reuters Institute Digital News Report 2018, Reuters Institute for the Study of Journalism, 2018.

years.[35] This is corroborated by the fact that the number of country-specific disinformation portals that are truly active has in recent years remained largely stagnant across the CEE countries.

> *"Despite the limitations that Russia's disinformation campaigns face in the CEE region, there are several trends that strengthen existing vulnerabilities or create new ones.*

For example, following the annexation of Crimea and with the rise of more aggressive information warfare tactics, the number of pro-Russian portals and blogs in Hungary skyrocketed in 2015. By early 2016 there were approximately 90 such websites.[36] This number has since remained virtually unchanged as there still are between 80 to 100 such online platforms.[37] Likewise, in early 2015 there were by one estimate 42 online platforms disseminating pro-Russian news in the Czech or Slovak languages.[38] In 2016 another study found 39 active pro-Russian disinformation websites.[39] In late 2017, 40–50 were identified.[40] The most recent efforts to calculate the number of active pro-Russian platforms in the Czech Republic, including by the Interior Ministry, reach similar conclusions.[41] A comparable situation can be observed in other countries of the region.

The recent inability of CEE's disinformation portals to further expand and increase their audience size, even as some attempt to do so by amplifying their output, emphasizes the limitations such portals face. Overall, it is unlikely that in the coming years they will be a factor that could significantly buttress Russia's current information warfare's effectiveness.

Finally, the limitations of Russian campaigns are epitomized by rising public awareness regarding disinformation. This trend stems from the fact that since the annexation of Crimea more CEE think tanks and initiatives have attempted to counter disinformation by informing the public. This has been accompanied by increasing media focus on the issue. Partly as a result, citizens in the CEE countries—particularly in Hungary, Romania, the Czech Republic, and Bulgaria—demonstrate considerable awareness of being exposed to fabricated news online compared to those in the rest of EU.[42] Nevertheless, the CEE region still has considerable room for improvement in this regard. In a 2018 poll, on average across 37 countries 54 percent of respondents said they were very or extremely concerned about fake news on the Internet. Romania was the only CEE country above this average, with 60 percent. The responses were less encouraging in Hungary (50 percent), Bulgaria (49 percent), the Czech Republic (43 percent), Poland (42 percent), or Slovakia (36 percent).[43] Hence, the CEE countries overall share a phenomenon of having a relatively high awareness of disinformation and fake news while being only moderately concerned about its potential implications.

Alarming Trends in Old and New Media Platforms

Despite the limitations that Russia's disinformation campaigns face in the CEE region, there are several trends that strengthen existing vulnerabilities or create new ones. A particularly alarming one is the relatively low trust in the objectivity of traditional media platforms and mainstream broadcasters. According to a 2017 survey, a significant proportion of respondents in the Czech Republic (46 percent), Hungary (39 percent), Poland (36 percent), and Slovakia (38 percent) did not consider mainstream broadcasters or newspaper as evenhanded. In fact, a common view was that, although they try to be

35 Roundtable discussion, conducted under the Chatham House Rule, on disinformation and security at the American Center in Prague on October 19, 2018.

36 Bátorfy Attila, "Fake news: Vladimir's Best Disciples," Atlatszo, June 15, 2017.

37 Ivana Smoleňová et al., United we stand divided we fall.

38 "42 českých a slovenských webů, které šíří ruské lži," Echo24, February 27, 2015.

39 Jakub Janda and Veronika Víchová, Fungování českých dezinformačních webů, Evropské hodnoty, July 26, 2016.

40 Ivana Smoleňová et al., United we stand, divided we fall.

41 "Vnitro má databázi dezinformačních webů. Koho na ni zařadilo?" Neovlivní, June 22, 2017.

42 Nic Newman et al., Reuters Institute Digital News Report 2018, p. 39.

43 Ibid., p. 18.

unbiased, major media platforms hold a "worldview which prevents them from reporting the full picture."[44] Analyzing 2017 data, the CEE countries were among the EU member states with the least trust in radio, television, or the print media. The only exception was Bulgaria where trust in television was above the EU average.[45]

The traditional media in the CEE region are simultaneously finding themselves undermined by governments. This has been particularly evident in Hungary and Poland. In 2003 Reporters Without Borders ranked Hungary and Poland 21st and 33rd respectively for freedom of the press.[46] By 2018, Poland has dropped to 58th and Hungary to 73rd. These are not isolated examples within the region. An even more significant plunge can be observed in Bulgaria, which fell from 34th to 111th.[47] The trend of declining media freedoms, although to a lesser extent, has also been noted in Slovakia and the Czech Republic, the only two CEE countries where the press is still regarded as free by Freedom House.[48] Such systemic deterioration throughout the region has adverse implications that make the situation more conducive for external disinformation campaigns.

> *"Whether it is already low or plummeting, press freedom in Central Europe increasingly represents a new vulnerability.*

Whether it is already low or plummeting, press freedom in Central Europe increasingly represents a new vulnerability, and not only because its erosion inherently undermines democracy.[49] With less press freedom, CEE publics are more likely to be driven away from otherwise well-regulated media platforms such as radio, television, or the written press (which are typically far more difficult for disinformation efforts to penetrate) as these will be the first to be affected, unlike the social media or Internet which are more insulated from the government's reach. Therefore, as freedom of the press diminishes, so does the trust in media platforms that have a considerably higher chance of not being polluted by misleading information and fake news.

While trust in traditional media platforms is often critically low in the CEE region, trust in the newer platforms has been particularly high there compared with the rest of the EU. This is ominous since disinformation campaigns are being conducted predominantly online. According to estimates, average trust in the Internet media platforms within the EU was at 34 percent in 2018. By comparison, CEE countries have some of the highest rates of trust in the Internet in the EU, with the Czech Republic (50 percent), Hungary (49 percent), Poland (46 percent), and Bulgaria (45 percent) ranking second, third, fourth, and sixth respectively. Slovakia (42 percent) and Romania (37 percent) are likewise above the EU average.[50] This creates vulnerabilities that make the CEE region overall more susceptible to information warfare tactics.

The consumption of traditional media channels in some CEE countries has thus been increasingly replaced by the consumption of news through social media—that is, platforms that are most rife with misinformation and with a high concentration of trolls and bots. It is by now widely documented that misleading information (fake stories and hoaxes) spread considerably faster and further on such platforms than fact-based information or news. Likewise, social media are an inappropriate source of news especially due to a lack of governmental regulations, which stems from the fact that legislation itself typically struggles with determining what type of definition should be applied when discussing such platforms.[51]

44 Public opinion in Hungary, Poland, Czech Republic and Slovakia, International Republican Institute, May 24, 2017.

45 Fake news and disinformation online, Flash Eurobarometer 464, European Commission, April 2018.

46 Press Freedom Index 2003, Reporters without Borders, 2003.

47 Press Freedom Ranking 2018, Reporters without Borders, 2018.

48 Europe, Freedom House.

49 "Protect press freedom to protect democracy and our rights, says FRA," European Union Agency for Fundamental Rights, May 3, 2017.

50 Market Insights: Trust in Media 2018, European Broadcasting Union, February 27, 2018.

51 Elina Lange Ionatamishvili, a senior expert from the NATO Stratcom Center of Excellence, interview, October 30, 2018.

Yet, significant portions of society in the region use social media as a source of daily news—47 percent of respondents in the Czech Republic, 41 percent in Hungary, 40 percent in Slovakia, and 34 percent in Poland. Additionally, 30–33 percent in each of these countries access news in this way once or twice per week.[52] Teenagers and the younger generations are far more likely to get news via such platforms.[53]

These trends related to new and old media platforms, exacerbated by declining media freedom across the CEE region, are alarming.[54] It is apparent that, rather than the Russian state-run media channels or disinformation portals, it is social media platforms that are of most concern and have far-reaching implications. Social media possess a relatively significant but not yet fully utilized potential in the region that disinformation could exploit, with the prospect of still attaining greater audience size and enhancing its effectiveness. What is more, computational propaganda techniques are very likely to allow for the further optimization of disinformation content for individual social media users on social media platforms.

Effective Countermeasures

Currently, one of the most considerable challenges in the debate surrounding tackling information warfare is its continuous repetition and the ambiguous advice it generates. The growing number of reports on tackling information warfare provide only vaguely defined recommendations such as improving critical thinking, strengthening civil society, or reforming education systems. Moreover, the debate also seems unable to make progress on this issue beyond the knowledge that was established by 2015 approximately. Seeking original approaches while developing the ability to adapt rapidly to the ever-changing circumstances of disinformation techniques is a key necessity that anti-information warfare initiatives and institutions should strive for. By no means should efforts endeavoring to enhance critical thinking, strengthen civil society, or reform education systems be abandoned but they do not offer any short-to-medium-term solutions.

It is near impossible to eradicate or abolish fake news and disinformation, or the resulting misinformation. These are now a feature of the landscape for democracies, which will need to learn how to live with them, as long as they desire to preserve the current levels of media freedom. Nonetheless, what can be accomplished is to limit significantly the ability of disinformation to impact society.

Debunking and Real-Time Tracking

In recent years numerous debunking platforms have either spontaneously emerged from civil society across the CEE region or have been established by the authorities, typically at the international level. The EU's East StratCom Task Force with its "EU vs disinformation" campaign and the StopFake website focusing on disinformation targeting Ukraine are excellent examples. Such platforms not only help to raise awareness about disinformation, they also yield hard evidence and tangible examples of what fake news looks like.

Nonetheless, even the most systematic and methodological debunking will never be sufficient.[55] In social media, fake news tends to outperform genuine stories in likes, shares, and comments by a considerable margin. It has also been demonstrated that once a misleading story has been published, the subsequent correction does not reach the full audience that consumed it.[56] The same dilemma can be applied to debunking attempts, where the response stories will never reach all of the disinformation's original audience. Furthermore, with the amount of disinformation circulating every day, there is virtually no institution that would have the capacity to pick up, target, and debunk every fake story that appears on social media platforms. Instead of attempting to flood social media with an endless trail of debunked disinformation, the effort needs to be highly concentrated elsewhere.

52 Public opinion in Hungary, Poland, Czech Republic and Slovakia, International Republican Institute.

53 Katerina Eva Matsa et al., "Younger Europeans are far more likely to get news from social media," Pew Research Center, October 30, 2018.

54 Mária Vásárhelyi, "The Takeover and Colonization of the Hungarian Media," Aspen Review, 1, 2017, Aspen Institute Central Europe, p. 23.

55 Jonathan Freedland, "Russia's brazen lies mock the world. How best to fight for the truth?" Guardian, September 15, 2018.

56 On-line propaganda: stará hra v nových kulisách, Prague Security Studies Institute, 2017.

The large majority of disinformation stories or fake news in daily circulation will never have a significant effect on a large part of a targeted society. Their impact will often be limited to only very marginal groups. Therefore, CEE governments should first strive to identify the disinformation that has the potential to become widespread

> *"Unfortunately, the CEE countries cannot fully rely on Euro-Atlantic or other joint Western platforms.*

or is being pushed by foreign efforts. Disrupting the process of transformation by which disinformation becomes misinformation with the potential of going viral on social media platforms represents a more effective approach. According to Jakub Kalenský, a former analyst on the EU's East StratCom team, the most effective tool is to kill the disinformation before its circulation amplifies.[57] The problem CEE countries often face is that they lack the ability to identify the trending disinformation that should be targeted. As a result, the reaction of local civil society initiatives or government institutions is often too little, too late. Developing such capacity should be a priority.

Online trolls and bots play a considerable role in boosting and spreading narratives. When there is an effort or desire to popularize misleading information, such accounts start to act by tweeting it, sharing it, and commenting on it, and more broadly disseminating it on a large scale. Having a platform that would follow and track a large number of such accounts in a near real-time would be highly desirable for combatting disinformation in the CEE region before it becomes viral.

Such projects already exist. For example the German Marshall Fund's Alliance for Securing Democracy runs the HAMILTON 68 dashboard, which follows Twitter accounts that have been identified as linked to Russian information operations. It provides data for the most recent trending topics, shared URLs, and hashtags.[58] Such an approach allows not only for a better understanding of Russian tactics, but also for a considerably enhanced ability to react rapidly to the most recent and trending disinformation or misleading news. Likewise, NATO's Strategic Communications Center of Excellence (NATO StratCom) developed and operates a machine-learning program that tracks Russian bot activity on social media platforms.[59] However, in this instance the results are not provided via an interactive interface but through the Robotrolling reports. Both initiatives are examples of best practice.

Should the CEE countries wish to increase their response capability and their overall agility within the information space, they need to develop a platform that would in (nearly) real time track, follow, and ideally publish the activity and narratives pushed by social media trolls and bots. In fact, by merely following a large enough number of pro-Russian accounts, a very accurate picture can be established as to which narratives are being promoted and most likely to go viral. Such data also provide a very clear and effective indication as to which narratives need to be debunked and dismissed as fake news before they become widespread throughout social media platforms.

Unfortunately, the CEE countries cannot fully rely on Euro-Atlantic or other joint Western platforms in this regard, due to the unique category of narratives that are exploited in the region. The narratives based on ideas such as the Russian world, Slavic unity, or Ostalgia do not typically emerge elsewhere in the Euro-Atlantic area. For example, disinformation based on Slavic unity might trend in the CEE region, or even just part of it, but might not appear as significant for platforms that follow trending narratives within the entire Euro-Atlantic area. Hence, a regional focus for such efforts is essential.

Government Capacity Building and Social Media Cooperation

Considering that social media platforms are most likely to aggravate the threat of information warfare, the

57 Jakub Kalensky, non-resident senior fellow Atlantic Council, interview, November 2, 2018.

58 "Hamilton 68," Alliance for Securing Democracy, German Marshall Fund of the United States.

59 Elina Lange Ionatamishvili, interview.

question arises as to who should tackle disinformation in this specific area. According to polls in the CEE countries, the majority of citizens see journalists and national authorities (relatively equally) as having the chief responsibility in combatting disinformation. The former being the most preferred solution in the Czech Republic,[60] Poland, Romania, and Slovakia. The national authorities was the preferred option in Bulgaria and Hungary (where journalist did not even make the top three options).[61] Such views create a very conducive environment for developing effective anti-information warfare measures or institutions at the governmental or inter-governmental level.

Typically, governments progress very cautiously on matters such as establishing institutions that would realistically engage in what is by some regarded as censorship of news and social media. Governments labeling what is genuine reporting and what is fake news can be very controversial. This is exacerbated by the fact that this view at times originates not only from the public but also from high-ranking politicians. For instance, in 2017 when the Czech government established within the Ministry of Interior a new Center Against Terrorism and Hybrid Threats, which also focuses on disinformation campaigns, President Miloš Zeman warned against its activities and publicly described the new institution as the "Ministry of Truth."[62]

Nonetheless the fact that opinion polls show rather strong support for national authorities taking actions against disinformation gives governments maneuvering space that should be utilized—the question then is how to do so most effectively.

Possibly one of the most effective ways to secure social media platforms against disinformation or malicious use is through cooperation between public authorities (governments and inter-governmental institutions) and private social media companies. The approach to each platform needs to be differentiated to an extent as each has, for example, diverging privacy settings. As a result, while quantitative computing and external studies of varying, potentially fake, accounts might be relatively easily applied to Twitter or VKontakt, the situation is diametrically opposite in the case of Facebook. Nevertheless, even for platforms like Facebook, several institutions have already developed effective tools and instruments to combat information warfare. For instance, NATO StratCom currently conducts and implements numerous experimental methods on a Facebook platform, ranging from hijacking pre-set accounts to purchasing specific ads and tracking where the "likes" originate from in order to expose the network's vulnerabilities. Discovered weaknesses and lessons learned are subsequently communicated directly to the social media platforms. Another auspicious development is the significant increase in the degree to which social media platforms are willing to collaborate, even if there is room for further improvement.[63]

> *"The fact that opinion polls show rather strong support for national authorities taking actions against disinformation gives governments maneuvering space.*

The CEE countries should follow such an example and strive to develop related or similar institutions on a national or regional basis that would have the capacity to communicate discovered vulnerabilities to these platforms. Additionally, they should also start to make a far greater contribution to already established initiatives. That can be done, for example, by providing seconded national experts focusing either on social media platforms or specifically on the region. Likewise, using diplomatic channels in order to press NATO and the EU to expand the role, magnitude, and staff of their StratCom institutions should be also considered. A comparison can be made with the European Border and Coast Guard Agency. Once immigration became a highly

60 "Press and Broadcasting Management" was another answer in the Czech Republic that was given as many times as "Journalists."

61 "Fake news and disinformation online," Flash Eurobarometer 464.

62 Barbora Janáková, "Centrum proti terorismu vyvrátilo za rok 22 dezinformací. Má i jiné úkoly," iDnes, March 23, 2018.

63 Sebastian Bay, senior expert from the NATO Stratcom COE, interview, November 2, 2018.

politicized issue at the EU level, the agency underwent a rapid expansion in its budget and staff. Between 2015 and 2017 its budget more than doubled and its staff increased to 488, with a goal of having 1,000 by 2020.[64] By comparison, NATO StratCom employs approximately 30 people, where less than ten focus on Russian disinformation operations on a continuous basis.[65] Similarly, the EU's East StratCom team consists of 16 full-time employees.[66] Consequently, institutions focusing on information warfare should be given increased attention and diplomatic support from the CEE region. Political will can significantly boost their operational capacity. Likewise, the CEE countries should be less hesitant in developing similar capacities domestically or jointly.

Social Media and Government Regulation

Another option in dealing with social media companies is to focus on the regulatory framework that governs them. Over the past decade social networks have transformed from mere platforms to socialize online into channels that provide daily news to large segments of society. Consequently, the implementation of appropriate regulatory framework is of the utmost importance.

Almost all interviewed experts agreed that improved regulation of social media platforms is needed. Here too, the fact that public opinion throughout the CEE is favorably disposed toward government action in this area should help in legislating for and implementing at least to some degree a better regulatory framework. Nevertheless, regulating social media has two essential pitfalls that are relevant for the CEE region.

Germany is one example of where some regulation has been effectively applied to social media platforms. Its Network Enforcement Act (NetzDG), which was passed in 2017, requires social media sites with more than 2 million members to remove hate speech, fake news, and illegal material in 24 hours or to face fines up to €50 million.[67] Platforms such as Facebook have acted accordingly; the company's German deletion center, one of its largest, grew rapidly to more than 1,200 content moderators who are tasked with eliminating material that violates the law.[68]

Such regulation has the ability to considerably restrict the reach of hate groups that have a well-established presence throughout social media platforms. They are effective particularly with regard to Russian "anti" narratives, which are often rife with racism and xenophobia. However, Russian world, Slavic unity, and Ostalgia narratives are not particularly affected, especially as they can be easily perceived as promoting peaceful perspectives. Consequently, regulations such as Germany's NetzDG can be a model for CEE governments for targeting openly hateful narratives, but their effectiveness has limits in a region where other types of narratives are also prevalent.

> *"Overregulating social media and online space in general can also have negative consequences.*

Overregulating social media and online space in general can also have negative consequences. Considering the recent trend of deteriorating press freedoms in the CEE region, this could in the medium-to-long term provide some governments not only with an excuse, but also real instruments to suppress political opponents who use the Internet as a refuge where they can voice criticism.[69] Already now, as indicated earlier, only the Czech Republic and Slovakia are perceived to have a fully free media, unlike the rest of the region where the media is viewed merely as partly free.[70] Strong government regulation of the Internet, and of social media in particular, could in

64 "Migration control top priority at Member State level—substantial growth of EU Agency Frontex," European Council on Refugees and Exiles, October 13, 2017.

65 Elina Lange Ionatamishvili, interview.

66 "Questions and Answers about the East StratCom Task Force," European External Action Service.

67 "Germany starts enforcing hate speech law," BBC News, January 1, 2018.

68 Katrin Bennhold, "Germany acts to tame Facebook, learning from its own history of hate," Independent, June 15, 2018.

69 Annabelle Chapman, "Pluralism Under Attack: The Assault on Press Freedom in Poland," Freedom House, June 2017.

70 "Freedom of the Press 2017," Freedom House.

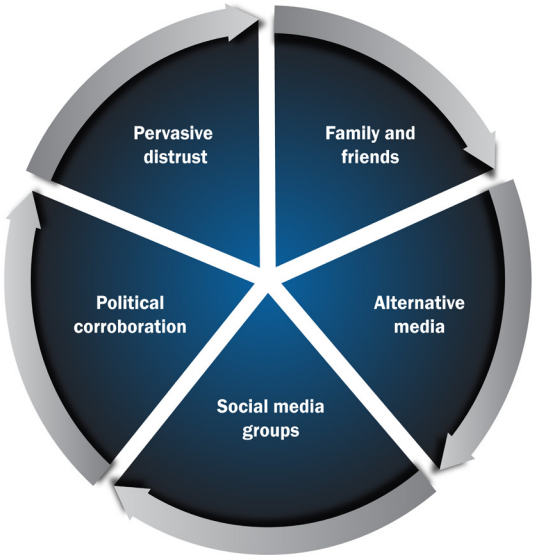
some CEE countries considerably undermine a space that is still relatively free from domestic political interference.

Social Media Transparency and the Private Sector

Since regulations can be exploited for political gain, striving and pushing social media platforms for increased transparency is another strategy that should be pursued and perhaps, considering the downsides of regulation, prioritized. Currently, they often operate in an environment of relative opacity, making it virtually impossible to carry out effective research into how to strengthen social media networks against information warfare in general and disinformation campaigns in particular. Yet, increased transparency and its resulting benefits could elevate information warfare countermeasures to a new level of effectiveness. As social media platforms are the most likely vehicle to be further utilized and expanded for disseminating disinformation, this is where governments should concentrate information warfare countermeasures and push for further transparency. In other words, borrowing a term once popular in Central and Eastern Europe, social media like the traditional media platforms before them need to deliver Glasnost.

Increased transparency within the social media space must be supported especially for accountability purposes, as only with accountability can attribution be effectively established. It is lack of attribution that makes disinformation campaigns so appealing to their perpetrators as there are only very marginal costs for conducting them.[71] Being able to better track the origin of harmful or misleading content would be among the initial benefits derived from greater transparency. Consequently, recent improvements in this regard, represented for instance by Facebook's tool that allows users to view at any given time the ads run by any Facebook page[72] or Twitter's decision to establish an Ads Transparency Center,[73] are auspicious. Progress in these areas will make social media networks safer. CEE governments are hardly in a position to contribute directly to such an endeavor, but they should collectively push for such an approach at the EU

Figure 3. The Circle of Disinformation.



level. Dealing with social media platforms through the EU is more likely to have a significant impact and might yield far more beneficial results than by individual governments. A similar logic should be applied to potential regulation of platforms. Instead of having numerous varying regulations on a state-by-state basis, regulating platforms at the EU level is far more likely to be effective.

Another strong argument in favor of greater transparency is that this makes it easier for the private sector to become more involved in combating information warfare and disinformation campaigns. Governments should strive to create as conducive an environment for private companies as possible and to incentivize their participation. Relying solely or predominantly on government-led initiatives and institutions will most likely only allow countries to be on par with Russia's information warfare capabilities. Instead of mirroring the Russian approach—which is essentially based on utilizing purely government or government-affiliated institutions—Western countries including the CEE ones should use the potential in the private sector. Being home to the leading information technology-oriented companies, the Euro-Atlantic private sector could

71 Elina Lange Ionatamishvili, interview.

72 Jordan Julian, "4 Reasons Why Facebook's New Ad Transparency Tools are Good for Marketers," SocialMediaToday, July 19, 2018.

73 "Ads Transparency Center," Twitter.

contribute considerably to building effective information warfare capacities and anti-disinformation instruments. As the potential of the Western private sector in this area far exceeds that of the one in Russia, capitalizing on this advantage should be pursued more dynamically.

First steps in this direction have been taken. In 2018 it was announced that the cyber-security giant FireEye considerably contributed to the efforts by Google, Twitter, and Facebook in combatting disinformation and election interference.[74] Other significant cyber and Internet security companies, such as Palo Alto Networks or CloudFlare, are likewise well suited for tackling misleading information online. CEE countries should therefore try to include and incentivize local companies, especially those involved in cybersecurity, such as local giants Avast Software or ESET, into developing their own capacities in this segment of information security. Furthermore, building private-public partnerships for the purpose of identifying and

> *"It is very difficult to determine the exact share of a population caught within the rather vaguely defined echo chambers across CEE societies.*

eliminating emerging information-warfare threats could become increasingly important. New technologies—for example, "deep fake" audio and video doctoring—are bound to make the differentiation between "fake news" and genuine reporting increasingly difficult.[75] Hence, CEE governments should reach out to local private companies to include them in establishing effective countermeasures.

Finally, greater transparency for social media platforms has another advantage in that it could contribute considerably to disrupting online "echo chambers," which have been often described as one of the key factors in the dissemination of misleading information.[76]

Echo Chambers and Media Disenfranchisement

Apart from the general trends that affect CEE's societies as a whole, there also are marginal population segments—found in so-called echo chambers—that are considerably more vulnerable to disinformation campaigns. A scenario where an individual is exposed to misleading news and disinformation on numerous levels while simultaneously perceiving mainstream media as biased is possibly the most conducive for information warfare exploitation. Furthermore, this does not typically trigger any suspicion, because according to the theory of echo chambers, people are intrinsically driven to ideas and views congruent with their own.[77]

Based upon the different types of news and information sources an average individual routinely uses it can be inferred that the "circle of disinformation" (see Figure 3) is complete when disinformation or misleading news penetrate person's interaction with friends and family, with media channels (typically represented by alternative media), with social media groups, and with political elites (having a public/political figure or a political party to follow that openly and publicly corroborates misleading narratives/perceptions). Finally, for most effectiveness the individual should also demonstrate a strong inclination for increased or very high distrust in the mainstream media.

It is very difficult to determine the exact share of a population caught within the rather vaguely defined echo chambers across CEE societies—partly as a result of this it remains difficult to determine actual impact that echo chambers might have on a wider population. Although social media echo chambers are frequently described as the crucial tool for spreading disinformation by creating filter bubbles, research highlights that evidence to support this is often lacking or is considerably flawed, especially because numerous related theories are not

74 Mae Anderson, "FireEye: Tech firms' secret weapon against disinformation," Apnews, August 24, 2018.

75 Jamie Fly et al., "The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies," German Marshall Fund of the United States, June 26, 2018.

76 David Robert Grimes, "Echo chambers are dangerous—we must try to break free of our online bubbles," Guardian, December 4, 2017.

77 Andrew Guess, et al., Avoiding The Echo Chamber About Echo Chambers: Why Selective Exposure To Like-Minded Political News Is Less Prevalent Than You Think, Knight Foundation.

examined in a realistic context of a multiple-media environment.[78] Studies also often point to only modest impacts of echo chambers, stressing that although social networks contribute to an increasing ideological distance between individuals, the very same channels increase users' exposure to materials from their less-favored side of the political spectrum.[79] Such conclusions challenge the perception that social networks inadvertently create echo chambers with far-reaching consequences for a society as a whole.

> *"The CEE governments should therefore strive to deliver their media literacy projects and initiatives supporting local journalism predominantly to the least-developed areas and socially excluded communities throughout the region.*

Nonetheless echo chambers, whether representing a critical or only a marginal threat, do exist and they should be tackled in order to diminish their potential impacts. The CEE governments should focus on maintaining this phenomenon at bay, instead of striving to eliminate it—which might be an impossible task. Implementing measures that would prevent individuals from falling into the trap of media disenfranchisement, and thus entering and being locked in a various echo chambers through social media groups, should be the primary concern. Although a certain segment (of an unknown size) of the CEE population could be viewed as trapped within pro-Kremlin echo chambers, the most effective instrument for combatting this phenomenon is by preventing others from falling into them as well, instead of trying to dissuade those already in them.[80] Therefore, first and foremost, the CEE governments need to make sure that an openness and accessibility to wide range of media channels is preserved so that social media do not become the only provider of an individual's daily news.

The CEE governments should therefore strive to deliver their media literacy projects and initiatives supporting local journalism predominantly to the least-developed areas and socially excluded communities throughout the region. These are most likely to face media disenfranchisement and are thus more vulnerable to disinformation campaigns.[81] Projects established on a countrywide basis would ineluctably be inclined to favor capital cities and richer regions that, due to their already well established academia and think-tank structures, answer such proposals more effectively than their counterparts in socioeconomically disadvantaged regions.

Simultaneously, as indicated above, increased transparency on social media platforms might also considerably contribute to effective disruptions of local echo chambers. For instance, more transparency and insight into the systems of social media algorithms used for selecting the type of content that appears on individual user's interface could contribute to the ongoing debate on information warfare countermeasures. This is particularly true as the most recent algorithms have typically prioritized content that engages users without regard for its accuracy or any indication of its truthfulness. Likewise, optimizing such algorithms solely for engagement inadvertently fosters polarization and can empower "mobocracy," thus also creating a conducive environment for echo chambers.[82] Such a reason, in addition to the wave of recent criticism, led Facebook in 2018 to introduce new algorithms ostensibly emphasizing "meaningful interactions" while striving to eliminate or minimize harmful content—a task in which the company cooperated with academics.[83]

78 Elizabeth Dubois, and Grant Blank, "The echo chamber is overstated: the moderating effect of political interest and diverse media," Information, Communication & Society, 21:5, January 11, 2018.

79 Seth Flaxman, et al., "Filter Bubbles, Echo Chambers, and Online News Consumption," Public Opinion Quarterly, 80:S1, March 22, 2016.

80 Jakub Kalenský, interview.

81 Peter Jančárik et al., Countering Pro-Russian Disinformation: Current Challenges And The Way Forward, Prague Security Studies Institute, May 31, 2016.

82 Wael Ghonim, and Jake Rashbass, "Transparency: What's Gone Wrong with Social Media and What Can We Do About It?" Medium, March 27, 2018.

83 Mike Isaac, "Facebook Overhauls News Feed to Focus on What Friends and Family Share," New York Times, January 11, 2018.

Such an approach could considerably curb the role echo chambers play in disseminating disinformation. Pushing for far more transparency in terms of how algorithms are designed could prove to be a powerful tool for disrupting echo chambers and societal polarization linked to them.

Conclusion

Russia's information warfare is here to stay. It cannot be fully eliminated, but it can be very effectively kept at bay, making sure that its effects on CEE societies remain marginal. Information warfare operates in a fast-paced and quickly changing environment. Partly as a result, it is more opportunistic than strategic. Effective countermeasures, especially those applied in the CEE region, must reflect this reality by being highly adaptable and agile—a factor that local anti-information-warfare capacities often lack. The dynamism of Russia's information warfare is illustrated by the fact that over the last decade at least two strategic shifts can be identified in it—after the Russian-Georgian war in 2008 and then in 2014 when Russia went from being risk-averse and stealthy to increasingly aggressive and risk-taking. It is very likely that information warfare will remain dominated by dynamism and ever-changing tactical shifts. The inability to develop capacities to operate effectively in such an environment could have considerable negative implications.

The CEE region represents a very unique space within the Euro-Atlantic area. Particularly because of its countries' several historical, linguistic, or ethnic ties to Russia, the narratives that are being circulated there often differ considerably from those observed in Western Europe or North America. As a result, the CEE region can be perceived as intrinsically more vulnerable to disinformation campaigns, especially because of the wider range of narratives that Russia can exploit there for such a purpose, including the Russian World, Slavic Unity or Ostalgia narratives. Simultaneously, the CEE region faces numerous deleterious trends that are favorable to Russian information warfare tactics. Most evident has been a continuous decline in citizens' trust in traditional media platforms, which are the least likely to be polluted with disinformation and misinformation. The inherent risks in such a trend have been exacerbated by increasing trust in online media platforms and reliance on social media networks for news, both of which are far more susceptible to disinformation and misinformation.

Russia's information warfare works through a process that can be described as an amplification pyramid that eventually transforms initial disinformation (information known to be false and spread deliberately) into misinformation (information not known to be false and spread unwittingly). The CEE trends epitomized by higher reliance on social media and online portals considerably increase the chance for the amplification process to succeed. Information warfare also thrives in an environment of opacity. The fact that numerous CEE government structures often still carry a pre-1989 legacy or a relative lack of transparency only makes the region exceedingly vulnerable. Ultimately, the CEE region is less resilient to information warfare not only due to weaknesses in civil society, media, and political structures—the mantra of dozens of reports and policy papers—but also because of the relatively high number of narrative categories that can be exploited there and the several negative trends currently witnessed in CEE societies.

> *"It is very likely that information warfare will remain dominated by dynamism and ever-changing tactical shifts.*

Nonetheless, there are also positives. Concerns about the effect of Russia's information warfare capabilities are vastly exaggerated. Disinformation campaigns have an impact, often particularly evident during periods of societal tensions. Nevertheless, once such a period subsides their effects begin to fade away relatively quickly. Likewise, Russia's information warfare has so far proved unable to change the geopolitical orientation of targeted societies in the region as once feared, especially during the European migrant crisis in 2015–2016. It has been capable, however, to exacerbate and capitalize on

ongoing societal tensions, yet without having an ability to create or sustain them over a longer period. Such short-term success validates previous claims that Russia's information warfare is inherently opportunistic. Similarly, although echo chambers form a real problem that should be tackled, its actual scale and impact in the CEE countries still remains to be determined, as is the number of people actually "caught" within them.

When compared with the rest of the EU, CEE societies today face the paradox of demonstrating a very high awareness of the issue of disinformation and fake news while showing only moderate concern for the potential implications. At the same time, CEE societies often view the authorities as responsible for taking a lead in tackling disinformation. This is auspicious as it provides governments with maneuvering space for implementing necessary regulations or establishing appropriate institutions.

Social media platforms could further considerably aggravate the implications information warfare might have. This will be reinforced by the emerging field of computational propaganda, which allows for dissemination of individually optimized content on social networks. Similarly, rapidly expanding technologies such as "deep fake" video and audio doctoring are likely to further exacerbate the effects disinformation have through social media platforms. Therefore, the platforms still have unutilized potential for disinformation unlike some other channels, such as the disinformation portals that boomed in the CEE region particularly in 2015 but have become largely stagnant and unable to expand beyond their initial base.

There are several areas and approaches that CEE governments should follow in order to strengthen local information-warfare resilience. One of the key challenges for the Euro-Atlantic area in general and the CEE region in particular will be to escape from the circular and repetitive debates surrounding information warfare that repeat, often vaguely defined, recommendations such as improving critical thinking, strengthening civil society, and reforming education. Since information warfare operates in an environment built upon continuously novel approaches, avoiding such a loop is essential. There is also a significant lack of reliable and quantifiable data that would give more substance to the ongoing discussions and could play a considerable role in furthering the advancement of research.

One fact remains strikingly clear nonetheless: information warfare and disinformation are inevitable. Consequently, governments and societies in the CEE countries will ultimately have to learn to live with them.

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

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

www.gmfus.org