Information Warfare
and the Role of Non-Governmental Organisations

Visegrad Fund

FORUM 2000

Authors: Mário Nicolini, Jonáš Syrovátka
Edited by Tomáš Bouška and Caitlin Triplett

Authors

Mário Nicolini has long been committed to inspiring and empowering the next generation of young leaders, including through his work as Founder and Honorary President of the Euro-Atlantic Center, Editor-in-Chief of Sebavedome.sk (Confident Slovakia), and Executive Director of the Forum of the World's Religions – Slovakia. During a decade of civil service, he advised two Ministers and six State Secretaries of Defence on strategic issues facing Slovakia as a NATO member, including troop deployments, defence transformation and public information. From 2008-2011, he served as Defence Counsellor at both NATO and the EU. Before joining the Ministry of Defence, he worked with the consulting company McGuireWoods LLP in Washington, DC.

Jonáš Syrovátka is a Project Coordinator at Prague Security Studies Institute, working primarily on projects concerning Russian influence activities in the Czech Republic. He leads the project „Czech election in the ear of disinformation" focused on the impact of disinformation on the elections.

The authors would like to thank Adam Lelonek, Lóránt Győri, Benedikt Vangeli, Jonathan Terra, Jakub Janda, Veronika Víchová, Daniel Milo, Katarína Klingová and Centre Against Terrorism and Hybrid Threats for their insights and contributions.

Summary

- Information warfare is not a new phenomenon but in recent years it developed rapidly due to the modern technologies
- Even though Russian hostile activities, in particular the spreading of disinformation to alter election results and undermine trust in democracy in the West, are the most notorius example of information warfare, it must not be forgotten that other non-democratic regimes and domestic actors apply similar techniques and network between themselves in pursuing like-minded policies
- Information warfare aims to influence not only military and political decision-making but also the civilian population at large; NGOs as key representatives of democratic societies are targeted routinely to alter public perceptions and manipulate popular will
- NGOs play various roles in information warfare – they may become Targets, Instruments or Defenders against information warfare
- NGOs should be aware about the serious threat that information warfare presents to civil society and their own existence; they should reflect it in their procedures and develop readiness to survive and recover from possible attacks
- NGOs should avoid being manipulated into becoming Instruments of information warfare and must be careful about reputation and public messaging
- NGOs are an essential ally for the state institutions in developing effective responses to information warfare, not only in security-related analysis, but also in other sectors, such as education, media literacy, or in strengthening democratic society in general
- The NGO community, while being a vital partner for government, presents no alternative to robust state engagement in countering hostile information warfare, which should be regarded as a national security threat
- Communication and collaboration among NGOs is essential in defending against information warfare
- NGOs from V4 countries have launched a range of successful projects detailed in this report with the aim of countering information warfare by foreign and domestic actors which should be seized upon both as a source of inspiration and as an object of assistance by allies and partners to counter this vital threat to democratic societies

Table of Contents

Introduction

The phenomenon of Information Warfare (IW) – sometimes described as disinformation, fake news, or propaganda – has gained significant attention and concern across Western countries in recent years. Events such as the Russian annexation of Crimea, Brexit, and Donald Trump's victory in the U.S. presidential election have shown that IW remains widely relevant and will not be an issue disappearing from the public space any time soon. It is an issue worth defining accurately and clearly as there can be a misunderstanding of its nature. One of the most important characteristics of IW is that it is not limited to military targets (even though the term 'warfare' could suggest otherwise). On the contrary IW is designed to infiltrate various targets including those separate from the state; one important target being non-governmental organizations. NGOs play two important roles in IW – both as victims and instruments of the hostile behavior.

Given the critical importance of this issue, the Forum 2000 Foundation dedicated an entire panel discussion, held during the 2018 NGO Market in Prague, Czech Republic, to the role of NGOs in IW. The discussion hosted five experts from the V4 countries and the United States. The videotape of the panel is available on the Forum 2000 YouTube channel. This text is based on the main ideas and opinions that were stated during the panel discussion.

The following chapters elaborate on the complex role of NGOs in IW presented in three sections. Firstly, it describes the phenomenon of IW and explains its impact on democratic societies. Secondly, it highlights how NGOs might be affected by these phenomena and gives general recommendations on how it should be tackled. Thirdly, it shortly introduces the situation in the V4 countries and presents organizations, initiatives and projects that successfully confront this challenge.

The phenomenon of Information Warfare

The idea that the amount and accuracy of the available information is as important as military strength is not new. Classical war theorists such as Sun-Tzu, Thucydides and Carl von Clausewitz saw deception or lies as important instruments in the toolkit of military commanders.[1] They also noted that war (especially the components of IW) does not have to be contained to a fight between armies but can and should target the civilian population as well. The ability to break the spirit of an enemy by undermining them was deemed even more important (and more effective) than the ability to physically destroy them. Hence, we can see that the phenomenon of IW and its main goals are not original. However, we should be aware that because the information environment has changed so profoundly in the past several decades, the nature of the warfare has changed as well. It is important to carefully examine the new techniques applied by actors waging conflict in the information space.

The change of the information environment – specifically its democratization brought about by the internet and social media – has also changed the nature of the involved actors. The weakening of information gatekeepers (such as traditional media or governments) has created a space that is vulnerable to the spread of specific messages by less influential, loosely organized, non-state actors. For example, these internet spaces can serve terrorist groups (like ISIS) in spreading (often violent) propaganda that reach, motivate and mobilize supporters across the globe and demoralize opponents.[2]

The democratization of the information space has also contributed to the increase in the unmonitored messages that flow through it. Thus, it has become easier for actors to disseminate a variety of false or partly false information that can undermine and manipulate the truthful narrative or interpretation of occurring events. Since the beginning of the Ukrainian crisis in 2013, Russia has been perceived as the main actor using these techniques. The shooting down of flight MH17 in Eastern Ukraine by pro-Russian separatists in 2014, accompanied by the spread of numerous contradicting theories aiming to undermine the official version of the story, can serve as an illustrative example of Russian propaganda campaigns.[3] This technique was repeated recently after the attempted poisoning of ex-GRU officer Sergei Skripal as tens of theories appeared describing who may be responsible for the killing.[4] Instead of simply sowing lies and denial, as it was in these other cases, Russian state and non-state actors have begun to exploit history, culture, language, nationalism, disaffection and more to carry out cyber-enhanced disinformation campaigns with much wider objectives. These objectives have appeared to include destabilizing and disrupting Western societies, undermining the notion of truth and discouraging rational discussion.

[1] More on these can be read in classical pieces like "Art of War" (Sun Tzu),"History of Peloponessian War" (Thucydides) or "Theory of War" (Carl von Clausewitz).

[2] More about this subject can be found for example in the book "Information War" by Karel Řehka

[3] More on this case may be found in analysis from Bellingcat or East Stracom (EU unit countering disinformation)

[4] More on the reporting about the Skripal case can be found in reports of East Stratcom or about the reporting on this issue in the Czech media space in the blog written by the author

This shows Russia's preference for spreading anti-narratives that destabilize and disrupt Western societies, rather than simply promoting its own positive message to establish its superiority.[5]

The techniques of IW are not exclusive to Russian and other outside authoritarian regimes but are also utilized by domestic anti-democratic forces. Recent years have seen a surge of popular support for political parties and politically motivated actors who have employed techniques similar to outside forces. Some have received assistance from Moscow, drawing on a toxic mix of instruments deployed by Putin's Russia. This includes the media, NGOs, politicians, academics, financial market agents, energy executives and their corrupt spin-offs, ethnic and regional activists and hackers. Indeed, the IW waged by the Kremlin against the West would not be effective without the support of local actors with interests either in regime change (i.e. the replacement of democracy by authoritarian rule) or in destabilization and chaos, colluding with the Russian Federation.

The challenge in identifying actors and their motivations makes it difficult to respond to IW in democratic societies, which are, by definition, pluralistic and inclusive of dissenting voices. In defending ourselves against IW, we must take extra care not to erode our democracies, thus furthering the goals of those who wish to undermine them. The very use of the term war might have undesirable consequences as it may give the impression of serious and likely violent tensions in society. The simplistic division of the "allies" and "enemies" may effectively silence the debate about certain issues not only among the general public, but also in the expert community. Securitization is even further complicated when we acknowledge that the spreading of disinformation and anti-democratic narratives fuels the very real and valid frustrations of citizens caused by social problems and the dysfunction of state institutions. Any attempt to shut down all critical and non-mainstream voices might lead to the debilitation of a very fundamental value of democratic society – the plurality of opinions. Much needed focus is then placed in merely ameliorating one of the many consequences rather than addressing the very root of the issue. In the worst case, labels such as disinformation or hybrid threat may be misused by politicians to suppress their political opponents, media or NGOs, as is already the case in authoritarian regimes. Therefore, we should be cautious while using the term IW. [6]

NGOs and Information Warfare

As it was pointed out in the previous chapter, IW is not limited to the military sphere but expands in targeting the civilian population. NGOs, serving as the most visible and vulnerable representatives of civil society, are a very tempting target for non-democratic actors. Since NGOs rely heavily on moral authority, reputation and the notion of credibility and competence, the dissemination of negative information about them can have a serious impact on their work and even existence. On the other hand, increased securitization of IW threats can serve negatively for NGOs as they might fall more subordinate to the power of the state (e. g. by codification of laws that labels them as agents of foreign states). For this reason, the NGO community should dedicate serious attention to IW, stand up in defense of the liberal democratic system that both allows and requires their existence as independent actors, take measures preventing possible negative consequences from this phenomenon, and become active stakeholders in the debate about the ways to tackle this threat.

Before we look at the possible roles that NGOs can hold vis-á-vis the challenge of IW, it is worth saying a few words about their relation with the state. Since the state is the entity responsible for maintaining security on its territory, the main actions preventing IW should be taken by the state. But as was described, this threat is so diverse that it requires active collaboration between state institutions and other actors, including the NGO community. Therefore, all sides tshould seek open dialogue, the exchange of expertise, and other forms of cooperation. This close collaboration should be accompanied by an understanding of the different nature of the parties to avoid misunderstandings and unrealistic expectations.

[5] More on the nature of Russian IW can be read in pieces of distinguished researcher Mark Galeotti (lecture on fake news or his polemical piece on so called Gerasimov doctrine), blog of Professor Stephen Hutchings, article by journalist Edward Lucas or piece by journalist Peter Pomerantsev. Further recommended readings are listed in the Annex of the article

[6] More arguments pointing out to the challenges connected with (particularly with the Czech) debate about IW are raised by researchers Jan Daniel and Jakub Eberle

For the purposes of this text, NGOs are described in the three possible roles they may have in IW. The roles described below are of course only ideal types and might change over time. Additionally, we must note that an individual NGO can play more than one role at any given moment. The roles of NGOs are the following:

- Instruments of IW – this term refers to NGOs that actively (wittingly or unwittingly) participate in spreading products of IW (such as propaganda, disinformation, misinformation etc.)
- Targets of IW – this term refers to NGOs targeted by IW activities
- Defenders against IW – this term refers to NGOs actively involved in actions aiming to mitigate the damages caused by IW

This chapter describes each of these categories and provides a general recommendation for NGOs that might help not only to prevent the negative consequences of IW but also to restore faith in democracy and confidence in Western values.

NGOs as Instruments of Information Warfare

NGOs might be unknowingly involved in spreading propaganda, false messages or simply one-sided views on the happenings. This can occur due to their low ability of self-correcting and excessive commitment to promoting their own ideological standpoints. In some cases, NGOs can be created to serve as a tool of IW.

At this moment, it is timely to introduce the category of Government-Organised Non-Governmental Organisations (GONGOs). This term refers to organizations that are using the benefits of being perceived as an NGO (e. g. seen as voicing independent opinion, having genuine interest in perusing it cause etc.), but in fact serve as instruments for promoting the interests of their state sponsors or direct superiors. GONGOs are often involved in a number of "soft" (and at first sight legitimate) activities – like education, cultural exchanges, history etc. Although GONGOs might serve as agents of foreign states, it is important to note that even though their activities might be undesirable, the targeted democratic state cannot interfere until they conflict with legal norms or present a threat to national security.

To avoid becoming an instrument in IW, NGOs should implement the following measures:

- Take caution when establishing collaboration with GONGOs to avoid (or at least understand) the possible risks
- Be transparent about their goals and motivations
- When collaborating with or being financed by state institutions, follow a clear and transparent code of conduct that will allow them to maintain their credibility
- Be mindful and cautious in selecting sources of financing to avoid possible controversies
- Be careful about the message to avoid becoming a source of propaganda or falsehood (this applies not only to NGOs as such but also to their representatives and employees)
- Do not be afraid to criticize other NGOs when they become an Instrument of IW

NGOs as Targets of Information Warfare

NGOs represent the very essence of a free and pluralist society based on the merging of various interests. Therefore, it is not surprising that organizations such as these are the first to be attacked by domestic or foreign actors preferring authoritative models of society. These attacks might take various forms – public blaming for various negative events in society, for working against the interests of the state or nation, threatening, spreading disinformation, or even blackmailing. Verbal attacks might transform into (or be accompanied by) more serious forms of intimidation – hacking, lawsuits or physical attack.

To avoid becoming the target of IW or to mitigate the possible damages, NGOs should:

- Perform their tasks professionally and be transparent about their goals and financing
- Communicate their activities, build their brand and seek partnerships proactively to be able to mobilize support in the case of intimidation
- Take the possibility of information attack seriously and have crisis management procedures in place, understood and rehearsed by its employees and collaborators as appropriate
- Allocate a sufficient part of the budget to security-related issues
- Create a network of like-minded stake-holders (such as other NGOs) that will serve in exchanging the best practices, coordinating actions and mobilization in times of crisis
- Consult the possible risks associated with IW with state institutions
- Monitor the possible risks to be able to timely react to attacks
- When necessary, take legal steps to deter possible intruders from future attacks

NGOs as Defenders against Information Warfare

NGOs should play an important role in fighting IW, given that it represents a targeted assault on the very nature of the democratic political system, on social cohesion, and national identity at large. Therefore, any efforts to counter the phenomenon must involve actors far beyond the bubble of foreign policy and security experts. Unlike state institutions, NGOs are flexible, free in choosing their issue of interest and applying new methods, approaches, and communication styles. NGOs focused on security issues (such as think-tanks) may be helpful in the analysis of IW (especially if they collaborate with universities or foreign NGOs). Another important task might be fact-checking and the debunking of elements of disinformation and hostile narratives that appear in the public domain. Since NGOs naturally communicate with journalists, this might be a very effective technique – especially in times of sensitive events (such as elections). NGOs can also play an important role in public advocacy and closed-door lobbying about IW-related policies. This pressure should not be limited to politicians but include journalists and private companies (who might support disinformation by placing advertisements on controversial websites). NGOs that are involved in education are also vital partners in tackling IW as they work on media literacy among the population. Transparency is a key issue for NGO-defenders since they might easily lose their credibility while being perceived as instruments of state interest. Therefore, NGOs should communicate their work in ways understandable to both expert and general audiences, be clear about their goals and background, and stand ready to defend their work publicly. The ability to do so is vital for gaining and maintaining public trust, which is the NGO's most important asset.

In order to be a Defender against IW, NGOs should:

- Collaborate proactively with like-minded actors
- In research, be transparent and precise about their methods in producing valid and undeniable data to prove that they are not influenced by the interest of donors
- In debunking efforts, be quick, persuasive, and fun
- Always be prepared to discuss and defend their work
- Present themselves in ways understandable to both expert and general audiences
- Establish networks to boost morale and disseminate findings, experiences and best practices – not only among NGOs but also other actors such as journalists or academic researchers
- Engage in other activities that address broader reasons why IW may be successful – such as improving media literacy, promoting civic education, fighting corruption or other activities aimed to increase the level of dialogue and trust in democratic societies
- Lobby governments to become more active in building new channels of communication and cooperation with civil society, to implement them into a legal and institutional framework on the national level, and to devise new strategies for education, training, public-private information-sharing, and other relevant issues
- Seek close collaboration with the media, especially in neutralising the influence of the „alternative" media, using new technologies, cybersecurity, fact-checking, counteracting disinformation and propaganda, connecting new legal regulation with the issue of the freedom of speech, and defending civil society and politics from foreign hostile influence.

Case studies of V4 countries

Czech Republic

The Czech Republic is one of the leading countries countering Russian subversive influence; it understands the threat and actively reacts on the state level. Civil society in the Czech Republic is active and has succeeded in placing the topic on the public agenda. The position of the Czech Republic is undermined by its President, Miloš Zeman, who is considered one of Russia's most prominent allies in Europe.

Czech strategy documents are quite sophisticated in terms of their identification and description of Russian influence and disinformation operations. The 2016 National Security Audit presented specific recommendations for enhancing resilience, including the establishment of centres for the evaluation of disinformation campaigns within relevant authorities, the creation of a system of education for public officials to make them more resilient towards foreign influence, and active media strategies for important democratic institutions or measures concerning media law. The Centre against Terrorism and Hybrid Threats was established within the Czech Ministry of Interior to monitor internal security threats including disinformation campaigns, advise the government on threats in the information space, and publicly debunk disinformation about domestic issues using a dedicated Twitter account.

Since the annexation of Crimea, Czech civil society has been active in terms of tackling disinformation. Many non-governmental organizations have proven successful in monitoring disinformation circulated in the media space and in debunking fake reports. The biggest shortage of activities exists in the areas of security issues, journalism, and media literacy.

The European Values think-tank established Kremlin Watch, a highly visible program which regularly fact-checks news reports originating in pro-Kremlin media, produces larger studies and bi-weekly reports on disinformation trends and narratives spread in the Czech Republic, and convenes a conference for public communication and security professionals called the StratCom Summit. It also focuses on policy development and advocacy to motivate governments to take further steps towards tackling disinformation campaigns. Partnering with the private firm Semantic Visions, European Values presented a data-based study on how Russian propaganda media portray European leaders.

The Association for International Affairs launched a Czech version of the Ukrainian website StopFake.org, dedicated to verifying disinformation about the conflict in Ukraine. The Prague Security Studies Institute launched an initiative to raise awareness about pro-Russian disinformation; it publishes articles and reports on the topic and organizes events and debates for both experts and the public. People in Need produced educational material for teachers on Russian disinformation. Likewise, the Czech academic sphere has not remained behind. The Department of Political Science at the Faculty of Social Studies at Masaryk University in Brno analyses manipulation techniques and emotions used by pro-Kremlin disinformation sources and provides media literacy training. It also launched a student project called Zvolsi.info, which focuses on raising media literacy amongst Czech and Slovak high school students. Similarly, the student project stuzak.cz is a hub for humanities´ students presenting interactive workshops in secondary schools that focus on various socio-scientific disciplines. The aim, closely linked to media literacy, is to raise interest in civic-related themes among youth and to improve their level of socio-scientific education.

Hungary

NGOs in Hungary are particularly vulnerable to defamation because civic organizations are increasingly stigmatized by the government as being "liberal" or working "against the nation state" on human rights issues. Hungary's special case stems from the fact that civic actors have long been targeted by the illiberal government of Prime Minister Viktor Orbán for allegedly "aiding illegal migration" or being the "agents" of Hungarian-born American billionaire philanthropist George Soros, of Jewish origin, in his alleged effort to "alter the ethnic composition" of the country. Due to the lack of strong opposition parties, Orbán's successive governments have adopted the policy to go after Hungarian NGOs as they present some sort of an opinion forming capacity (illustrated by successful court cases against the government in corruption scandals), but most importantly, as they cannot, in any real way, compete politically with the ruling Fidesz-KDNP party. Consequently, Hungarian NGOs have received prime time in government-controlled media that have nurtured conspiracy theories about, for example, a "world government" set up by the "Soros NGOs."[7] Hungarian NGOs are attacked on geopolitical grounds as some sort of an international liberal conspiracy of the West

[7] The example from local press can be seen here

(or the United Nations) against the Hungarian government, posturing as a defender of a Christian "Fortress Hungary" against masses of Muslim migrants welcomed by Hungarian human rights organizations.

To fend off this putative threat, the Hungarian government adopted two rounds of measures: a bill on the transparency of organisations supported from abroad that need to register with the court and publish this fact on every public document they produce[8], and the "Stop Soros" package, a legislative proposal of three bills that target civil society organisations working on migration with similar or harsher measures. Both measures copy President Putin's legal offensive against those NGOs that criticize the government, citing national security interests to stigmatize, financially cripple or, in the most extreme cases, ban certain organizations.[9]

Academic work on disinformation and propaganda is limited to Political Capital Institute's studies on Russian influence and certain pieces of high-quality investigative journalism. Several Hungarian journalistic efforts have featured stories on how Russian propaganda outlets try to manipulate public opinion and point out the connections between the local and the Russian version of the same news article. The investigative portal atlatszo.hu managed to find out that the servers of several pro-Russian websites, such as szentkoronaradio.hu are operated from Russia. The portal vs.hu also includes information on why fringe portals have been created.

When pondering Hungary-specific approaches to countering the threat of IW, focus should be on embedding NGOs with society by creating a nationwide network and establishing pro-democratic rural counterparts against the right-wing extremists and populists. People need to develop personal experiences with NGOs who are mostly based in Budapest and depicted by the media in a negative fashion. Secondly, massive "folk-education" is needed to counterbalance the government's hatred campaigns while challenging the nationalistic and populist conceptions of national identity that are widely accepted and respected by the society. Rather than focusing on merely symbolic issues that divide, place emphasis on issues that connect people irrespective of their ideological stance. Thirdly, cooperation should be strengthened in the (1) civic movements, (2) civil society organisations and (3) citizens triangle; parts of the triangle are under pressure but not able to rely on the others.

Poland

The issue of information warfare is not new in Poland. Nevertheless, it is only the beginning of identifying, analysing, reacting, preventing or deterring the relevant threats, as well as developing strategies or building the legal and institutional mechanism on the state level. There is an ongoing process of securitization of certain spheres. The main focus of government authorities is on cybersecurity, not connected with the security of the Polish information space. The other important fact is the militarisation of the problem of both cybersecurity and information security. The main actor in those areas is the Ministry of Defence. This position, given to the military sector by the state, has some advantages. For instance, there are broader possibilities in dealing with deterrence and strengthening the security of the country in general. The MOD also has the largest capabilities in terms of preparing a more complex coordinated response to different security risks or hybrid threats. The drawbacks are, for example, limited information sharing with the public or NGOs, classifying different security-related processes, and thus narrowing the collaboration between the state and civil society.

A great challenge is the deficiency in the number of experts. On the civil market, there is only a few experts on information and psychological warfare. There are even less people in this group who have practical experience in Eastern Europe and/or know the East-European languages. Formally, there are four institutions which have at least one expert on information warfare: three of them are NGOs, of which two focus mainly on cybersecurity, and one is a Polish state think-tank. More NGOs organize events or publish materials about the issue, but usually involve external experts into domestic or international grant projects.

The other important participant in the internal Polish discourse about information war are media outlets and journalists individually. Their work and input, however, tends to have limited analytical or cognitive value. Their knowledge and experience is different from the analytical community. Their conceptual matrix is also full of oversimplification; for many of them the broad problem of foreign interference is limited to fake news. What is more, the journalistic environment is polarised either on the grounds of internal politics or on the level of ideology. Sometimes it is hard to tell with precision whether some journalists misuse important issues connected with the security of the Polish information space unintentionally, because they have too little knowledge and experience, or on purpose, as a tool to pursue political or other interests. Still, the work of many Polish journalists is invaluable in raising awareness about the threats.

Through its Information Warfare Initiative, the US-headquartered Centre for European Policy Analysis (CEPA) has analysed, rebutted and exposed Russian disinformation.

[8] The content of the law is explained here

[9] More about the law is possible to find here

The initiative includes, inter alia, a regular monitoring of country-specific applications of Russian disinformation content and techniques and an Information Warfare website centralizing data and analytical inputs on disinformation in the CEE region. Another think-tank involved in the analysis of IW is Center for Propaganda and Disinformation Analysis Foundation. Furthermore, Poland has several initiatives run by civic activists. The Russian fifth column in Poland, a Facebook page edited by blogger and translator Marcin Rey, reveals connections between people and organizations that spread propaganda or take concrete actions on a regular basis.

Slovakia

As of spring 2018, Slovakia, long thought to be an island of normalcy in a region descending into chaos, has gained a serious problem. With a government in clinical death, massive anti-corruption rallies, a divided opposition, a fascist party in parliament, extremism on the rise and serious doubts in the population about the country's geopolitical orientation, Russia has exploited Slovakia as NATO's weakest link. However, the country also has a serious asset: its vibrant NGO scene, carrying the message of the Velvet Revolution that sent Communism into the dustbin of history. It was the civic activists and the independent media, working with pro-democratic opposition parties, who defeated the authoritarian leader Vladimír Mečiar in 1998.

The Slovak model of countering propaganda by non-state actors already serves as an inspiration to other nations in Central Europe and beyond. This is arguably the only nation where a truly networked response has emerged. The effort involves individuals in and out of government, including NGOs, journalists, social media activists, bloggers, academics, cultural and interfaith activists, civil servants, politicians, and business representatives. The new Security Strategy of the Slovak Republic clearly identifies the threats of disinformation and propaganda, the need for strategic communication across all branches of government, and the imperative of working with civil society. The government is committed to developing a "comprehensive program of training and education" focused on democratic citizenship, the prevention of extremism, intolerance and xenophobia, social inclusion, critical thinking, patriotism, democratic values, and defense awareness. A concept on countering hybrid warfare has been drafted, detailing the measures to be taken.

Notable efforts, from public discussions to scientific research to media engagement, are conducted by the GLOBSEC Policy Institute, the Slovak Security Policy Institute, the Institute for Public Affairs, the Slovak Foreign Policy Association, STRATPOL, the Euro-Atlantic Center, the Centre for European and North Atlantic Affairs and many others, including media outlets such as Denník N, SME, Pravda, and týždeň. The work of these and other institutions, informal groups, and empowered individuals is complemented with collaborations venturing far beyond the bubble of foreign policy and national security professionals.

Drawing on previous work by the Central European Policy Institute, the GLOBSEC Policy Institute's Strategic Communication Program has produced, inter alia, opinion polls under the title GLOBSEC Trends and the Vulnerability Index on subversive Russian influence in Central Europe covering the four Visegrad nations. Media and Disinformation is the first online course on disinformation and media literacy in the region, produced jointly by GLOBSEC, the Central European University and the Faculty of Political Science and International Relations of University of Matej Bel. Countering Disinformation Online is a tool for civil society organisations, active citizens and any curious individuals who want to know more about helping free societies from the pressure of disinformation and false news.

Konspiratori.sk is a periodically updated list of conspiracy outlets which has moved 1400 Slovak companies to remove their advertisements from disinformation outlets. Conceived originally as a list of conspiracy websites by teacher and activist Juraj Smatana, the project now includes the Bullshit Detector, a downloadable plugin for Google Chrome that alerts readers to suspicious websites. Blbec.online aggregates and analyzes publicly accessible data from Facebook and provides updates on the trending statuses and commentaries from 800 pages by "Nazis, Communists, conspirators and other losers", allowing other individuals and projects to engage on this content. Facebook-based platforms include #somtu, a collective of Facebook users determined to "re-civilize" the social network by providing counternarratives based on universal values, as well as the hugely popular pages Prečo ľuďom hrabe? (Why Are People Nuts?) and Zomri (Keep Calm and Die), making fun of idiotic behavior in general and extremist rhetoric in particular. Dezinformácie Hoaxy Propaganda has focused on debunking pro-Russian and right-wing disinformation while also providing counternarratives.

While much remains to be done both in terms of quality and quantity, mainstream media have contributed to countering hostile narratives. Bolstered by successful crowdfunding campaigns, Denník N has produced three manuals for students and teachers on Facebook lies and conspiracies, critical thinking, and the functioning of the media. To illustrate the extent of the effort, the first of these manuals reached 40,000 students at 350 high schools. The blog section of Denník

N also includes Dezinformácie Hoaxy Propaganda. SME has used its strong online presence to debunk hoax stories on a continuous basis. Aktuality.sk, a top online media outlet, has featured a column with the best content culled from the Prečo ľuďom hrabe? project. Such efforts illustrate how social media and traditional media can complement each other.

Sebavedomé Slovensko (Confident Slovakia), a discussion platform for the youth, has produced thought-inspiring content in attractive formats (patriotic comic strips, vlogs, and infographics), encouraged discussion on critical issues affecting Slovakia's future, and mobilized the young generation around a modern concept of patriotism. Antipropaganda.sk, a portal maintained by the Slovak Security Policy Institute, has focused mainly on mapping and debunking hostile propaganda and developing counternarratives. In addition to daily output, the portal includes a timeline aggregating relevant news from around the world.

V4-at-large

Given the political and cultural proximity of the region, NGOs from the V4 nations have a history of coming together to work on international projects. Facilitated by donors seeking to fund projects with a regional scope, these collaborations have extended into information warfare-related efforts. Some of these have been listed in the national sections, ranging from full-fledged partnering to regular or ad hoc collaboration.

The Beacon Project's ICT data collection tool, >versus<, which is now localized in the four V4 languages, has been developed by the International Republican Institute to aid local media monitors and researchers to obtain qualitative and quantitative data from a wider range of sources. This data is further supported by national polling initiatives, which include IRI's own surveys, and shared through international conferences, media briefings and other public activities in the region and across the transatlantic area. Working with the Globsec Policy Institute, Political Capital Institute and European Values, IRI's Beacon Project showed the use of hyperbolic, disingenuous, uninformative and fear-stoking language in the coverage of Angela Merkel in some CEE media.

Demagog (in Slovak and Czech mutations) has been a valued fact checker of political discussions; a unique resource for journalists, think tanks and policy wonks since 2010. The collective has also shared its know-how with high school students and partnered within the V4 on projects such as Closer to V4 Policy.

VSquare is an independent, cross-border journalism initiative dedicated to improving the quality of investigative reporting and independent press in the Visegrad Region. It brings together the Reporters Foundation (PL), the Czech Centre for Investigative Journalism, Atlatszo (HU) and Mono.sk.

Conclusion

The threat of IW for NGOs is not easy to describe due to its fluid nature. It manifests itself in a number of ways depending on the actors, topics, techniques, or environments in which it appears. As the previous chapters suggest, the differences are present even among the individual V4 countries. Due to the fuzzy character of IW, NGOs may be targeted or involved even without their knowledge.

Therefore, this topic deserves continued attention, discussion, and applicable measures that will improve the resilience of NGOs. First and foremost, it is important to acknowledge this threat, and reflect upon the procedures of individual organizations to address it. By doing so, they will be able to mitigate the damage of possible attacks. NGOs should also pay close attention to the fact that they can be manipulated in order to become the instrument of IW and take care when choosing their partners or selecting information that will be used for various purposes. NGOs also are an important (even indispensable) ally of the state institutions while tackling this challenge, not only in security related analysis, but also in other sectors such as in education, improving media literacy, or the strengthening of democratic society in general.

The work of NGOs from all V4 countries provides numerous examples of successful projects that are trying to react to the challenge of IW. The measures adapted in particular countries provide examples worth following and imitating in the other states. Among the named projects, those that stood out were realized by NGOs from various collaborating countries. This leads to the final, crucial point: the successful countering of IW lies in the ability to create cross-border networks of various NGO actors. This flexible network is able to provide warnings, expertise and competencies needed at the time, and accumulate innovative ideas for future projects. Because—as with many other challenges—a group is always more resilient than an individual organization in combating complex issues such as Information Warfare.

Annex

Recommended readings on IW

- "Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe"
  http://cepa.org/reports/winning-the-Information-War
- "The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe"
  https://www.csis.org/analysis/kremlin-playbook
- "Russian Propaganda: ‚The Weaponization of Information'"
  https://www.voanews.com/a/russian-propaganda-weaponization-information/3036087.html
- "Russia's information war in Central Europe: New trends and counter-measures"
  https://www.globsec.org/publications/russias-information-war-central-europe-new-trends-counter-measures/
- "Combating Misinformation: An Ecosystem in Co-creation"
  http://ica-it.org/images/publications/Combating-misinformation.pdf
- "Handbook of Russian Information Warfare"
  http://www.ndc.nato.int/news/news.php?icode=995

EU documents about IW

- "MEPs sound alarm on anti-EU propaganda from Russia and Islamist terrorist groups"
  http://www.europarl.europa.eu/news/en/press-room/20161118IPR51718/meps-sound-alarm-on-anti-eu-propaganda-from-russia-and-islamist-terrorist-groups
- "Understanding propaganda and disinformation"
  http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2015)571332
- "Final report of the High Level Expert Group on Fake News and Online Disinformation"
  https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation
- Communication „Tackling online disinformation: a European approach"
  https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach

Others

- "Advice from Journalists and NGOs: How to lessen the impact of disinformation"
  https://www.globsec.org/advice-journalists-ngos-lessen-impact-disinformation/
- Book "Média, lži a příliš rychlý mozek" by Petr Nutil (CZ)
- Book "Průmysl lži" by Alexandra Alvarová (CZ)
- Website "EU vs Dezinfo"
  https://euvsdisinfo.eu/