Countering Information War

Lessons Learned from NATO and Partner Countries

Recommendations and Conclusions

GLOBSEC POLICY INSTITUTE

NATO OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

Credits

Globsec Policy Institute, Klariská 14, Bratislava, Slovakia
www.globsec.org

GLOBSEC Policy Institute (formerly the Central European Policy Institute) carries out research, analytical and communication activities related to impact of strategic communication and propaganda aimed at changing the perception and attitudes of the general population in Central European countries.

Authors:
Daniel Milo, Senior Research Fellow, GLOBSEC Policy Institute
Katarína Klingová, Research Fellow, GLOBSEC Policy Institute

Layout:
Peter Mandík, GLOBSEC

This publication received funding from the NATO Science for Peace and Security Programme.

Executive Summary

„Russia is waging the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare.“

Gen. Philip Breedlove, NATO Wales summit, September 2014.

In 2013, General Valery Gerasimov published an article, now know famously as “Gerasimov’s Doctrine”, which defined information warfare as the combination of electronic warfare, cyberwarfare and psychological operations into a single, coordinated military effort. Information warfare, however, is not new and various forms of psychological operations and propaganda have been a part for warfare for ages. What is new is our increasing reliance on the information sphere in every aspect of our lives, which is making us even more susceptible to such tactics.

Russia, aiming to restore its regional supremacy and weaken the EU and NATO, has been successfully exploiting this weakness with a robust campaign of information warfare. Russia’s disinformation activities are in compliance with its diplomatic activities, energy and economic policies, and support for mainstream and fringe political forces who are sympathetic to the Russian narrative.

Countries not integrated into the Euro-Atlantic political and military structures such as Georgia, Moldova or Ukraine, have been exposed to these subversive activities for years, while other NATO member countries, such as Czech Republic, Slovakia or Hungary, were caught unaware and unprepared for this new form of warfare.

The 2008 war in Georgia was a warning of things to come. Since the outbreak of the Ukraine crisis, information war, as an integral part of hybrid warfare, has been employed by Russia in its neighbourhood as well as in many NATO member and partner countries. It took different forms, and the tactics varied in each country, but the overall pattern was always the same: to confuse, distort, dismay, distract, and ultimately antagonise population to the euro-Atlantic orientation of the given country.

Information war`s ultimate goal is to inflict damage to the West`s core institutions – NATO and the EU. To that end, it employs various techniques such as disinformation campaigns, political and economic espionage, strategic corruption, automated systems and bots, and traditional and social media channels. Information warfare operations are modified according to the country`s specific political constellation, location, historic heritage, linguistic proximity and vulnerabilities.

Important element of successful information warfare operations is the tailoring of the content and narrative to match the vulnerabilities of a given population. Therefore, Russian information warfare efforts are characteristic by not using a single narrative, rather they employ a variety of narratives and local proxies to make sure the content resonates with the target audience.

In order to stimulate exchange of knowledge, lessons learnt and to identify promising practices in addressing and countering information war, GLOBSEC Policy Institute organised Advanced Research Workshops in Tbilisi on 27-28 September 2016 and in Bratislava on 28-29 November 2016. Both workshops were kindly supported by NATO-SPS programme and organised in partnership with Information Centre on NATO and EU in Tbilisi. They attracted more than 100 participants from 15 counties and produced a number of relevant **recommendations** reflecting different aspects of information war:

I. Recommendations for NATO and its institutions

1.1. Develop common terminology
1.2. Create and implement emotionally positive, pro-democratic narratives
1.3. Develop "new" playbook for NATO and Western countries
1.4. Strengthen communication efforts in NATO candidate countries
1.5. Enhance NATO's capacities to analyse and counter information war

II. Recommendations for national governments

2.1. Officially acknowledge the impact of foreign subversive efforts
2.2. Adopt whole-of-government approach to countering information war
2.3. Set up dedicated national StratCom capacities
2.4. Re-build trust and the credibility of institutions
2.5. Enhance research and monitoring of information war and its techniques
2.6. Support debunking and fact checking
2.7. Develop protection mechanisms for the victims of trolling
2.8. Strengthen the democratic immune system
2.9. Support training for media professionals and journalists
2.10. Ensure transparent media ownership
2.11. Close the democratic gap and reach out to audience and voters

III. Recommendations for other actors: NGOs, media and private sector

3.1. Increase the role of IT companies in countering disinformation
3.2. Support study of digital culture and social media
3.3. Build network of actors countering disinformation
3.4. Develop new subscription based models for traditional media
3.5. Set up an independent fund for investigative journalism

I. Recommendations for NATO and its Institutions

1.1. Develop common terminology

Development of common terminology and concepts of information warfare are a must. All actors, whether international or domestic, should have a clear and common understanding of the terminology used - what constitutes strategic communication, what is propaganda and how it differs from disinformation, which elements comprise information warfare, and what countermeasures need to be applied.

1.2. Create and implement emotionally positive, pro-democratic narratives

Since propaganda is essentially a fight for the hearts and minds of citizens, there is an urgent need for creating a credible, coherent and emotional narrative explaining our democratic values and fundamental principles. During these times of post-factual democracy and filters creating information bubbles, the old narrative of economic prosperity, freedom and moral superiority is no longer effective. The West needs to step up efforts aimed at developing an easily understandable, appealing and engaging narrative. Such a narrative should inspire citizens to stand up for these values, raise the flag of democracy and reject attempts to replace it with autocracy. Similar to the narrative of our opponents, this positive narrative should be tailored in each country to reflect its history, values, culture and sources of pride and patriotism. Once fully developed, it should then be used consistently in all communication efforts by NATO, its bodies, member states and their governmental structures.

> ***"Putin is trying to establish himself as Che Guevara of the anti-establishment."***

The rise of populism and extremism in Europe as well as in North America, show that citizens are growing distant from the democratic values and beliefs NATO represents. People have short-term historical memories and take the benefits of democratic society for granted. However, democracy is not a given. Democracy is not a stage that is reached but rather a continuous process to be defended, reaffirmed and explained to people. Therefore, the European Union and NATO need to employ skilled PR agencies, which should develop better communication strategies for explaining their principles, stories and achievements.

1.3. Develop "new" playbook for NATO and Western countries – Better dissemination of our stories and narratives / Re-branding of the West

The European Union and NATO need to explain their values and the principles to other countries better. While NATO abandoned its Cold War communication procedures, its opponents did not. The Russian Federation employs its information confrontation tactics both during warfare as well as during peace. In the case of Ukraine, it was possible to observe that the Russian Federation started to spread hostile disinformation targeted against Ukraine two years prior to the

annexation of Crimea and eruption of hostilities in Eastern Ukraine. A similar technique of hybrid warfare is applied by China, which understands the world as an information confrontation on three levels – psychological, media and legal. Therefore, the West, with its open communication and transparency, lags behind the Russian Federation and China in their perception of how warfare is conducted. These countries view the world as information confrontation. Storytelling and narratives are crucial factors of information war. Military strategies and narratives are interlinked. It is impossible to win an information confrontation and hybrid war only with facts. While NATO's principles are based on open communication, fact-based argumentation and transparency, Russia does not abide by such rules and pursues information confrontation based on lies and fake news. In the post-factual world Russia is great at telling stories that capture the hearts and minds of ordinary people and beat NATO's data and argumentation. Russian propaganda is also very effective in spinning stories, targeting specific audience and capturing public's attention.

> ***"We need to bring back our cool factor."***

It is possible to observe the clash of narratives between that of the Russian Federation and of NATO. Therefore, NATO needs to rebrand itself. It must take initiative and re-develop its value-based narratives. The West needs to learn what makes people "tick" and employ narratives that resonate. Debunking disinformation is important, but it needs to go hand in hand with the creation of our own strong narratives.

> ***"Propaganda effects are similar to cooking a frog - heating up the water until it is too late to react. We need to wake up and jump out of the water."***

1.4. Strengthen communication efforts in NATO candidate countries

The European Union and NATO should enhance their communication strategies and efforts to spread their narratives in the Balkan and Eastern European countries. It seems that the magnetic power of these organizations is lost and people in these regions do not understand the benefits and privileges of being a member. If citizens of candidate countries do not clearly know what these supranational organizations stand for anymore, then the European Union and NATO have lost their normative power. The European Union has been a unique civilian power, pursuing a communicative normative universalism, as well as human security, while NATO has provided hard security to its members. These Western organizations have transformed various regions through the focus on peace-building and good governance and stabilized Eastern European countries through benchmarking and reform processes. These narratives and achievements need to be refreshed and rejuvenated.

1.5. Enhance NATO's capacities to analyse and counter information war

NATO should apply lessons learnt from the Cold War and enhance both its analytical and public diplomacy capacities and activities pertaining to information war. The existing structures such as

NATO STRATCOM CoE and the StratCom team at SHAPE should be further strengthened. Pooling resources and expertise from across NATO could be decisive in turning back the tide in information war. Individual countries cannot resist the pressure of subversive efforts of regional powers alone. A combination of resources and capabilities at the international level coupled with dedicatedfunding for such efforts would be required to repel and counter concentrated info war attacks.

II. Recommendations for National Governments

2.1. Officially acknowledge the existence and impact of foreign propaganda efforts

Official recognition that propaganda and the impact of hostile foreign influence pose a threat to domestic democratic processes, and the society as a whole, is a first step towards developing a comprehensive response to information war. Recognition by state authorities and international institutions is paramount for raising awareness among decision makers and the general public of the dangers posed by information war and its actors. NATO should make its findings regarding the nature, scope and means used in information war by foreign actors, accessible to national authorities. At a national level, the intelligence services, Ministry of Interior and Ministry of Defence should publicly state the nature and aims of the current efforts by Russia, China and other hostile foreign actors and the methods and tools they use to destabilise individual countries and the whole Euro-Atlantic security architecture.

2.2. Adopt whole-of-government approach to countering information war

Subversive efforts of undemocratic actors are particularly effective due to the fact they skilfully combine activities and impact of various actors – media, intelligence, cyber operations, strategic corruption, diplomacy, energy and economic pressure. As such, they should be confronted with the same response – a coordinated, integrated whole-of-government approach. Relying on isolated measures implemented by individual agencies and institutions is no longer enough. In order to achieve such a coordinated approach, national coordinating structures should be established. Examples of such structures exist in several NATO countries (the Czech Republic, Latvia) and they prove to be very effective in addressing information war efforts in a comprehensive manner.

> ***"Russia's influence in CEE works like a microwave - heating up water molecules inside the meat (these countries) that are home-grown for their purposes."***

2.3. Set up dedicated national StratCom capacities

Every country should develop dedicated strategic communication capacities and policies. Strategic communication should be an integral part of national security strategies and structures. Interdisciplinary and inter-ministerial cooperation involving strategic leaders is necessary. NATO member countries should establish specific capacities that would focus on strategic

communication and countering disinformation on the domestic and foreign policy levels. These could be further enhanced if need be. Individual states should have the necessary capacities to provide countermeasures against foreign hostile influence. While international organizations such as NATO or the European Union should provide guidance, complete reliance on their hybrid war countermeasures, and the belief that these supranational organizations are going to solve everything for their members, is unacceptable. The development of countermeasures and dissemination of "our" narratives should be a joint effort, requiring the active involvement of every country. While national solutions are necessary, national doctrines should be aligned with NATO policies. The recent achievements of the Czech Republic - the establishment of specialized Czech strategic communication unit and internal security audit – could serve as a good example for other European countries to follow.

> ***"A civilian, not military body, should be responsible for StratCom measures."***

2.4. Re-build trust and the credibility of institutions

One of the main narratives of Russian disinformation policy is the motto of Russia Today – question more. This narrative aims to sow distrust and dismay among people - to trust no one including the state institutions. If you don't know what's going on, you do nothing. This inactivity or inability to respond promptly is one of the main goals of hostile foreign influence – Russia wants to undermine the decision-making processes of foreign governments. Russian disinformation methods are utilizing the increased lack of trust in state institutions and the perception that the system is corrupt in Western countries.

> ***"When was the last time the CIA was portrayed in a movie as the good guy?"***

The perception of "the enemy" in Bond and Bourne movies, as well in TV series' such as the X-Files or Person of Interest, highlights the emotional and cultural context in which the citizens of Western countries are living – trust no one. Therefore, transparency and the unmasking of corruption are crucial in re-establishing trust in state institutions and fighting an information war.

2.5. Enhance research and monitoring of information war and its techniques

Due to the rapid changes of the information era and the ever-increasing impact of social media and citizen journalism, methods and techniques used in information war should be continuously studied and analysed to identify patterns, trends and to develop effective countermeasures. Aside from further expanding the scope of NATO STRATCOM CoE activities, similar analytical capacities should be established at the national level, making use of the excellent NATO STRATCOM CoE research.

2.6. Support debunking and fact checking

By debunking false stories being spread by disinformation outlets, their appeal diminishes and they are shown for what they are – media outlets spreading lies and manipulating their viewers and readers. However, in order to be effective, debunking and fact-checking should be country specific, since the disinformation outlets are also customised and translated into national languages to increase their impact. Initiatives such as Stopfake should be further expanded and their outcomes widely publicised.

2.7. Develop protection mechanisms for the victims of trolling

One of the most prominent wake-up calls in Europe, in terms of revealing the power of social media and trolls, was the hate and discrediting campaign against Jessika Aro, a Finish journalist who tried to map the influence of online trolls in Finland. In general, people and institutions uncovering the "ugly truth" are often targets of the army of online trolls, cyberattacks, lawsuits, denial-of service attacks or hacking. Therefore, governments, using appropriate measures, should provide support to such people or institutions. Protective measures for victims of disinformation or cyberbullying should be an integral part of state countermeasures developed to target hostile foreign influence.

2.8. Strengthen the democratic immune system

The battle for the hearts and minds of people is not a new concept. However, the technological development of our society and social media have increased the dissemination of fake news and so changed the information environment. There are very few restrictions on what cannot be posted on social media and no gate keepers such as editors or accredited journalists that control the quality of the content on social media.

"Social media have become weapons of mass destruction."

Media literacy and critical thinking are the first barrier to deception and manipulation by disinformation and propaganda efforts. Everybody, a social media user or not, should know how to distinguish a distorted story. We need to empower people to defend their own information systems. The development of skills and awareness among people leads to more resiliency towards disinformation and hostile foreign influence. However, many NATO member and partner countries lack the adequate curricula and structures enabling the most vulnerable groups to equip themselves with such skills. Therefore, incorporation of media literacy skills and critical thinking into school curricula is essential to successfully prevent young people from falling into the trap of false information and media manipulation by disinformation.

2.9. Support training for media professionals and journalists

Journalists and traditional media still play a major role in informing public and forming political opinions. Yet, journalists often lack the basic skills enabling them to detect and spot disinformation and fake news. Therefore, media professionals should be given an opportunity to further develop and increase their skills on fact and source checking, as the disinformation content also

spreads to traditional media. Fact checking content should be incorporated into curricula as well as professional development courses.

2.10. Ensure transparent media ownership

Concentration of media ownership threatens media pluralism and unbiased reporting on political and societal developments. In many cases, it is very difficult to track the real owners of media, since they use offshore companies to hide the real ownership structure. Due to their huge impact on the general public, a complete ban on offshore ownership of media companies should be introduced at the national level. Transparent media ownership coupled with effective anti-trust measures would diminish the impact of undemocratic actors on local media.

2.11. Close the democratic gap and reach out to audience and voters

One of the aspects of information war is the use of local allies – fringe political parties and actors - to spread the anti-western, anti-democratic narrative. By using domestic political actors, the anti-western narrative has much broader impact, compared to direct communication by foreign entities. In many countries, such efforts are directly or indirectly supported by the Kremlin. In order to counter them, democratic political actors need to step up their direct communication with voters and fundamentally change their online presence. Fringe political actors sympathetic to the Russian narrative are far more effective in communicating their messages on social media. There is an urgent need to match these efforts and close the gap in online presence between fringe political parties and democratic political actors.

Aside from online communication, direct interaction between political elites (decision and opinion makers) and the people in the regions should be greatly enhanced. Opinion makers should step out of their information bubbles, listen to concerns and respond to the needs of people living outside of political and cultural centres.

III. Recommendations for Other Actors: NGOs,Media and Private Sector

3.1. Increase the role of IT companies in countering disinformation

While social media are inherently neither good nor evil, they can be very effectively and easily used for both purposes. An image or video is more efficient in making a point than any text full of credible arguments and data. Furthermore, everybody with a smartphone has become a journalist or a “useful idiot”, disseminating particular narratives. Currently, the structure of online advertisement earns those who get the most views and clicks money.

“Fake news generate an incredible amount of money”

Online advertising does not question the validity of information. Furthermore, social media operated by private companies are used by everybody – they spread both disinformation and real news. The knowledge of search engine algorithms and social media tools rests with private companies. Therefore, private businesses such as Twitter, Facebook and Google should be actively involved in countering disinformation. For example, a Facebook news verification system flagging potentially fake content should be established.

> ***"We need better marketing for the truth during times when lies spread like fire."***

3.2. Support study of digital culture and social media

In the so-called post-factual world, the democracy sphere depends on the number of clicks. Technological development has occurred so fast that many policies and decision-making processes are still trying to catch up. Some of the state departments and institutions are slowly exploring the possibilities of social media and are attempting to communicate with the public via these outlets. However, there is little data on how information or disinformation is spread via social media, what articles or posts people react to on social media, as well as what makes them share and further spread these narratives. There is also limited knowledge on how bots and automated systems are used to spread disinformation in hybrid war.

Already all the clicks and preferences of social media users are being collected and processed. This data, given unwittingly, is eventually used by companies to shape people's decision-making processes and re-instate the information bubbles people are locked in on social media. Therefore, it is important to study the vastness of digital culture and what impact it has on people and democracy.

3.3. Build network of actors countering disinformation

Resources available for countering disinformation are scarce. Therefore, organizations active in this field, whether governmental or non-governmental actors, should actively cooperate. Pooling and sharing know-how and resources would increase efficiency and the impact of countermeasures. It is important to build strong networks of governmental institutions and strong civil society organizations united by common values and ideas. State institutions and international organizations need to actively cooperate with think-tanks and academia. In case of emergencies, a pool of opinion makers and experts should be available to be employed to address the public and counter disinformation.

3.4. Develop new subscription based models for traditional media

The technological development of our society and social media have drastically changed the news and information environment. While traditional mainstream media were too slow to adapt to this change, they still play an important role in being the watchdogs of reality and investigators of society. However, while fake news is free and easy to access, the different subscription models of investigative news outlets create another obstacle for people to get the facts and truth.

These information paywall bubbles are splitting society into two parts – those who have subscriptions and thus have information, and those who rely on "free" easily-accessible (dis)information.

"Traditional media is like a farm horse in the age of automobile."

Therefore, big traditional media like the Wall Street Journal, the Economist, the News York Times or the Washington Post should abandon the model of individual subscription and should use the subscription-based model used by music companies such as iTunes. This financing model would still provide media with revenue and subscribers would pay only for the articles and news they read.

3.5. Set up an independent fund for investigative journalism

An anti-elitist, anti-establishment attitude also manifested itself in an anti-journalist attitude. Fake news industry generates a lot of money, but it is not possible to label all such practices as Russian propaganda since they are driven purely by commercial interests. Therefore, big social media companies should set up a fund to support investigative journalism. This fund will enable media outlets or civic organizations to pursue their stories further and investigate. News outlets, freelance journalists or watchdog organizations would have resources for long-term data collection and in-depth analyses.

Conclusions

Organised state-sponsored disinformation campaigns have become an important tool of hybrid warfare weakening the institutional framework of the European Union and NATO, democratic values and undermining the security architecture of Europe. According to available information, the Kremlin has significantly increased its budget for media spending, which includes disinformation campaigns. The RT (formerly known as Russia Today) television network alone operates in 100 countries with budget of some 300 million EUR from the Russian government and Sputnik, online news service established by the Russian government-controlled news agency Rossiya Segodnya, spreads the Russian narrative of online news in 32 foreign languages and countries.

In addition, according to unofficial sources, thousands of people in Russia, including those in troll factories, are actively working on producing and spreading disinformation and Russian narratives - of the 'evil West' with an aggressive NATO and the EU in shambles; the (distorted) world according to the Kremlin, in particular on the Crimea Conflict and Ukraine; and the narrative of the good Russia portrayed as the protector of peace and safety.

The impact of these efforts is further strengthened by the click-bait model of the rapidly growing fake news industry, spamming social media with its distorted version of reality and bombastic tabloid headlines. Such outlets, mostly set up for the profit of their owners, not only produce their own dismaying hoaxes and distorted news, but also serve as echo chambers for the content produced by state-sponsored disinformation media channels. Thus, the vastness of media outlets and decentralization of information flows enable the direct impact of disinformation and propaganda narratives on public opinion in countries, which in turn affects the policy debate.

Although the public diplomacy activities of many NATO countries have been instinctively increased in order to mitigate the impacts of the information war, adequate attention needs to be paid to the development and coordination of strategies to address this threat systematically. NATO and its member states must plan and train for scenarios of hybrid war including military as well as paramilitary elements well integrated into a comprehensive, centralised effort comprising diplomatic, business, criminal, intelligence, propaganda and other means. The conflict in an era of hybrid warfare may go through several stages before reaching the threshold of Article 5 and our responses and planning should reflect this new reality.

NATO and its member and partner countries need to think bigger, analyse deeper, and use every available opportunity to learn from each other if they are to succeed in winning this new form of conflict. The Kremlin and other foreign powers have laid the groundwork for their propaganda machine for years. They have a head-start but we need to close this capability gap if we are to succeed. Sharing lessons learned and successful models of countering and preventing the negative effects of information war across the larger NATO family is therefore essential to our success.


Ján Cingel
Ketevan Tsikhelash
NATO
OTAN


Countering
Information War
GLOBSEC
POLICY INSTITUTE
TO OTA


NATO
OTAN


Filip Djuranović
Milan Nič


Lessons Learned from NATO and Partner Countries
GLOBSEC
NATO


NATO
Irakli Porchkhidze


Countering
Information War
Lessons Learned from NATO and Partner Countries
GLOBSEC
POLICY INSTITUTE
Jakub
WIŚNIEWSKI
Mark
LAITY


at is new?
Every second, on average, around 6,000 tweets are tweeted on Twitter, which corresponds to over 350,000 tweets sent per minute, 500 million tweets per day and around 200 billion tweets per year
Useful Stats


From Bond to Bourne
JAMES BOND IS BACK!
FROM RUSSIA WITH LOVE
THE BOURNE SUPREMACY
THE BOURNE ULTIMATUM


Countering
Information War
Lessons Learned from NATO and Partner Countries
GLOBSEC
POLICY INSTITUTE
Martin M.
ŠIMEČKA
Hovhannes
NIKOGHOSYAN
James
MILLER


PARLAMENTARNI
IZBORI


Information War
Lessons Learned from NATO and Partner Countries
INSTITUTE
Pavel
MACKO


Countering
Information War
Lessons Learned from NATO and Partner Countries
Philip N.
HOWARD
Ljubica
PENDAROSKA
Mirian
LEXMANN

GLOBSEC
POLICY INSTITUTE

GLOBSEC Policy Institute
Klariská 14
811 03 Bratislava
www.globsec.org