GLOBSEC
IDEAS SHAPING THE WORLD

NATO and Countering Disinformation

The Need for a More Proactive Approach from the Member States

16 May 2022

www.globsec.org

GLOBSEC
IDEAS SHAPING THE WORLD

Author: Amb. Tomasz Chłoń

Ambassador of Poland to Estonia (2005-2010) and to Slovakia (2013-2015)
Director of NATO Information Office Moscow (2017-2020)

Contents

The Western world must do more to combat disinformation. NATO leaders are expected to approve a new Strategic Concept at the Madrid Summit in June 2022, but will the need for a proactive response to this challenge be reflected in the Alliance's second most significant document after the North Atlantic Treaty[1]? Most likely yes; however, in the fight against disinformation, the real question is not what more NATO can do for its Allies, but what they can do for the Alliance. While specific disinformation related to military deception is beyond the scope of this paper, the recommendations in it have been validated ever more so by Russia's full-scale invasion of Ukraine.

Russian Disinformation – 2022

One of the founding myths of Russian foreign policy (developed below) relates to a betrayal by the West. Many in Russia are either unwilling or too scared to challenge the veracity of this tale since it has become national dogma. As the freedom of speech constitutes one of the fundamental and respected rights of democracies, this myth is also widely spread throughout the West. Moreover, the West's culture of open debates, which respects differing points of view, puts Russian masterminds of false narratives in a privileged position when it comes to influencing Western societies and their decision-making processes. It also renders NATO and EU countries increasingly vulnerable to influence from pro-Kremlin propagandists spurred on by an unbridled sense of initiative and combined with active measures as well as armed conflicts[2].

The matrix of the myth of Western betrayal and Russian self-victimisation is the "broken promise of not enlarging NATO to the East". The Kremlin has also used this myth to justify the full-scale invasion of Ukraine on 24 February 2022 – a move that has potentially incalculable consequences for European and even global security. This new stage in Russia's confrontational policy has been further solidified with support from the increasingly belligerent Belarusian dictator although Alyaksandr Lukashenka's standing has also been weakened through his complete dependence on Russia.

Minsk, assisted in turn by Moscow, created a migration crisis on the Belarusian border with Poland, Lithuania and, to a lesser extent, Latvia, thereby opening an additional hybrid front. Increased tension on NATO's entire eastern flank and the war waged by Russia against Ukraine have been exacerbated by Russian and Belarusian hostile disinformation activities, which are unprecedented in terms of scope, intensity and toxicity.

In both Russia and Belarus, the highest political authorities, diplomats, state-controlled media, special services and their proxies have been actively involved in spreading familiar but intensified false narratives as well as new concoctions that are particularly harmful to the public in the Russian-language, state-controlled information environment. Unfortunately, some of these narratives fall on fertile ground in certain circles in the West and are cynically exploited in local political struggles. The goal of disinformation is to undo the cohesion of the transatlantic community, undermine the credibility of NATO and EU members and, ultimately, derail the existing rules-based international order.

The "new-old" story is that: *Russia, and now Belarus, are surrounded by foes, and the heightened security crisis is the fault of the West, which had been allegedly pushing Ukraine towards war. Having rejected the Minsk agreements, Ukraine had been preparing to launch military operations against the inhabitants of Donbas, occupied Crimea and regions in Russia itself; to this end, Kyiv had been concentrating its forces and resources (including weapon systems received from NATO countries) in the east of the country. Polish and American mercenaries were also operating and preparing armed provocations in the east of Ukraine; this means that not only Ukraine but also the West itself had been preparing to attack the Russian Federation and Belarus. Ukraine had been mobilising troops on the border with Belarus, against which Poland has been making territorial claims.* Finally, Vladimir Putin justified his illegal assault on Ukraine with *the need to demilitarise and denazify Ukraine*. He did so despite the fact that the Ukrainian nation lost 8 million people in World War II fighting Nazi Germany and is a country led by a Jewish president who won the popular vote in a free, fair and democratic election; an election which showed the Ukrainian neo-Nazi parties having less support than probably anywhere else in Europe.

Countering Disinformation: Challenges and Actions

Although it is not easy to measure, the pernicious nature of Russian disinformation and interference abroad has been "tested" positively in several cases, with prime examples including the attacks against Ukraine, the U.S. and French presidential elections, as well as the Brexit referendum. The extent to which social polarisation and internal political fights are causal effects of Russian (and others) meddling in the West could be discussed elsewhere, but what is of importance for this paper is that such frictions are certainly being exploited and amplified by the opportunistic organisers of external disinformation.

In any case, the cumulative result can be seen, for example, in Slovakia where a significant part of the society blames the Alliance for the current Russian crisis (at least that had been the case before the full-scale war against Ukraine started) or in Croatia where the president has been questioning the Alliance's Eastern policy. The actions of candidates for the highest political positions in France who propagate anti-NATO slogans are even more concerning. Sympathy for the Russian regime is shown by representatives of ruling or co-ruling parties in NATO and EU member states, including Fidesz in Hungary and Podemos in Spain (which should be particularly sensitive to disinformation following the Kremlin's interference in the Catalan independence question).

Moscow uses other tools to exert its influence in Western countries, but their effect may be more prevalent in countries with elected parties that have pro-Kremlin inclinations (e.g., AfD in Germany). Russia has been known to drive political corruption, use blackmail tactics and even resort to acts of terrorism. The growing popularity of conspiratorial and pro-Kremlin narratives in Germany, France and Spain that are spread through encrypted social channels linked to Moscow have become a fact of everyday life[3].

While it is challenging to fully assess how effective countermeasures to tackle foreign interference have been, examples from countries that have taken them up with determination show that the fight against foreign meddling can have a genuine impact. Most ways and means of counteracting disinformation in this political warfare fall under the responsibility of sovereign states (and the European Union due to its legislative prerogatives). It is predominantly their responsibility to build resistance to disinformation and to respond to it with both deterrence and punishment. NATO's role in this regard is limited. At the same time, the Alliance – as an organisation at the centre of false accusations and hostile propaganda – knows how to defend itself, which is evidenced by the overall high level of public support for NATO among its members. Nevertheless, it seems that the Alliance's potential to combat disinformation is not fully utilised by its individual members, which could benefit from NATO's expertise and coordinating capabilities to a greater extent than they have thus far.

[1] "Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation" Adopted by Heads of State and Government in Lisbon, 19 November 2010, **https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf**

[2] R. Kupiecki, "Western Betrayal": The Founding Myth of Russian Foreign Policy, in:
A. Legucka, R. Kupiecki (eds.), Disinformation, Narratives and Memory Politics in Russia and Belarus, Routledge, London 2022.

[3] Ein Virus des Misstrauens: Der russische Staatssender RT DE und die deutsche Corona-Leugner-Szene,

NATO’s Response

Tackling disinformation remains an essential part of NATO’s communication strategies and day-to-day operations, which includes media monitoring, analysis of the information space and proactive communication in a coordinated and fact-based manner. Its goal is to inoculate or “pre-bunk” the mediasphere rather than debunk each false claim, i.a. through “Setting the Record Straight” narratives and activities which counter the Kremlin’s myths about NATO.

In 2019, NATO adopted an updated and systematic package of appropriate objectives and measures to combat disinformation. The following year, NATO’s Response to Disinformation on COVID-19 became realised in an Action Plan issued to Allies by the Secretary General. This document sought to bring together multiple strands of work on countering hostile disinformation surrounding COVID-19. In 2021, NATO’s Toolbox for Countering Hostile Information Activities was created; it reflects the Alliance’s twin-track model to respond to hostile information activities: “understand” and “engage”, underpinned by “coordination”. The document aims to provide Allies with a toolbox to assess hostile information activities, including disinformation, and to assist in determining possible courses of action. Furthermore, NATO IS staff holds biweekly briefings on Russian and other disinformation activities at various relevant committees. Within the Civil Emergency Planning Committee, as part of a long-term effort, and covering resilience baselines – spanning across many domains including communications – Allies share information about how prepared they are to face various key civil security challenges, including disinformation.

The organisation supports member and partner states by providing guidance as well as co-financing for social and scientific projects that strengthen their resilience to disinformation. Rapid-reaction teams have been made available to member states as part of NATO’s strategy to fight hybrid threats. The organisation is also cooperating more closely with the European Union to ensure that NATO benefits from the EU’s Rapid Alert System set up to counter disinformation.

Towards a Consistent Response to Disinformation

At the same time, the West has yet to prepare a coherent, comprehensive and coordinated response to Russian disinformation. It is up to nations to fully utilise NATO’s potential. A response practice has been developed and seen partial success within some states and Euro-Atlantic institutions, but it has not yet been translated into a real common policy or strategy.

At national levels, political declarations and agreed action plans are still not fully implemented in too many instances. Western states approach disinformation in varied ways due to differences in history, regional security, wealth, education, media quality, political and legal culture and – most importantly – the current state of their relations with Russia. As a rule, some states prefer bilateral approaches that safeguard national prerogatives. This may change now following the Russian invasion of Ukraine.

Nevertheless, the challenge of disinformation has begun to attract higher political attention. In the European Union, this has transpired through the adoption of the European Democracy Action Plan[4] and the presentation of new regulations on digital services in December 2020. These regulations aim to address the core issue of the business model developed by disinformation organisers who instrumentalise social media platforms. The report by the Special Committee on Foreign Interference in all Democratic Processes in the EU, including Disinformation (INGE), has also promised that other means of influence will be addressed[5].

In an effort to combat disinformation, the Digital Services Act (DSA)[6] is a breakthrough legal instrument that will fundamentally change the rules of the game for the information environment in the European Union, member states and partner countries; it will also have an impact on national approaches worldwide.[7] The DSA will impose numerous legal obligations on operators of online platforms that are more demanding than the previous voluntary commitments outlined in the Code of Practice for Fighting Disinformation. Companies will be obliged to cooperate with independent researchers and allow them to access their data. They will also participate in complaint and appeal procedures regarding content moderation and dispute resolution. The DSA will provide for the companies’ obligatory consultations, including with civil society organisations. It will also introduce the institution of trusted whistle blowers, who, among other things, will notify the companies about suspected crimes online. The act will correspondingly establish a European Digital Services Council and advisory body made up of national digital service coordinators responsible for implementing legislation at the national level. It will impose specific additional duties on exceptionally large online platforms with more than forty-five million users per month. These obligations will include assessing systemic risks resulting from their services, identifying actions to reduce such risks, conducting independent audits, setting appropriate conditions for algorithmic recommendations of user content and ensuring additional transparency in advertising (including political ads).

Among international organisations and institutions, the European Union plays a leading role in counteracting disinformation and introducing new effective measures against it. The future regulations on transparency in financing political parties and election campaigns gives hope for limiting corruption and external influence in the affairs of the member states.[8]

NATO and the EU share similar membership compositions and were created based on comparable value systems, so it is reasonable to assume that counteracting disinformation will be more prominently reflected in NATO’s new Strategic Concept. A need for this has been suggested by the authors of the NATO2030 expert group report prepared ahead of the Madrid Summit in June 2022[9]. As a result, countering disinformation could be given a more visible place on the agenda of NATO ministerial meetings and summits, and more proposals with clear commitments by member states to tackle disinformation may be unveiled. NATO also has the opportunity to strengthen the mandates of existing committees to better coordinate national efforts.

[4] European Democracy Action Plan, European Democracy Action Plan, European Commission, https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en

[5] EU should build a sanctions regime against disinformation, European Parliament, January 2022, https://www.europarl.europa.eu/news/en/press-room/20220119IPR21313/eu-should-build-a-sanctions-regime-against-disinformation.

[6] The Digital Services Act package, European Commission, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

[7] After the project has been presented by the European Commission, it is processed in the European Parliament. It shall enter into force in 2022.

[8] Despite some activities, the role of other international organizations, such as the UN, OSCE, and the Council of Europe, is limited, whether due to membership, the participation of notorious disinformers among them, or systemic low effectiveness.

[9] NATO2030: United for a New Era, NATO, November 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

Strategic Context

The Alliance's new Strategic Concept could therefore reflect more comprehensively the key tenets of an enhanced approach to disinformation, encompassing public diplomacy, strategic communication and social resilience. Such an approach could also consider new and innovative tools to combat disinformation, given that these can fit into a broader strategic context of NATO's work.

In 2019, the Alliance approved not only the first secret military strategy in over 50 years but also a strategy for developing the necessary military and technological potential in connection with the changing nature of conflicts (NATO Warfighting Capstone Concept). With its stronger deterrence and defence approach to security, NATO began implementing a policy that enabled the coordinated development of breakthrough technologies, recognising that technology development will be a priority in seven areas: (i) artificial intelligence, (ii) advanced big data analysis, (iii) autonomous technologies, (iv) quantum computing technologies, (v) biotechnology, (vi) hypersonic capabilities and (vii) space technologies. In February 2021, the Allies approved the Coherent Implementation Strategy on Emerging and Disruptive Technologies. Eight months later, in October, the first NATO strategy on artificial intelligence was approved. From the perspective of disinformation activities, the future of artificial intelligence can be seen as a dual-purpose tool. Depending on human decisions, it can become a sword in the hands of opponents of freedom or a shield that protects societies and individuals against the consequences of their actions.

NATO Strategic Concept and Recommendations

In light of the current security environment in Europe and worldwide, traditional threats are still a priority, and collective defence will remain one of NATO's core missions, even more so than in the 2010 document.

Among the tasks supporting this existing mission, there will also be development of a full range of instruments aimed at neutralising new risks, including disinformation. As experience has shown, threats evolve in terms of intensity, goals, methods and means. The challenge for the negotiators of NATO's new Strategic Concept will therefore be to provide for adequate flexibility when crafting current and future countermeasures that will guide the Alliance's activities for years to come.

Overall, NATO's (and the West's) coherent response and efforts against foreign disinformation, both nationally and internationally, should focus on: (i) their civic resilience, (ii) their offensive capabilities as much as their defensive ones and (iii) minimising the differences in how individual Western countries approach disinformation in practice. In other words, deterrence must be pursued through both punishment and denial. The following recommendations apply specifically to NATO but also to other organisations that can cooperate more with the Alliance as well as the member states themselves, for which NATO can act as a catalyst in the development of national policies and practices[10].

NATO

Threats and risks stemming from disinformation should be more prominently featured in the agendas of ministerial meetings and NATO summits. In addition to presenting clear proposals that encourage a commitment to combating disinformation, NATO should also strengthen the mandate of existing bodies that focus on strategic communication to better coordinate national efforts. This could include the exchange of information about threats, incidents and best practices of response. There is a room for improvement in how the European Union, NATO and G7 coordinate and cooperate as well as how they consult with other institutional partners like the United Nations and the OSCE.

Specifically, NATO should:

- assign existing groups within NATO to coordinate the exchange of best practices of counteracting disinformation as well as refine, standardise, operationalise and test them during dedicated exercises.[11] National plans presented to NATO allies and accounted for in the annual planning cycle could also be considered as disinformation anticipation and pre-bunking measures.

- upgrade existing toolkits that address the needs of the organisation and member states so that they can better counter disinformation.

- more effectively use the embassy network of Alliance member states, which act as Contact Point Embassies (CPE) and have a clear mandate for conducting public diplomacy on the Alliance's behalf in as many as 40 partner countries[12].

In the longer term, attempts to divide the Alliance could be countered by NATO's expansion and sponsorship of information campaigns, such as #WeAreNATO. In such campaigns, educating students in the senior grades of primary and secondary school about NATO and its security policy should be more actively promoted.

NATO and Other Organisations

A model and practice of pre-election and pre-bunking activities should be developed as part of pre-election missions in EU and NATO member states, possibly in cooperation with the OSCE. The outcome would be an assessment of pre-election threats, including cybernetics and related countermeasures.

Together with the EU, NATO should create a programme that will support local initiatives in partner countries. These initiatives could be supported by EU representations and NATO Contact Point Embassies as well as by national embassies of member states.

It is essential to level out the differences in resilience to disinformation due to Russia's tendency to leverage systemic weaknesses in various EU and NATO member states and use local actors in one country to attack other countries. The creation of projects from the European Union, NATO and the United States through existing networks of representations, embassies and funds to support the Western Balkan states would be particularly beneficial. Additionally, a separate programme dedicated to civil society and media in Serbia would be useful in promoting disinformation resilience.

[10] T.Chłoń, "Does the West Need a Coherent Response to Russian Disinformation?" in: A. Legucka, R. Kupiecki (eds.), *Disinformation, Narratives and Memory Politics in Russia and Belarus*, Routledge, London 2022.

[11] Member states make assessments through different methods. All members (not just few as is the case now) should send their reporting on disinformation to NATO to provide stronger situational awareness.

[12] Contact Point Embassies in partner countries Contact Point Embassies in partner countries, NATO, https://www.nato.int/cps/en/natohq/topics_49190.htm?selectedLocale=en

NATO Member States

In particular, countering disinformation focuses on addressing the polarisation within democratic states that Russia continuously attempts to exploit. Owing to its regulatory prerogatives, the response from the community's members, supported in Europe mainly by the European Union, should be based on:

- strengthening resilience to disinformation through education on democratic values, improvement of election standards and increased monitoring of transparency in electoral campaigns.
- improving media education. At the primary and secondary level, media education should focus on developing competences in critical thinking. In the case of high school and university students, the curricula should teach methods of confirming or disproving statements appearing in the media or on the internet (i.e., fact-checking).
- a media policy aimed at strengthening trust in the media. Specifically, this involves better funding and support for media independence and standards, investigative journalism and fact-checking.
- assertive action towards social media platforms. This includes identifying users, ensuring the neutrality and diversity of algorithms, managing content selection and guaranteeing that ads are transparent. Transposing the DSA to national legislations should be done as expeditiously as possible.

Western states should also be more proactive in raising the costs for perpetrators of disinformation. This could be done by publicly exposing their activities and imposing sanctions. In particular, they should:

- draw attention to Russian media that sows propaganda and operates abroad.[13] This will make these entities clearly identifiable to recipients and help harmonise the decision-making standards of regulatory authorities regarding such media. Moreover, Western states should standardise the procedures for imposing disinformation-related penalties, as was the case in the United Kingdom and the Baltic states' response to RT and Sputnik. Countries should also make bolder decisions about sanctions directed against employees of Russian propaganda centres and outlets.
- expose disinformation and influence operations, disavowing them at the highest level and in special services' reports. As a standard, such reports should be publicly available in all EU and NATO member states.
- proactively use alert systems within the European Union, NATO and G7. In the case of the European Union, this is also a matter of credibility as the current operation of the Rapid Alert System has been assessed as weak.

Attribution could be facilitated by further work on terminology, including clarifying concepts related to disinformation; it would also benefit from legal clarification on the violations of the fundamental rights of freedom of speech and election interference. Such arrangements would help develop protocols for identifying and exposing perpetrators, which could in turn help overcome serious political dilemmas linked to attribution.

[13] They dispose of effective research instruments in this respect, namely: The Centres of Excellence on Strategic Communications in Riga and on Hybrid Threats in Helsinki.

In Lieu of Conclusion

In many ways, the Russian invasion of Ukraine in February 2022 created a completely new situation for the fight against Russian manipulation and propaganda. The invasion exposed the Kremlin's earlier disinformation about its intentions towards Ukraine as people worldwide watched on their smartphones, computers and TVs the savage destruction and death inflicted in Kyiv, Kharkiv and above all, Mariupol – the Ukrainian Aleppo. The relentless attacks against civilians and forced exodus of millions exposed Putin's true plans and cynicism as well as the Russian genocidal machine behind them. This metaphorical Waterloo (at the time of writing, it is still unknown whether we will witness an actual military defeat as well) could suggest that, from a strategic point of view, the pre-war hybrid actions taken against the West, including disinformation, were ineffective. This hypothesis does not appear to be justified, however.

Peacetime rules have given way to the laws of war, and the democratic world has stood up for victims and condemned their aggressors. At the same time, the situation begs the following question: if the West had been quicker to introduce stringent sanctions against Russia's disinformation apparatus, as called for by many civil society groups, and had undermined Russian propaganda from the outset, would the war have erupted in the first place? Immediate and firm sanctions would have not only shown that the West was determined and united, but it would also have made Western societies more resilient to fake news, manipulation and political corruption, which could have resulted in a different relationship with Russia. Before the ongoing information war reached its most heated phase, the West's primary issue was not Russia's effectiveness but its own lack of preparation.

It's impossible to ascertain whether the war would have erupted under different circumstances. There is no doubt, however, that the West has shown unprecedented unity for the victims of this brutal aggression and attack on the foundations of international order. Yet, it is difficult to declare victory over disinformation or democracy's triumph over authoritarianism. It is unclear when and what kind of Russia will emerge from this war in the long term, nor what direction Russian society will take. Should we expect a bloody farewell to imperial ambitions, as was the case in the French war in Algeria? At the global level, China will undoubtedly also draw lessons from recent events.

Russia's recent attack on Ukraine has underlined the gravity of information manipulation problems and highlighted the potential to combat them. What once seemed complicated and difficult concessions from EU member states have suddenly become swiftly adopted initiatives and commitments. The information "anti-war" has helped bring to a spectacular end the monopoly of countries, traditional media and specialist non-governmental organisations in fighting disinformation. A surprising number of Internet users and groups have notably become actively involved in the process, including Anonymous, a hacker group that previously would not have been expected to play a role in combating disinformation. Meanwhile, the significance of strong leadership has been highlighted through the figure of Ukrainian President Volodymyr Zelenskyy. At the same time, it has become increasingly evident that social media dominates today's information environment and is a powerful tool but also a double-edged sword (given how the Russian authorities use Telegram channels).

Sanctions imposed as a result of the war were met with expected countermeasures from the Kremlin. Russia's response also included blocking access to Western traditional and social media and shutting down the last independent news outlets in Russia (*Ekho Moskvy and Dozhd TV*). As this occurred, the primary challenge shifted from protecting against Russian disinformation in the West to finding a way to reach the indoctrinated Russian society.

However, the "Russian Wall" of (dis)information raised by Putin is not as leakproof as he would like.

Millions of Russians have installed VPNs – data shows that 6.4 million apps were downloaded from the Apple App Store and the Google Play Store in the first three weeks of the war compared to 230,000 in the three weeks prior. Russians are bypassing censorship using Tor technology, which makes it possible to create portals and networks (including for Twitter) on the dark web. Russian citizens receive tens of millions of pieces of information about the war through regular text messages, emails and online ads. We also cannot underestimate the importance of the international traditional media, which is publishing content about the war in Russian in the largest newspapers in Poland (*Gazeta Wyborcza*), the Nordic countries (e.g., *Helsingin Sanomat*) and in Germany (*Bild*), for example. However, most Russians remain under the overwhelming influence of the regime's propaganda, but the main battlefield for "souls" are big cities (specifically Moscow) and the younger generations. These audiences are the reason why Putin has shut down the country's last independent news outlets - *Ekho Moskvy* and *Dozhd TV*.

During the extraordinary NATO summit on 24 March 2022, it was determined that the Alliance would continue to counter Russia's lies about its war in Ukraine and expose fabricated narratives, operations and provocations. NATO members also decided to prioritise increasing the resilience of their societies and infrastructures in the face of Russia's ominous influence, which includes strengthening their cybersecurity and disinformation response capabilities. During the summit, NATO also called on China to stop spreading the Kremlin's false narratives, especially about the war and NATO[14]. The European Union, for its part, adopted the Strategic Compass, which sets the EU's framework in the field of international security, including foreign influence and information manipulation[15]. Only time will tell how long the Alliance, the EU and the West remain determined in fighting disinformation in international politics. It is already clear, however, that the fight against disinformation is not doomed to be Quixotism. On the contrary, the free world has all the data to win this fight even, or perhaps especially, in conditions of war.

Still, the recent developments in Russia's aggression towards Ukraine and confrontational policy towards the West warrant a further shift in attitudes in tackling disinformation. Unless Putin steps down or is removed, Russia's behaviour will not change for the better, and the West will have to reckon with more challenging disinformation warfare by Russia and Belarus. Moreover, China will soon present a formidable challenge with its own set of methods and tools of disinformation.

Therefore, where appropriate, Allies should overcome any remaining reluctance and uncooperative tendencies that limit the role of NATO in combating new threats, especially hybrid ones. First, tackling disinformation should gain greater political attention among all Allies. National countermeasures undertaken in some member states (e.g., France, Germany, the Baltic States and the UK) or partner countries (e.g., Finland and Sweden) testify to the importance they attach to the problem of falsehoods in international politics. When allowed, NATO could better serve as a coordinator and multiplier of good practices (of which these countries are, to a significant extent, a model). Second, there is no need to reinvent the wheel. The work ahead can be built on the existing acquis and institutions without substantial additional resources, which is important given budgetary constraints. Third, there is clearly more scope and possibility for NATO to foster synergies with other organisations – most notably the EU – in helping each other and partner countries to fight foreign disinformation. Overall, NATO and the West must take a more offensive approach in tackling this ever more dangerous scourge.

[14] Statement by NATO Heads of State and Government, https://www.nato.int/cps/en/natohq/official_texts_193719.htm?selectedLocale=en

[15] A Strategic Compass for the EU (2022), EEAS, https://eeas.europa.eu/headquarters/headquarters-homepage_en/106337/A%20Strategic%20Compass%20for%20the%20EU

GLOBSEC
IDEAS SHAPING THE WORLD

Vajnorská 100/B
831 04 Bratislava
Slovak Republic

+421 2 3213 7800
info@globsec.org
www.globsec.org