NATO 2030: NATO-Private Sector Dialogues with GLOBSEC

The Information Landscape as a Theatre of Geopolitical Competition – 25 February 2021

Policy Takeaways

NATO, its allies, and the private sector are all facing the reality of an ever-changing and increasingly complex information landscape. Striking a balance between fundamental freedoms and calls for increased digital regulation requires developing a coordinated transatlantic approach. Responding to these challenges will require more extensive and innovative collaboration between the Alliance and the private sector. The fourth of the NATO-Private Sector Dialogues with GLOBSEC brought relevant stakeholders together to exchange views and insights about how the private sector can contribute to dealing with decision making on emerging infrastructure, the weaponization of the information space, the future of governance of the information landscape, and how storytelling is impacted by the digitalization of the information space.

- **Techno-political Decision Points on Emerging Infrastructure –**

Key insights:

- The public and private sectors recognize the urgent need for information sharing, but cooperation remains especially low in implementing responses to shared threats.
- There is a need for collaboration on threat analysis that is separate and protected from dialogue about platform regulation.
- In addition to AI and 5G, areas that will gain importance with regard to securing emerging infrastructure include investment screening, sustainable investments and reliance on green technology, autonomous systems, and societal resilience.
- Private-public sector engagement has often suffered from the 'fog of war' problem and often seemed like a lose-lose situation but identifying common goals and shared threats facilitates communication.

Discussion points:

In recent years, public-private engagement has significantly increased in the area of information sharing and especially the detection of threats. However, deeper and more consistent collaboration is needed. Participants highlighted five key areas for improvement during the discussion.

First, there is a need for collaboration on threat analysis that is separate and protected from dialogue about platform regulation. Combining these discussions often stalls progress. *Second*, government officials need additional education on cyber infrastructure and defence. In particular, the public sector often treats cyber defence as a one-time investment rather than viewing attacks on information infrastructure as an ongoing and constantly evolving threat, requiring dynamic adaptation of infrastructure and support services. *Third*, there is often no direct link between corporate entities and NATO with regard to information sharing, often because national governments serve as interlocutors. However, a positive example that already exists in this area is the NATO Industry Cyber Partnership (NICP). *Fourth*, NATO needs to be more forward-looking in its acquisition of infrastructure and emerging technologies rather than relying on Minimum Military Requirements in order to avoid investing in obsolete technology. *Fifth*, NATO should seek to merge technical and geopolitical considerations as it continues to formulate long-term strategies for combatting threats in the information landscape. Prioritizing security from a holistic perspective – e.g., building trust and encouraging societal resilience – will become increasingly crucial moving forward.

On encouraging further public-private collaboration in the information space, participants noted that it is crucial that all parties feel safe sharing their information and stand to benefit from the interaction. Participants also pointed out some challenges that both private and public actors face, including defining what constitutes 'critical' information infrastructure and adapting to the reality that physical infrastructure is rapidly decreasing in importance. The latter issue should motivate NATO to move away from investing in purpose-built hardware and building against physical requirements. Instead, NATO should build to a statement of objectives and service level so that it is able to implement current technologies and adapt to the ever-changing information landscape.

Lastly, participants underscored the fact that NATO possesses unique power to outline principles, promote democratic values, and set examples in the information space. Contributors agreed that NATO's initiatives in this space should (or should continue to) include bringing in outside experts, setting up tools and mechanisms that built trust, and creating communities of interest in order to tackle current and future challenges in the communications and emerging infrastructure space.

- **The Weaponization of the Information Space** –

Key insights:

- Small and medium sized enterprises (SMEs) and civil society organisations (CSOs) are being overlooked with regard to information sharing.
- SMEs and CSOs have the potential to share with NATO considerable analysis and know-how from the ground up.
- The supply of information is greater than the capacity of the governments to respond to it.
- Governments need to have a better understanding of information architecture.
- Private sector entities need to be brought closer to governments and to NATO.

The weaponization of the information space is not new and it has been an important component of warfare for decades. Yet the speed, ease of access to advanced technologies, and the massive scale and impact of these activities is new. With the ever-increasing pace of technological development, it is crucial that cross-sectoral cooperation becomes an essential element of any future policy. Private sector actors could bring innovative solutions, out-of-the-box thinking, and cost-effective solutions. Participants discussed the importance of small and medium sized enterprises (SMEs) and civil society organizations (CSOs) as a source of relevant information and situational awareness.

SMEs and CSOs have considerable expertise in countering disinformation; however, participants identified several obstacles for cooperating with NATO in this area. First, NATO should rethink its approach to combatting disinformation threats and recognize SME and CSO abilities in this space. Second, SMEs and CSOs could share analysis and know-how from the ground up. However, their capacities are limited due to low resources and their access to public funding is difficult. There is a need to develop and implement a different approach to public funding, one which would be more flexible and easier to access by SMEs and CSOs. Third, enhanced cooperation between the public and private sector could lead to better preparedness and capacity to respond to the over-supply of disinformation. In order for this to happen, private sector actors need to be more transparent about their own networks, and governments need to be more forthcoming.

Lastly, NATO and the private sector should empower individuals to recognize and reject false narratives and disinformation. NATO could use its STRATCOM Centre of Excellence in Riga as an avenue to interact with the private sector. The Centre also has the potential to engage in enhanced interaction with citizens, including addressing disinformation, promoting media literacy, and more.

- **The Future of Governance of the Information Landscape** –

Key insights:

- Given the different attitudes towards privacy throughout the Alliance, NATO needs to facilitate more solutions-based discussions between allies as well as between the public and private sector.
- To combat constant misinformation and disinformation, NATO and its allies need to promote media literacy and emphasize the importance of data protection among armed forces and the general public.
- In order to properly deal with the challenges posed by disinformation and misinformation, NATO and its allies need to understand that these two concepts are distinct from one another and will require different approaches from the public and private sector.
- The greatest challenges for governance in the information landscape are posed by digital authoritarian regimes.

Discussion points:

Disinformation and misinformation are two distinct issues that will require different approaches from NATO and its allies. Fully controlling the spread of misinformation in an open society is an impossible task. Private sector actors can and do act to dismantle disinformation networks that are run by state actors such as Russia and China but going after misinformation that arises within a democracy opens up the private sector to political criticism. In addition, disinformation and misinformation are ongoing and constant issues, although they often get the most attention during elections. Attempting to manage their impact on elections will not solve the wider issues that drive them. This is why it is important for NATO and its allies to promote media literacy among the public and the armed forces. NATO can educate its forces on the importance of data protection when engaging with social media so as to safeguard sensitive missions.

Although misinformation can never be fully controlled, the private sector has come up with positive steps. For example, Twitter has already expressly banned political advertising and has strict regulations when it comes to micro-targeting. However, questions persist regarding how fairly the terms of service of major social media platforms are enforced. In addition, the incentive structures of the private sector can put them at odds with the public sector. At the moment, there are a range of approaches across the Alliance on the issue of digital governance. A cohesive trans-Atlantic digital regulatory approach is critical moving forward. More solutions-based discussions between the public and private sectors will be necessary. It is also essential to remember that the private sector is not just composed of companies such as Facebook and Twitter. Smaller companies should be included in these public-private conversations going forward.

Furthermore, authoritarian regimes will increasingly use the governance of information as a cover for nondemocratic aims. For example, terms like misinformation and hate speech could be manipulated, and have different legal and political meanings in different countries. Even within the Alliance, there are very different approaches to issues of privacy, takedown rules, and hate speech. If democratic countries seek to create or enhance legal structures governing the internet, non-democratic countries and authoritarian regimes will do so as well. This is a potential drawback of involving the public sector more extensively in internet governance. In short, just because a government says something qualifies as misinformation or hate speech does not inherently mean this is an accurate assessment of the information. This is why it is still important for companies to independently verify alleged misinformation.

- **How Storytelling is Impacted by the Digitalization of the Information Space–**

Key Insights:

- To make NATO's storytelling more effective, it should consider creating media products that both informalize and contextualize messages to ensure they resonate with the target audience.
- To complement NATO's regular production of non-fiction media products, the Alliance should explore the merits of producing more fiction-based products or establish necessary cooperation with relevant stakeholders (films, books, TV, video games) that are embedded in popular culture to better demonstrate how its work serves the security and interest of the community.
- To appeal to a broader cross-section of the general population, NATO needs to consider enlisting the support of more creative and unconventional surrogates to deliver NATO's story.

Discussion points:

In a disruptive information landscape, NATO is engaged in competition to win and retain the hearts and minds of its citizens. Unlike the Cold War, where the purpose of NATO was unambiguous, more efforts to explain its raison d'être and justify its necessity in a complex and fluctuating security landscape must be made.

Although NATO does a good job at communicating its ethos to its core followers, defence and security experts, its public image could be improved with other constituencies who view the Alliance as a strictly military organization. In addition, many false narratives have been systematically spread about NATO and its activities. For those who, outside of NATO structures, are challenging toxic narratives in the public arena, a support network that might insulate them from online trolling and harassment could also be pursued.

NATO is often perceived to be defined by its adversaries, not itself. This is especially regrettable given that much of the population views NATO as an abstract concept and does not necessarily comprehend what the current battlefields are or what escalation resembles today. Consequently, communicating and reinforcing the importance of NATO in the daily lives of citizens is a public diplomacy exercise that must be prioritized. Generating positive coverage would go a long way in reinforcing an image of the Alliance that people might relate to more naturally. Despite the difficulty of this task, the Alliance has taken a proactive approach to communicating human-interest and community-based stories to citizens in allied states. For this initiative to gain traction, NATO should develop tailored communication products on its websites and social media accounts in local languages that are accessible and easy to understand. Finally based on the scope of the media challenge, NATO cannot be the sole actor in advancing NATO storytelling. Instead, it must better support the narratives and stories disseminated by its Allies within their own countries.

In parallel with this, the spreading of disinformation erodes the Alliance's ability to properly tell its story. NATO should focus on calling out the disinformation techniques and methods of its adversaries. Creating more infotainment products, like an online game, is one area to which more reflection and resources should be devoted. Moreover, NATO featuring in popular Hollywood movies or online streaming franchises could increase its visibility. NATO could also profit from loosening its bureaucratic structures and adopting a more flexible approach that allows its staff more online autonomy.

NATO should also look to enlist more appealing influencers, in and out of the NATO bubble, to promote its storytelling. Great potential exists inside NATO, via its personnel who should be present on social media platforms more often. Enlisting the support of external surrogates who might not fit the traditional NATO bill is also worthwhile exercise that should be combined with agile marketing campaigns to achieve more outreach success.