NATO 2030: NATO-Private Sector Dialogues with GLOBSEC

The Private Sector's Contribution to Alliance Security– 21 January 2021

Policy Takeaways

The role of the private sector in national – and by extension Allied – security has grown and evolved. The private sector routinely outspends the public sector in research and development. In new technological areas, private sector companies designing primarily for civilian use have gained in weight, with some firms, in particular in the world of digital technology, big data, and social media dominate their markets. The second 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 increasing situational awareness, define critical infrastructure challenges, foster innovation, and find the necessary capital to maintain the technological edge in the global "techno-political" competition.

- **Situational Awareness -**

Key insights:

- To make the most out of its extensive sets of data, NATO should strive to improve its internal management and sourcing to ensure it is used effectively and can smoothly receive new data from private sector partners in times of emerging crisis to improve decision making.
- In order to engage a broader section of private sector actors and benefit from their analysis, NATO should consider updating its current Standardization Agreements (STANAGs), to properly reflect the current state of technologies to enable more private sector participation in problem solving and assessing situational awareness.
- To generate more valuable insights from the private sector, NATO should design a value proposition matrix to generate more legitimate business buy-in from private firms to encourage them to share more sensitive data and analysis to advance their interest.

Discussion points:

NATO must utilize every resource and better leverage data to keep Allies safe. A critical part of this exercise consists of generating accurate, topical and compelling situational awareness. As a process, situational awareness must remain adaptable. Traditionally, situational awareness was monopolized by military and diplomatic personnel inputs. Given that the private sector is now the primary engine driving capabilities development and innovation, it was argued that a broader constellation of experts is needed.

To date, NATO has yet to fully incorporate the outlook of this broader pool of expertise and monitoring antennas that would help refine its threat assessment and impose costs upon adversaries. A routine information exchange between private and public sector actors could be a steppingstone in this regard. Yet there are issues related to the classification of data and, for instance, to the willingness of private sector actors to share sensitive insights about their environment, or to the objectivity of data from self-interested private actors.

It was remarked that a more stringent coordination of efforts by NATO bodies and agencies could pave the way for more effective private sector inputs; it appears at times that NATO could achieve better synergies.

NATO is also missing a business style relationship with private firms and needs to do a better job of creating a clear business value proposition. In this context, the current Standardization Agreements (STANAGs) risk falling into irrelevance due to the acceleration of technology development cycles. Imagining a STANAG-2.0 to better connect private firms to NATO's evolving capabilities requirements is an imperative, also to maintain advantageous and timely situational awareness. Finally, all firms, small or large, working with NATO must ensure a baseline of hardened cyber security networks to avoid being compromised.

- **Established and Emerging Critical Infrastructure –**

Key insights:

- On the surface, it appears that everything within society can be categorized as critical. For NATO this cannot be the case and to ensure its continuity of services during crisis, it must actively continue to assess and prioritize what truly constitutes critical infrastructure.
- Despite governments normally being responsible for critical infrastructure, today, businesses are the primary administrators of these services who should be taking a more leading role in their protection and recovery. NATO should consider this feature as they assess what is established and emerging critical infrastructure.
- NATO is viewed as a guide for member states in terms of security and must work to bring overarching guidelines into national systems. Incorporating baselines as reference to national law and regulations to ensure security when it comes to NATO relevant infrastructure is an option worth exploring to create more synergies.

Discussion points:

The rising complexity of what constitutes critical infrastructure requires enhancing public-private sector cooperation. There is no single definition of what infrastructure is critical. To ensure the continuity of government services and public goods delivery, not all infrastructure is critical. Yet, there is more than ever a substantial interdependence between the public and the private sector, such that a standardized and harmonized approach is needed to protect and at times restoring essential enabling infrastructure.

There is no consensus on where responsibilities fall for the delivery of critical services in times of crisis. Governments are accountable for the receipt of key services, while businesses are often the ones delivering them. Businesses should take responsibility as the ones delivering the said services already under normal circumstances.

The private sector tends to consider itself more resilient and capable of more agile reaction in times of crises, compared to governments. The private sector is often willing to work with public authorities, but without prejudice to business imperatives. To create resilient networks, consultations and cooperation are needed early on, during the definition of standards and guidelines.

Private sector actors welcome NATO's creation of resilience baselines but look to an agreed process to apply them in concrete terms. Publication of NATO's baselines would help. One idea is to refer to such baselines in national legal texts. In this way, the security of critical infrastructure would be better safeguarded.

- **Investment and Ownership –**

Key insights:

- Given the current complex security environment, there is much merit to expanding Environmental, Social, and Corporate Governance (ESG) standards to include issues that concern national security.
- A lingering struggle that remains unresolved between business and investment throughout the transatlantic community is how to make supply chains more transparent.
- Existing regulatory frameworks in the transatlantic business community are not sufficient to deal with the threat posed by Russia and China, with the latter representing a greater challenge.

Discussion points:

It is crucial to balance competing investment, ownership, and security considerations if we are to improve public-private sector cooperation. Striking this balance will remain a long-term goal of open societies and open economies. Countries such as Russia and China that do not share our values of democracy and of the rule of law invest heavily in Western private businesses. This represents a security concern, especially in emerging

technologies and defense sectors. There is a strong need to devise more sophisticated solutions that increase security without stifling innovation.

It is important for both public and private sector actors to think about and seek a sustainable balance of risk between economic development and security and have a strategic approach to foreign direct investments (FDI). The proper balance between security and economic concerns is not a one size fits all concept; it will vary. Standards will be calibrated and assessed in a tailor-made approach. Although some mechanisms are in place to deal with these concerns, they are not comprehensive. Comprehensive and transparent systems are needed to ensure that FDI from can be better tracked and regulated.

One of the most significant obstacles to getting a handle on this issue is a lack of transparency in the complex supply chains of many business sectors. Many companies do not know their own investment supply chain past the third or fourth level. One way to address the lack of supply chain transparency is to expand Environmental, Social, and Corporate Governance (ESG) to include national security compliance concerns. Moving forward, more comprehensive monitoring and tracking systems need to be implemented to reduce risk and potential exploitation.

Greater transparency would reduce private sector risk and increase public sector confidence. It requires avoiding two traps that often arise when dealing with the issue of FDI risks: the regulatory trap, where governments become so protectionist that investment and innovation in the technology or defence sectors become impossible; and the innocence trap, which results when the private sector takes on undue risk. Given these two traps, public sector actors ought to serve as a guardrail when determining the optimal balance.

- **Enhancing Competition and Innovation –**

Key insights:

- Small and Medium-sized Enterprises (SMEs) and start-ups still face significant entry barriers when seeking to cooperate with NATO, from access to relevant information to lack of clarity or transparency about procurement processes and a significant delay in the product development cycle.
- Private sector needs fast revenue and no commitments attached to the funding- risk capital - that allows to maintain a technological edge
- NATO could provide more support, either by providing a range of advisory services to SMEs and start-ups or by enabling a customer relationship with interested allied nations
- NATO and private entities should structure future interaction recognizing the value of data as a new asset. NATO could create common data pool – based on open data and other sharing mechanisms – to facilitate training algorithms developed by start-ups and encourage data-based military and security innovations.

Discussion points:

NATO's current efforts to encourage competition and innovation, especially the importance of ACT as well as various NATO advisory groups in this regard, have been acknowledged. Yet, persistent barriers that small and medium sized enterprises (SMEs) and start-ups face when seeking to cooperate with NATO have been pointed out.

Since private actors must fulfill extensive administrative requirements before engaging with NATO, possible improvement areas for NATO-SME interaction include: easier access to information regarding procedures, expectations, and potential payment, a faster and/or more risk-tolerant approach to procurement, an onboarding process that provides clarity regarding long-term expectations and returns, and the ability to test new products.

Participants underlined the importance of creating innovation ecosystems and expressed interest in human capital transfers, which could influence Alliance strategy via the immersion of NATO personnel in start-ups. This type of program may also encourage NATO decision-makers to accept that incurring small risks in the short-term may be unavoidable in order to ensure long-term 'home runs'.

National authorities sometimes limit the focus of NATO efforts to only the most essential aspects of common support and integrating existing capabilities. For this reason, and the fact that the vast majority of funding for

SMEs and start-ups comes mostly from nations themselves, it may be wise for private actors and NATO to focus on engaging further national entities in order to enhance innovation.

A possible new model for enhancing competition and innovation could allow for NATO to be a partner that would connect a given company to interlocutors at the national level, in addition to its role as customer. Using a results-driven approach, NATO could initiate the early stages via small funding that bears no attachment to capital, and the provision of advisors.

Data collection, integration, and standardization was also highlighted as a crucial element to foster innovation. NATO and private entities should structure future interaction recognizing the value of data as a new asset. With this in mind, NATO could create a common data pool – based on open data and other sharing mechanisms – to facilitate training algorithms developed by start-ups and encourage data-based military and security innovations. Collecting as much data as possible and standardizing its format will be essential for this endeavor. Potential access to the data pool would attract engagement from start-ups, which will be important for achieving progress in data source integration and building public-private partnerships. National concerns regarding sharing sensitive data will of course need to be taken into consideration, as well as similar worries expressed by the private actors.