# NATO 2030: NATO-Private Sector Dialogues with GLOBSEC

## Critical Infrastructure and Security of Supply Chains - 22 April

**Policy Takeaways**

NATO, its allies, and the private sector are all facing the consequences of the increasingly complex and global nature of critical infrastructure. The evolving parameters of this landscape, and the tensions this uncertainty raises among NATO allies and companies requires developing a coordinated transatlantic approach. Adequately responding to these challenges will require more extensive and innovative collaboration between the Alliance and the private sector. The sixth 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 decision making on the new challenges in critical civil infrastructure, emerging critical infrastructure, critical dimensions of NATO's military advantage, and the emerging challenges of supply chain security.

### – New Challenges in Critical Civil Infrastructure –

*Key Insights:*

- The long-standing process of the optimization of private sector firms, looking to be "lean and mean', has reduced the ability of firms to absorb shock and bounce back in the face of unpredictable changes.
- Due to economic considerations and the desire to maximize profits, it is common for private sector firms to utilize a single source supplier within their supply chains which has created a dangerous reliance on third parties that is subject to potential weaponization.
- Protecting civil critical infrastructure across the transatlantic sphere must be a shared responsibility in the future between governments and private sector firms that achieves a balance between an acceptable level of security and an acceptable level of costs.
- As the transatlantic community shifts towards an energy transition, based on green technologies, it is critical not to create new dependencies that could be exposed by adversaries.
- While the private sector can assign economic and financial value to concepts like ESG, the same incentivization to pursue innovative solutions and technologies to secure critical infrastructure is currently non-existent that requires more active intervention and leadership from the public sector.

*Discussion Points:*

Participants agreed that a prolonged period of peace and economic prosperity, throughout the Transatlantic community has installed a sense of complacency. This false sense of confidence has been revealed with the Covid-19 pandemic which has exposed the structural weakness of many logistic processes and operations.

Policy makers have never had access to as much data and information as they do now. Despite this perceived advantage, it was asserted that recipients were overwhelmed by the heavy flow of information flow and unable to manage it properly. The current "complexity trap" engulfing government decision makers and private sector actors is a major shortcoming that must be resolved through better management systems to avoid the continuing application of knee-jerk solutions to complex problems.

Although the private sector can assign an economic and financial value to concepts like environment social governance (ESG) when it comes to existing critical infrastructure, it was argued that the same cannot be said more broadly for security concerns. Members of the private sector argued that they are not sufficiently incentivized to pursue innovation in this field, and that there is a lack guidance on the issue from allied governments. The combination of these facts in part explains why many aspects of critical infrastructure across the transatlantic sphere remains vulnerable to attack or inadequately resilient in times of disaster. Furthermore, it was argued that there is a currently an unreasonable financial and administrative burden on corporate interests to sufficiently protect critical infrastructure, where a more sustainable position needs to be reconciled through increased support by governments and NATO. These challenges to critical civil infrastructure include but not limited to physical sabotage, cyber-attacks, as well as third-party hostile takeovers.

From an operational standpoint, in times of crisis NATO must rely on a host of nationally managed civil critical infrastructures facilities, such as airports and ports. While many of these requests to allied governments tend to arrive with little notice, it was argued that NATO should improve its communication of baseline competencies at these facilities to improve planning for an assortment of contingency scenarios. The concept of private facilities providing capacity for a "just in case" scenario for NATO is not financially sustainable. It requires reform and further involvement of allied governments to ensure it remains financially attractive for the private sector.

Moderate up and down cycles of demand that are predictable is a feature that many logistics companies are traditionally able to cope with. In some areas, like maritime shipping, the Covid-19 pandemic has created massive swings in critical demand that many firms did not anticipate. Nor are they able to scale up capacity on such a short timeline. Consequently, NATO should look to help moderate swings, when possible, in critical demands. Underscoring this feature is the valuable role NATO nations play in keeping sea-lines open to ensure the flow of transatlantic and global commerce through adding capacity building to partner nations and increase force presence in volatile regions.

A major threat NATO should not lose sight of is biosecurity and its impact on supply chains. It was noted that transatlantic providers will need to maintain wider and deeper situational awareness of a larger number of potential biosecurity threats like epidemics and pandemics; history has confirmed these threats will not end with the global stabilization of Covid-19. Experts anticipate that major epidemic events of global significance will occur every two to five years, regional disruptions at least annually, and a pandemic approximately every ten years. These threats are disruptive on both the supply and demand sides, interrupting production capacity at every step, and causing difficult-to-foresee spikes in demand. As supply chains move from a "just-in-time" to a "just-in-case" logic, alternative "switching options" will be needed for decision makers, increasing the value of better and earlier warning systems for which NATO has a contributing role to play. Private providers of early warning solutions should be considered a key resource to help NATO corporate partners manage the difficult task of broad situational awareness and be integrated where possible. Intelligence vendors who specialize in a particular threat category can maintain expertise and focus to a degree not possible for institutions responsible for general threat detection and response.

## -Emerging Critical Infrastructure-

*Key Insights:*

- The definition of what counts as critical infrastructure and the ways it can be manipulated and consequently protected has evolved rapidly due to the massive changes in technology and data computing.
- There is a growing tendency within the private sector of subsuming everything into a general ecosystem and understanding how that ecosystem works with other critical features. Interoperability within the ecosystem should constantly be on the agenda – including between the Allies, on the multiple nodes in the critical infrastructure ecosystem.
- There is a need for staying up to date on situational awareness: NATO must be up to date on the current discussion regarding emerging critical infrastructure and when possible, provide a platform for exchange with industries from Allied countries.

*Discussion points:*

The world is going through several paradigm shifts. Importantly, the shock of the Covid-19 pandemic, has placed national resilience and self-reliance squarely on the political agenda. As a result, it also deepened the necessity for NATO to step in, in addition to the efforts done by allied states and the EU. The definition of what counts as critical infrastructure remains in flux.

It was agreed that the evolving scope of critical infrastructure is nowadays considerably broad and depends on the situation and threat. The most important areas of critical infrastructure identified were; data and cloud storage, 4G, 5G, and in future 6G, and their associated data centers, computing infrastructure, AI, intellectual property. Furthermore, physical infrastructure supporting data such as cables as well as quantum elements both hold the potential to disrupt supply chains.

Data can today be classified as a major weapon of the 21st century. There is a surplus of data exchange and governments are not able to effectively manage it. Another area of concern is the comparative disadvantage of Europe with regards to supply chains. At the moment, Europe is not sufficiently aware of its various vulnerabilities. The discussion highlighted the importance to regain autonomy and the need to develop a continental system that would better support national companies.

With regards to critical infrastructure, there is a growing importance amidst the private sector of converging everything into a general ecosystem. Interoperability within this critical infrastructure ecosystem should be considered one of NATO's top priorities. Specifically, the theme of improving interoperability between Allies on the multiple nodes in the critical infrastructure ecosystem should constantly be assessed. Defining and identifying potential critical nodes of our states and societies should be enhanced by increasing cooperation between the private-public sector.

In order to realize better private-public sector cooperation, there is much merit in creating a permanent forum for debate and discussion between NATO and the private sector in order to deepen cooperation. Furthermore, an effective risk assessment system could be a major component of any forum that would allow key providers to share and evaluate risks with NATO. Additionally, there is a need for multidimensional simulation of supply chains. Even though supply chain security represents a concern of national governments, the strategic context and the level of dependencies has changed. It was argued that allies see an added value in using NATO as a forum for discussion, and for sharing of best practices. In this regard, supply chains should be more flexible, dynamic and NATO should encourage a greater variety of suppliers.

## -Supply Chain Security and Security of Supply: Critical Dimensions of NATO's Military Advantage -

*Key Insights:*

- On the procurement side, the public sector should take example from the best practices of industries and not rely solely on one supplier. Having multiple suppliers is an effective way to ensure continuity of business in case of disruption of the supply chain.
- Closer collaboration and coordination between the United States and the European Union on a NATO level is necessary to ensure appropriate interdependencies are in place.
- Security of supply comes at a price. NATO should collaborate with the private sector to make the case to allied governments.

*Discussion points:*

Buzzwords such as insourcing, re-shoring, strategical autonomy and technological sovereignty have become commonplace while discussing the critical dimensions of NATO's military advantage. There needs to be a re-conceptualization of what makes up supply chain security and security of supply. At the present time, there is no agreed definition between NATO's allies on what precisely constitutes supply chain security. It is clear that it involves physical security, procurement aspects and logistics; but the access to the best technology at the best price as well.

Throughout the discussion, participants identified the current reliance on China as one of the biggest challenges to the security of supply. The ability to secure raw materials critical to military technologies while reducing dependence on China was determined to be of utmost importance. Some participants believed the matter could be partly solved by the private sector on an individual basis by adopting a vertical integration within companies. Even in such a scenario, access to raw materials would remain challenging due the unavailability of alternative sources of supply or to current strict US regulations on the use of raw materials coming from the United States.

Furthermore, representatives from the private sector pointed out that even if they were able to source the necessary raw materials from within the Transatlantic region, such a move would result in higher costs. Hence, NATO should play an active role in educating and informing allied governments about the necessity of accepting higher costs to ensure the security of supply for critical materials.

In terms of collaboration, the participants recognized the value of joint public and private dialogue when assessing the challenges and vulnerabilities in supply chain security and security of supply. However, collaboration has not always been effective. A lot of policy work therefore needs to be carried out in order to make sure the public-private incentives align. Similarly, participants believed closer collaboration and coordination between the European Union and the United States is necessary at a NATO level. This collaboration is seen to be essential on matters of R&D where the allies could jointly work on finding alternatives to materials coming from China. Transatlantic coordination in this regard is paramount so as to avoid duplication of the same R&D processes.

The EU and NATO should also cooperate on the assessment of Foreign Direct Investment in European critical infrastructure which has the potential of jeopardizing the security of supply chains. Furthermore, collaboration between allied governments is needed in unifying cross border procedures and requirements to facilitate the transfer of essential materials. A proposed solution to this question is an improvement of already existing frameworks like the Trans-Atlantic Defence & Industrial Cooperation (TADIC) as a way of enhancing the defence industry within NATO.

It would be beneficial for NATO to review its best practices and procedures adopted during the Cold War in relation to the security of supply then. At the time, for example, the security of supply was contractualized. Many bilateral and multilateral procurement MoUs between nations exist to this day. An effort should therefore be made to update them and inform the private sector of their existence.

## -Supply Chain Security – Emerging Challenges -

*Key Insights:*

- NATO and its allies need to commit to harmonizing regulatory systems related to supply chains. The current regulatory heterogeneity is causing uncertainty within the private sector, tensions between allied governments, and confusion within the EU.
- NATO and its allies should diversify their perspectives and investments when it comes to technological innovations relating to supply chains. Although new technologies like 5G may prove revolutionary, tried and true technologies can be re-tooled in innovative ways as well.
- Global supply chains have brought innovation and prosperity to all allied states. NATO, the EU, and other Alliance partners should avoid engaging in economic protectionism by defining critical infrastructure too broadly, because this would ultimately harm both the Alliance and the private sector.

*Discussion Points:*

National level discussions relating to supply chain security often get caught up in larger geopolitical debates. Therefore, it is important that NATO and its allies focus on practical solutions and innovations. This is particularly important because burden sharing is much broader today than it was during the Cold War. NATO should focus its efforts on strategic materials and military planning channels, leaving the development of regulations to the EU and national allied governments.

The current heterogeneity of regulations throughout the Alliance is a weakness because it leaves space for states like Russia and China to play different Alliance partners against one another. This is especially prevalent in strategic industries where dependency on Russian and Chinese goods is high. Participants from the private sector voiced their full support for increased regulatory harmonization between NATO and the EU and mentioned that new regulations are already exposing companies to increased legal liability. These participants from the private sector did not question the validity of this increased scrutiny, but rather highlighted that a clearer and streamlined regulatory system would be welcomed.

Many current supply chains remain efficient and work well. A number of participants cautioned NATO and allied governments against defining critical infrastructure too broadly. Although there will always be tensions on how to define critical infrastructure, NATO and its allies should not fall into the trap of allowing security precautions to become cover for economic protectionism. This kind of protectionism, like the US regulations regarding semi-conductors, can have unintended consequences that create tensions within and damage the Alliance. Rather, the standard for critical infrastructure should be a small yard with a high fence.

In addition, innovation does not only come from new technologies, but also from using older technologies in innovative ways. For example, it is now possible for private actors or SMEs to produce parts and machines that were previously only made by states or massive corporations. Furthermore, data process mining, graph technology, and risk event streams were brought up as being particularly promising new technologies.

Although these developments also have their drawbacks and complications, most participants agreed that emerging technologies are a net positive for ensuring supply chain security now and in the future. It is important for both NATO and the EU to highlight the positive role those emerging technologies like 5G can play in securing supply chains. Highlighting these positives would help alleviate fears.

Participants also noted that national authorities focus on state risks, which means that crime and theft which plague the private sector are often overlooked. However, there is a spillover of risk. When criminals tamper with supply chains, this impacts national security. The weaknesses that allow criminals to take advantage of supply chains will also allow potential adversaries to use criminality as a cover for their own ends. This aspect of supply chain security needs to be addressed more head on by allied governments.