GLOBSEC
IDEAS SHAPING THE WORLD

GLOBSEC
Vajnorská 100/B
831 04 Bratislava
Slovak Republic
+421 2 5441 0609
info@globsec.org
www.globsec.org

Public-Private Dialogue series

'Enhancing NATO's Cyber Resilience"

Date: 29th January, 15:00 on Zoom

Policy Takeaways

Evolving Cyber Threat Environment due to Geopolitical Changes:

- Changes in the geopolitical landscape – included but not limited to Russian cyber activities in Ukraine and spillover effects in North America and Europe - are contributing to an increasingly volatile environment in cyberspace.

Global Cooperation in the Technology Ecosystem

- As technologies like Artificial Intelligence transform the economy and security landscape, it brings both opportunities and challenges – especially when it comes to potential misuse by adversaries.
- Focus should be on creating a secure cyber environment which means acknowledging the risks associated with AI and other emerging technologies and actively cooperating on a global level to ensure the safe and responsible development and use of these technologies

Pressing Need to Enhance Cyber Resilience

- Focus on enhancing cyber resilience to better withstand and recover from cyber threats
- Nurturing public-private partnerships for scaling effective monitoring and detection of cyber threats
- Advocating for the exchange of threat intelligence and best practices through early warning systems

Group 1: *How has the cyber threat landscape evolved in the past decade and what are the immediate vulnerabilities that NATO faces in this regard?*

Address uneven cybersecurity capabilities across NATO Member States

- There is glaring gap with respect to levels of Information Technology systems deployed across NATO Member States
- This poses a significant problem to the overall cyber defence posture and effective coordination within NATO to tackle cyber threats

Develop Comprehensive Cybersecurity Regulations

- Nations should establish robust regulatory frameworks focusing on resilience and interdependencies across both public and private sectors.
- These regulations should extend beyond government directives to include self-regulation, guided by a unified goal of achieving common security.

GLOBSEC
Vajnorská 100/B
831 04 Bratislava
Slovak Republic
+421 2 5441 0609
info@globsec.org
www.globsec.org

Invest in Technological Modernisation

- Modernize military and defence technologies to ensure that new capabilities are supported by advanced IT, network, and software security.
- This step is critical to protect against the increasing sophistication of cyber threats.

Enhance Military Education and Training

- Implement comprehensive training programs for military leaders and personnel to understand and effectively utilize cyber capabilities.
- Education should focus on the operational and legal aspects of cyber warfare

Prioritize Protection of Communication and Early Warning Systems

- Ensure the security of critical systems such as communication networks, early warning systems, and logistics infrastructure against potential cyber-attacks.

Foster Public-Private Collaboration

- Strengthen collaboration between the public and private sectors in cybersecurity initiatives. This collaboration should focus on intelligence sharing, joint defence mechanisms, and coordinated responses to cyber threats.

Adapt to the Permanence of Cyber Threats

- Acknowledge and prepare for the ongoing nature of cyber threats, recognizing that the cyber domain is a constant battleground rather than a peacetime environment.

Group 2: *What are the key factors or challenges that influence effective collaboration between NATO, the EU and private sector entities in countering cyber threats and how can these partnerships be strengthened?*

Commercialization of Public-Private Exchange

- Promote commercialization of public-private collaboration through a format akin to a NATO center for exchanging civil-military information on threat intelligence.

Diverse Approaches to Information Sharing

- Acknowledge that information sharing can be intimidating and recognize the absence of a one-size-fits-all approach.
- Stress the importance of trust and the necessity for broader cooperation in the public-private alliance.

Establishing a NATO Platform for Private Sector Engagement

- Advocate for the creation of a platform or center within NATO where the private sector can engage and collaborate.
- Address the issue of trust within the mutual public-private alliance by institutionalizing the relationship.

Focus on Civilian Sector Cooperation

- Highlight limitations in actual cooperation with the private/civilian sector due to a lack of common ground for sharing classified information.

GLOBSEC
Vajnorská 100/B
831 04 Bratislava
Slovak Republic
+421 2 5441 0609
info@globsec.org
www.globsec.org

- Address the challenge NATO faces in building trust with civilian entities, exploring ways to measure concrete results within the NATO framework.

Potential for a Joint EU-NATO Center:

- Consider the establishment of a joint EU-NATO center/platform for threat intelligence sharing.
- Analyse existing political roadblocks and identify mechanisms to overcome them.

Critical Infrastructure Protection

- Stress the importance of critical infrastructure protection within both EU and NATO, focusing on energy grids and ocean bed cables.
- Propose a NATO cyber defence pledge to establish order within NATO infrastructure and utilize the collective knowledge of allies effectively.

Solutions and Ideas: Enhancing Trust and Collaboration

- Advocate for creating platforms to enhance trust and collaboration.
- Highlight the abundance of information as a challenge and suggest drawing lessons from transparency efforts in Ukraine.

Innovative Approaches Outside EU-NATO Framework

- Propose solutions outside the EU and NATO framework to avoid regulatory roadblocks.
- Suggest the creation of a cyber defence platform to bring public-private sectors together on the defence agenda.

NATO's Role in Cybersecurity

- Emphasize the importance of not overburdening NATO with tasks already addressed by others, such as the EU.
- Encourage NATO to plan potential military operations enhanced by cyber enablers and explore possibilities for sharing more classified information.

Balancing Transparency and Security

- Identify the need for a balanced approach to information sharing.
- Emphasize transparency about points of contact and ensure agility in mechanisms for effective collaboration.