European Cyber Agora:
The Role of the Private Sector during Hybrid Conflict

This workshop on the role of the private sector during hybrid conflict addressed the need to foster shared responsibility and collaboration between the private and public sectors to ensure security when hybrid threats, including cyberattacks targeting critical infrastructure and essential services, occur.

The discussion, which convened a total of 46 attendees from the public and private sector, industry associations, consultancy firms, NGOs and academia, addressed these questions:

- How to enhance public-private cooperation, common responsibilities and coordination?
- How to reinforce the concept of “trusted providers” and what are the risks when companies become trusted providers?

The shortage of “cyber talents” as a current key issue

To ensure responsiveness from the private sector and smooth coordination with the public sector in times of hybrid threats, one of the most pressing issues is the shortage of "cyber talents," which impacts both the public and private sectors. Several factors contribute to this shortage, including inadequate stakeholder cooperation, a lack of standardized skill frameworks, limited training resources, and insufficient interest in cybersecurity among the general population.

Some proposed solutions to address this gap include enhancing existing training programs, improving certifications, and facilitating access to workshops to build and upskill the cybersecurity workforce. Organizations may also explore outsourcing or collaborating with external providers to supplement internal capabilities. This approach, drawn from experiences such as those in Ukraine, can be vital in responding to immediate threats and achieving short-term cybersecurity goals. Establishing minimum requirements for cybersecurity training and certifications could encourage broader participation.

The benefits of closer cooperation

Closer cooperation between the public sector and large-scale companies, especially within their cybersecurity ecosystems, could be mutually beneficial **for three primary reasons**:
(1) collaborating with large companies allows the public sector to tap into their extensive talent pools, strengthening cybersecurity capabilities; (2) by engaging with large-scale companies, the public sector can effectively monitor the activities of chosen IT providers, ensuring compliance and security standards are met; and (3) this collaboration provides valuable insights into emerging strategies for addressing hybrid threats, enabling proactive responses.

Trust is key to bolster closer cooperation between the two sectors

When addressing hybrid threats, one of the main challenges from the private sector is the **diversity of certifications,** which complicates partnerships between public and private sectors. Streamlining certifications is essential to foster trusted collaborations. Clear communication of such directives by the public sector, along with guidance on implementation, is vital for private sector understanding and compliance. Many organizations are unaware of cybersecurity directives, or possibly hesitant as implementing measures require substantial investments. To build trust, the public sector must **establish clear regulations and minimum requirements** that align with private sector capabilities and expectations.

Another current limitation to addressing public-private cooperation in hybrid threats is the **limited trust** among national authorities of EU Member States, as well as rivalry between regulatory and technical authorities. Implementation issues also arise at decentralized levels, particularly among regional administrations. Overcoming distrust requires more than just certifications. While certifications may work at the state level, they must be strengthened for cross-border cooperation. **Joint exercises and simulations** can facilitate information exchange and prepare both sectors for real-world incidents, helping to bridge gaps and understand the hybrid nature of threats. Implementing joint exercises, akin to military practices, can be beneficial to enhance preparedness. Recent events in Ukraine have highlighted the public sector's increasing reliance on the private sector for national defense.

Changes in the cybersecurity landscape and resulting impact

Organizations now find themselves in a frontline role, actively engaged in cybersecurity defense and potentially involved in conflicts. While the state retains a central role in the monopoly of the use of force, there is a **growing expectation that the private sector contribute to national defense efforts**.

The results of these changes include, firstly, a notable **shift in language from defense-centric approaches to emphasizing resilience**. The focus is on ensuring that organizations can withstand and recover from cyber incidents even if they cannot completely prevent them. Furthermore, there is increased **demand to hold threat actors accountable and enhance deterrence measures**. Efforts are directed towards addressing root causes of cyber threats and incidents. Finally, companies are now confronted with significant geopolitical challenges not traditionally within their purview. This requires organizations to adapt quickly to navigate complex international landscapes and emerging threats.

Best practices from certain countries and sectors

The German Cyber Security Directorate has established trusted relationships by setting up **frame contracts with certified partners**. Entry into this scheme as an IT security provider is rigorous, ensuring high standards of expertise and reliability. All departments can access external support through this network, which is exclusively open to certified companies and personnel.

The British NCSC's i100 initiative exemplifies public-private collaboration. Private sector participants undergo vetting and are then embedded within government entities for one day a week or month. This arrangement enables institutions to tap into specific skills from the private sector, and public sector

participants benefit from enhanced information access and networking. The initiative includes foreign companies like Fujitsu, fostering broader collaboration and knowledge exchange.

It is crucial to avoid backdoor contracts, particularly considering geopolitical implications such as the Huawei debate in Germany. Many companies (especially in the aerospace sector) have global markets, including substantial sales in China, necessitating careful consideration of technology trends, principles like the "zero trust" approach, and individual accountability in cybersecurity practices.

About the European Cyber Agora

The European Cyber Agora (ECA), an initiative led by the German Marshall Fund, Microsoft and the EU Cyber Direct project at the EU Institute for Security Studies, is a multi-stakeholder platform bridging the gap between government, civil society, and industry across the EU to shape the European technology and cybersecurity policy agenda and identify European perspectives on global cybersecurity policy debates. It promotes collaboration across sectors including diverse voices and contributes to evidence-based policymaking through research-driven and stakeholders' engagement oriented to deliver practical outcomes. Since 2021, the European Cyber Agora has demonstrated the need for a dedicated European platform to leverage multistakeholder input in EU policymaking. In 2024 the ECA community and partners will convene throughout the year in four different workstreams tackling issues that include: 1) the future of multistakeholder cyber diplomacy, 2) taking stock of the EU cybersecurity policy, 3) AI, transatlantic alignment and geopolitics, and 4) the role of the private sector during hybrid conflict. The European Cyber Agora will also convene in Brussels at its 4th Annual Conference on 23-24 April 2024.

About GMF

The German Marshall Fund of the United States (GMF) is a nonpartisan, nonprofit, transatlantic organization headquartered in Washington, DC, with offices in Ankara, Belgrade, Berlin, Brussels, Bucharest, Paris, and Warsaw. GMF envisions a democratic, secure, and prosperous world in which freedom and individual dignity prevail. GMF strives to champion democratic values and the transatlantic alliance by strengthening civil society, forging bold and innovative policy ideas, and developing a new generation of leaders to tackle global challenges. GMF delivers hope by upholding the dignity of the individual and defending freedom in the spirit of the Marshall Plan.