Shaping Cybersecurity Conference 2023:

Cyber in Conflict – Supporting Partners and Avoiding Escalation

The second iteration of the Shaping Cybersecurity conference took place on June 19 at the European School of Management and Technology Berlin. Hosted by the German Foreign Office, the Institute for Peace Research and Security Policy, and the Digital Society Institute, the conference brought together cyber experts and practitioners from government, business, and academia. The main focus of the conference was to advance the discussion on "Cyber in Conflict - Supporting Partners and Avoiding Escalation".

Given recent developments, the importance of cybersecurity is increasing, and there is a pressing need for critical reflection on effective prevention and conflict management tools among like-minded partners. The cyberattacks and information operations accompanying the Russian invasion of Ukraine have demonstrated the disruptive potential of digital technologies beyond the immediate conflict zone. Even before the war, criminal cyberattacks against critical infrastructure posed significant national security threats, exacerbating geopolitical tensions with tacit or active state support. Therefore, the conference aimed to share lessons learned, exchange experiences, and stimulate new ideas on effective policies in an era of rapid technological change and growing geostrategic competition.

The conference commenced with opening remarks by Melissa Hathaway, former Cybersecurity Advisor to President Obama, who discussed the current impact of cyber conflict and its future development. She emphasized that nation states' disruptive and destructive activities in cyberspace are increasingly motivated by various factors, leading to potential escalation and miscalculation. Following, two panel discussions delved into international security, technological disruption, and the formulation of effective cyber responses for future conflict scenarios.

The first panel, titled "International Security in an Era of Technological Disruption," featured experts from the military, academia, NGOs, and diplomacy who explored how cyber and AI are shaping the nature of future conflicts. They examined the impact of cyber on the situation in Ukraine during the Russian invasion and drew key lessons from cyber warfare. It is crucial to highlight that the war in Ukraine had already begun in cyberspace before physical conflicts escalated, although these cyber warfare activities are less apparent than conventional military movements. Since the war started, cyberattacks have significantly increased not only in Ukraine but also throughout Europe. However, it became evident that kinetic attacks, such as physical military actions, are still more effective than cyberattacks. Cyberattacks could be employed by aggressors in conjunction with other means to undermine democratic processes and erode civil society. In this context, AI can have a disruptive impact.

Nonetheless, experts also highlighted that AI brings not only risks but at the same time new opportunities. Therefore, it is vital to explore these new opportunities and not solely focus on potential risks. For instance, Ukraine has utilized AI for intelligence purposes and cloud storage to safeguard its data, underscoring the importance of innovation as a source of power. Ukraine's ability to leverage innovative approaches has played a significant role in its resilience. The involvement of the private sector, including threat intelligence companies, further emphasizes the significance of public-private partnerships in addressing cyber challenges. Additionally, agility in adopting innovation is crucial, not only within the military but also as a society that embraces a culture of learning.

Since innovation plays a key role in gaining a cyber advantage cooperation among EU member states and other like-minded countries, along with public-private partnerships, is essential, as is investing in relevant education to drive innovation. Stakeholders from the public and private sectors, as well as civil society, should collaborate to harness the potential of new technologies. Additionally, cyber capacity building (CCB) is crucial to enhance resilience and promote the implementation of existing rules and norms in cyberspace.

The second panel focused on "Effective Cyber Responses for Future Conflict Scenarios" and addressed potential approaches to react to, deescalate, and prevent cyber incidents. The role of cyberspace poses a new challenge for strategic stability, rendering traditional concepts like deterrence unsuitable in this domain. Panel experts emphasized the necessity of communication channels between like-minded states and other actors, with the OSCE serving as a crucial platform for such dialogue. Confidence-building measures (CBMs) form the foundation for establishing a common understanding, such as defining red lines and determining actions and reactions in cyberspace. Nevertheless, the nature of cyberspace presents unique challenges, particularly regarding information sharing. It is vital to involve the private sector in these communication structures due to their critical role. Moreover, attribution also plays a significant role in communicating violations of norms, requiring coordinated response behaviors. However, the rapid development of capabilities and innovations in the cyber domain poses immense challenges in this regard. The Cyber Diplomacy Toolbox offers response options, which should continue to be developed by the EU and supplemented with sensitive and effective sanction mechanisms. Further, coordinated response processes must be expedited, potentially involving the private sector, which possesses vast amounts of relevant data. Cybersecurity exercises can also contribute to preparedness for real-life emergencies. Additionally, regulations play an essential role in enhancing resilience.

Throughout the conference, participants engaged in three thematic workshops that delved into various cyber issues through interactive activities. The workshop on "Prevention, De-Escalation, and Post-Conflict Stabilisation," organized by the Digital Society Institute, examined challenges and solutions for managing conflicts in the digital domain. Participants immersed themselves in a cyber crisis scenario, assuming roles such as the attacked/attacking country, the private sector, the global community, or civil society. One key takeaway was the importance of communication

between stakeholders during a cyber crisis to find ways to de-escalate tensions. Given the transnational nature of cyber issues, a multi-stakeholder approach proves most effective in preventing and managing confrontations.

The workshop on "Capacity-Building and Emergency Assistance," conducted by the Institute for Peace Research and Security Policy, emphasized the urgent need to enhance cooperation and capabilities through a multilateral approach. This workshop stressed the significance of strengthening alliances, involving more countries, promoting transparency, establishing acceptable legal frameworks, and facilitating communication.

The final workshop, "Strengthening International Law," conducted by the German Foreign Office, explored the creation and reinforcement of legal frameworks for cyber conflict at the international level. The workshop addressed legal issues based on three scenarios and developed recommendations for governmental actions.

The conference concluded with a reflection on the workshop outcomes and closing remarks by Dr. Regine Grienberger, the German Cyber Ambassador. The Shaping Cybersecurity Conference 2023 successfully convened cyber experts and practitioners from around the world. Through panel discussions and interactive workshops, the conference covered a broad range of cyber topics related to security and diplomacy, facilitating valuable exchanges of experiences. The keywords can be highlighted to sum up discussions: resilience, agility, and innovation. Thus, participants emphasized the need to foster trust in the international arena when addressing cyber issues and highlighted the importance of promoting capacity-building activities. While cooperation among like-minded partners remains crucial, the global geopolitical competition requires dialogue with diverse actors representing different perspectives. In this regard, the role of the private sector in cyber defense and infrastructure was also highlighted, exemplified by the ongoing war in Ukraine.

The rapid evolution of cyberspace demands a sense of urgency to work together more efficiently and expeditiously. Therefore, it is essential to build a community, cultivate expertise and capabilities, and strengthen cooperation. The implementation of existing rules and norms is of utmost importance, as cybersecurity should be viewed as part of a broader picture rather than just a technical endeavor.