Cyber Security Roundtable Berlin
November 6, 2017

Summary Report

What are the current shortcomings of the EU legislative agenda and policy debate on cybersecurity? Is Europe sufficiently prepared to deal with cyber aggression by third countries and which instruments should Europe develop to respond to large-scale cyber-attacks? How can the political deadlock in the cyber norms process between Western "like-minded" states and Russia/China be overcome? And how is technology impacting geopolitics and how is geopolitics impacting technology? These were some of the crucial questions that were discussed at the MSC Roundtable on Cybersecurity on November 6, 2017 in Brussels.

The MSC Roundtable on Cyber Security was co-hosted with Microsoft at the Microsoft Center in Brussels. John Frank, the Vice President for EU Government Affairs at Microsoft, and Wolfgang Ischinger, the Chairman of Munich Security Conference, opened the Cyber Security Roundtable with initial remarks before the participants discussed the future of cybersecurity in Europe as well as the path forward in the international cybersecurity norms discussion. The event finished with a public fireside chat and an off-the record formal dinner.

Participants of the MSC Cyber Security Roundtable included **Michele Markoff** (Acting Coordinator for Cyber Issues, U.S. Department of State), **Heli Tiirmaa-Klaar** (Head of Cyber Policy Coordination, European External Action Service), **David Koh** (Deputy Secretary for Technology and Special Projects, Ministry of Defence, Republic of Singapore; Chief Executive, Cyber Security Agency), **Iddo Moed** (Cyber Security Coordinator, Ministry of Foreign Affairs, State of Israel), **Ludwig Leinhos** (Lieutenant General, Chief of Staff of the Cyber- and Informationspace Command, Federal Armed Forces of the Federal Republic of Germany), **Udo Helmbrecht** (Executive Director, European Union Agency for Network and Information Security), and **Sorin Ducaru** (Ambassador, Assistant Secretary General for Emerging Security Challenges, North Atlantic Treaty Organization).

The Future of Cybersecurity in Europe

Participants agreed that significant steps had been taken in recent months to strengthen the cybersecurity regime in Europe, such as the EU's Cybersecurity Act. However, there continues to be a significant amount of fragmentation - Europol, the European Defence Agency, the European Union Agency for Network and Information Security, to name just a few of the "big players" in the institutional landscape at the European level. Another impediment for further steps at the European level, participants stressed, were different

levels of maturity in terms of cybersecurity between the member states. As a result, better common standards represent a prerequisite for successful collaboration at the European level, according to some participants.

During the discussion sessions, the participants also debated the role of public-private partnerships in the realm of cybersecurity. Participants acknowledged the significant potential of such partnerships, as private companies are currently more advanced and poss than state agencies and own a large part of critical infrastructure, including critical software and programs. However, they also noted potential challenges, such as the need for the sharing of sensitive information between companies and organizations like NATO.

All participants agreed that NATO and EU collaboration had improved over the past few years. The speed of cooperation, common exercises, and information sharing were some areas where progress had been achieved. Going forward, some participants mentioned the need for common or at least coordinated "playbooks" for cybersecurity.

Charting a Path Forward in the International Cyber Security Norms Discussion

The international discussion on cyber norms experienced a backlash this year when the UN's Group of Government Experts could not agree on a report on how to move forward. Cyber norms are increasingly important, as cyber-attacks increase in number and scale, and as there are only few treaties and agreements in place that regulate cyber space.

Interpretations as to what that means for the cyber norms process differed between participants. Some stressed that the lack of agreement was "business as usual" and that this did not mean that the important political and diplomatic process towards the formulation of cyber norms had come to a halt. Others emphasized that the cyber norms discussion at the UN level had not primarily failed due to inherent differences between states on what norms are but rather because general disagreements (e.g. role of international organizations, global trade, climate change) and tensions in the international community are increasing.

How should the process be moved forward? Some of the experts present at the roundtable noted that a parallel approach rather than a consecutive approach might be more fruitful. Rather than building on previous agreements in cyber norms, different cyber norms processes – be they regional, non-state or bottom-up – should be supported simultaneously. Agreements might be reached in these smaller formats, which might then lead to agreement in larger formats later on. Others argued that the international community should use the current moment as a "strategic pause" in the cyber norms process and rather focus on raising awareness in countries that are currently not significantly involved in the cyber security process. Finally, some discussants argued that the cyber norms process will always, by definition, lack behind cyber security practice: The pace of politics was very different from the pace of practitioners, and the cyber norms process served primarily as a forum for discussion on cyber security rather than the concrete formulation of cyber norms.

After the two discussion sessions, the Microsoft Center opened its doors to the public and welcomed more than 100 participants for a public discussion session on: “Tinker, Tailor, Soldier, Cyber: Technology’s Role for International Security and Diplomacy”. John Frank of Microsoft and Wolfgang Ischinger of the Munich Security Conference discussed the impact of technology on international relations. The Roundtable closed with a formal dinner at the Representation of the Free State of Bavaria in Brussels.