Cyber Security Summit 2014 – Documentation

Panel discussion:
Recent Developments in Cyber and Information Warfare

Cyber attacks are increasingly being used in military conflicts. The current developments in this area, and the ways they are being handled politically, were the focus of the panel discussion "Recent Developments in Cyber and Information Warfare." The panelists for the discussion, which was moderated by Georg Mascolo, were Sorin Ducaru (Assistant General for Emerging Security Challenges, NATO), Elmar Brok (Chairman Foreign Affairs Committee, European Parliament), Christopher Painter (Coordinator for Cyber Issues in the U.S. Department of State) and Karl-Theodor zu Guttenberg (Chairman Spitzberg Partners LLC).

In their introductory statements, the panelists outlined the extent of the phenomenon of cyber warfare. It quickly became clear that there is no generally accepted definition of the term. "We are seeing a growing mix of very different methods of warfare," Sorin Ducaru noted. The existing definitions and differentiations – between kinetic and non-kinetic attacks, state and non-state operations, and high-tech and low-tech methods – no longer apply. "Military cyber attacks are now designed to enable attackers to deny any responsibility," explained Ducaru. With respect to the relevant NATO mandate, the ambassador stated that it is limited to defense aspects. It is focused on establishing effective defense structures that can ward off attacks. Information manipulation is a current trend, he added. This phenomenon reaches even into social media, which are used for the purpose of influencing public opinion, he noted.

Brok: A lack of trust in partners

Elmar Brok discussed the issue of hybrid warfare and confirmed that it also includes propaganda and misinformation. He called the attack on Estonia in

the year 2007 the most serious and clearest case of such warfare to date. A series of denial-of-service attacks led to the failure of national Internet services of the Estonian parliament, as well as of banks, ministries and broadcast stations. Brok noted: "countries and companies are increasingly dependent on IT, and this is making them more and more vulnerable and subject to manipulation – to the point at which their infrastructure can be paralyzed." Brok identified a lack of trust in partners as one of the difficulties encountered in cooperating at the international level. Currently, a total of 140 countries are developing their own strategies against cyber warfare. At the European level, this fragmentation needs to be overcome, he urged. Common standards are needed, he added.

Zu Guttenberg: Confusion about responsibilities

"We see a great deal of confusion about responsibilities – at the national, European and even multinational levels," Karl-Theodor zu Guttenberg noted, in criticizing the current political handling of the issue of cyber warfare. While information war per se is nothing new, the actors and tools now involved in it are new, he added. We thus need to look at the extent to which archaic concepts are being paired with state-of-the-art technologies. As an example, Guttenberg mentioned the approach of the ISIS terror organization, which flexibly uses social media for a wide and diverse range of goals – from intimidation with gruesome images to reports for donors and to recruiting. With regard to countermeasures, Guttenberg called for intensified information exchange between countries, also in cooperation with industry. Companies such as Google could be of use in evaluating propaganda strategies in the network, he added.

Painter: Worldwide, great awareness about cyber security

After Georg Mascolo praised the U.S. government for its handling of ISIS in the Internet, especially its rapid deletion of decapitation videos, Chris Painter emphasized how important freedom of speech is in the U.S.. However, freedom of speech cannot mean that such messages must be allowed to

remain in the network, he added. Not every deletion was initiated by the U.S. government, he pointed out. Companies such as Facebook, Google and Twitter have their own criteria and handle accordingly. "Terrorists move in cyberspace in order to obtain financing or prepare attacks. Those are actions that one can detect and at least block to some extent," Painter said. Worldwide, at the highest political levels, he noted, there is now very good awareness about cyber security issues. This provides a good basis for multinational cooperation – for example, in efforts to counter botnets. In the U.S., there have been denial-of-service attacks against financial institutions, for example. The relevant bots were distributed over more than 100 countries. The U.S. government then successfully initiated cooperation at the diplomatic level. A great deal was also achieved in the UN framework. The UN agreements in the area of armed conflicts now also extend to cyberspace, he pointed out.

Ducaru: International law also needs to apply in cyberspace

Following the panelists' opening presentations, Georg Mascolo opened up the floor for questions. The panelists largely agreed with a critical remark that was made to the effect that instead of trying to design new definitions and structures especially for cyber warfare, we need to make better use of the existing structures. "We need to ensure that international law also applies to cyberspace," Ducaru said. Karl-Theodor zu Guttenberg commented that no institution currently covers offensive components. In addition, he added, exchanges with countries such as China, India and Brazil should be intensified, but a suitable platform for such exchanges is still lacking. A discussion of legal standards ensued regarding the issue of whether the creators of Stuxnet violated Article 1 of the Geneva Convention. This again highlighted the difficulty of categorizing military cyber attacks and their consequences in the context of the existing political framework.

Finally, the panelists identified a lack of a common understanding of exactly what cyber security is as a central problem in institutionalizing protection against cyber attacks. In the coming years, they agreed, we will need to work

to eliminate mistrust and build cooperation. Chris Painter proposed that stakeholders learn from existing nonproliferation strategies. Such strategies have enabled countries to come together in the face of the nuclear threat and to agree to refrain from, and sanction, certain actions, he pointed out. A similar type of approach could work for cyber warfare, too, he added.