Cyber Security Summit 2014 – Documentation of the working groups

Working Group 2: Cyber Governance – The State of Play and the Road Ahead

Cyber incidents have become a major threat for the political, social and economic systems of entire countries and regions. Governments, agencies and companies are thus called on to work together more closely on prevention and defense. The internationally staffed CSS Cyber Governance working group urged that existing agreements and procedures be used more intensively; this would make it possible to address these issues more quickly. In addition, the workshop participants welcomed the proposed Directive on Network and Information Security that the EU Commission presented in 2013.

Directive on Network and Information Security (NIS)

The working group supports the central requirements that the NIS Directive would impose. Among these are that every Member State should establish, and adequately fund and staff, a national agency for cyber security. In addition, the directive would create a mechanism for cooperation between Member States for the purpose of exchanging early warnings, EU-wide, on security risks and cyber incidents. The directive would also obligate operators of critical infrastructures (energy, finance industry, health care and transports), operators of central Internet services (especially app stores, cloud computing, e-commerce, payment services, social networks and search engines) and public administrations to introduce suitable methods for managing cyber risks and to report major security incidents.

Making use of existing standards

In light of the great many interest groups that need to be integrated, there cannot be any globally valid patent remedy for all cyber governance issues. This was a majority opinion of the working group. A relevant international agreement would require 20 years to be negotiated, ratified and implemented. In light of the rapidly growing challenges, several working group participants urged that cyber governance be divided into sub-areas for which it would be

easier to get stakeholders together. That said, the extent to which existing standards, regulations and agreements can also be applied to cyberspace must always be reviewed. As an example, the workshop discussed cybercrime as a criminal law issue. The working group noted that about 120 countries are now using the "Budapest Convention on Cybercrime", which was developed by the Council of Europe, as a guideline for their national legislation in this area. The Council of Europe has also achieved real successes in the area of data privacy. For example, the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (Convention No. 108), which was introduced in 1981, has been adopted by numerous third countries in addition to the member countries of the Council of Europe. Both agreements – the Budapest Convention and Convention No. 108 – have shown, according to the working group, that existing regulations can be used, pragmatically, as guidelines for establishing internationally comparable levels of protection.

The role of industry

A number of workshop participants highlighted industry's responsibility for the proper functioning of cyber governance. Hardware and software producers, and infrastructure and services providers, should be required to close identified security gaps quickly. In addition, according to the group, security and data privacy need to become key design principles in product development. In this way, security management will not only support threat prevention and protection, it will also become a central competitive advantage – both in marketing of secure technologies and in development of new business models.