Cyber Security Summit 2014 – Documentation of the working groups

Working Group 1: Digital Defense – From Prevention to Resilience

Germany continues to be a popular target for industrial espionage. The numbers of digital attacks are constantly increasing, and hackers' strategies are constantly becoming more sophisticated. This trend cannot be completely stopped. The participants thus discussed measures for keeping attacks within certain limits.

Economics no longer respects national boundaries. Most production and supply processes have long since become globally interconnected. The working group participants thus consider it neither possible nor useful to try to isolate relevant data traffic with the help of national domains. Instead, means and ways of reducing espionage activities via the World Wide Web need to be found.

How then can we move from prevention to greater resilience? The discussion participants identified three main areas of action: "people – policies – technology." With regard to "technology", there was agreement that the relevant technologies, while now highly developed and mature, still need to be expanded and upgraded.

The participants saw a clear need for action in the area of "policies." Information exchange between individual companies, between nations and between companies and the political sector is still underdeveloped. In the view of the participants, the aim must be to intensify international communication of national data privacy and security activities and then, ultimately, to harmonize such activities. Internationally binding regulations and standards in this area would be desirable, they added.

They also saw a need for efforts to prepare people for cyberspace. "Digital citizenship" is still underdeveloped; all too often, people are unaware of the opportunities and risks of the digital world and are too careless in the way

they move in cyberspace. Many companies also need to catch up. In addition to regularly updating their existing security applications, they need to carefully analyze what company information especially needs to be protected. The participants saw another problem in a lack of IT specialists. Furthermore, companies today are especially called on to sensitize their employees to IT security and data privacy issues. The recommendation is for awareness and risk management to be enshrined at the top levels of companies.

In summary, the participants agreed that there is no such thing as absolute security in the Internet age. Nonetheless, policy makers and companies alike should routinely address IT security and data privacy issues – focusing on such issues should become just as routine as using safety belts in cars is. While such a focus will not prevent "accidents", it certainly can considerably reduce their consequences.