Second Cyber Security Summit, November 11, 2013 in Bonn

Final communique

On November 11, the Cyber Security Summit was held for the second time in Bonn at the invitation of the Munich Security Conference and Deutsche Telekom. Since the first event in 2012, the subject has not lost any of its relevance – on the contrary. While the first summit was dominated by the issue of cybercrime, the current allegations of espionage by foreign intelligence agencies meant that this year we had to extend our agenda to include issues such as digital industrial espionage and an apparently groundless mass spying by intelligence services. After all, this new aspect of cyber security raises key questions for the future of business, politics and society. It's not just about trust as a basic requirement for the acceptance and use of digital services that are essential to business and society, it's also about morals, ethics and respect for the right to informational self-determination. In short, it's about what kind of digital society we want to live in.

Unsurprisingly, the discussions consistently revealed that there is no desire for a digital society of transparent citizens, whose freedom to make decisions and act is curtailed not only by criminal attacks on personal rights, but also increasingly by state surveillance. Near comprehensive surveillance of electronic communications, regardless of whether or not a specific suspicion exists, is rejected – even when the aim is counter-terrorism. No conflict of objectives was seen to exist between freedom and security: freedom without risk is just as impossible as total security. A balance must be struck in the virtual world between these two legally protected rights; any interference into the individual right to informational self-determination in favor of collective security must adhere strictly to the principle of proportionality.

The huge loss of trust resulting from the current spying affair damages society and the economy. That is why we now need comprehensive clarification as quickly as possible about the extent of state surveillance in cyberspace. At the same time, we must look forward and in the medium term launch an international, binding framework for cyberspace based on trust, transparency and cooperation. An agreement of this kind that also comprehends the right to informational self-determination and the protection of personal data, must form the basis for a digital security culture.

To make cyberspace secure, nothing must be unthinkable. The possibility of a Schengen routing, for example, must be considered with the objective of a legal regulation under which pure data traffic solely within the Schengen Area would no longer be permitted to leave those borders. Data traffic in a legal domain should remain within that legal domain without impeding the achievements of a free global Internet. The same applies for a legal regulation that would only permit the processing of connection data within the Schengen Area in the future. The intention

is not to isolate an area of the Internet, but to implement measures that would make strategic communications intelligence more difficult for foreign intelligence services to obtain and would strengthen the region as a hub of ICT.

But in clearing up and dealing with the PRISM and Tempora affairs, we must not let up in the fight against criminal activities in cyberspace. Cybercrime is now a global threat, with huge implications for the economy, politics and society. Cyber criminals are increasingly involved in organized crime, have immense financial resources and, at little risk and with minimum effort, can cause the greatest possible damage. We have to ask ourselves if we are doing enough at present to counteract these threats.

At this year's Cyber Security Summit, top managers from German companies and top politicians discussed challenges and solutions in all areas of cyber security. It clearly emerged that there is a need for a shared discourse and consensus between society, politics and business. It was also apparent that there is a desire to hold this discourse not only about the risks and threats, but also about the opportunities and potential of cyber security and to embed them in an overall strategy. The following proposals were put together to lay the right foundations for greater security in cyberspace:

Raising awareness

Summary: All participants attached great importance to the issue of raising awareness. We need to systematically exploit the heightened public awareness of the risks in cyberspace resulting from the spying affair, so as to further raise awareness of risks and prevention, but also of the opportunities of cyber security. Only informed users of digital services and products can react sufficiently and protect themselves. This applies for companies and authorities, but also for private end users. Security affects us all.

- For this reason, we must work toward clarifying the extent of the surveillance by intelligence services as quickly as possible. This includes information about the legal basis on which security authorities collected and analyzed data and the methods used for this purpose. Diffuse and contradictory reports cause trust in the security of digital communication to erode further.
- Not only do companies have to justify their reputation and demonstrate their trustworthiness, they must also better protect themselves from loss of knowhow and intellectual property through industrial espionage and from sabotage of production facilities. This is why we must ensure that managers, employees, customers and partners are aware of the risks in cyberspace, but also of the technical protection measures they can take. The basis for this is transparency and knowledge of how to handle personal data. In terms of the economy, it is small and medium-sized enterprises in particular who need to be

made more aware and given more help with regard to potential and risks in cyberspace. Overall, it is therefore necessary overall to expand in-house training and continuing education in the area of security.

- Cyber-security products and services need to be diversified. Business has a mandate to offer the state, companies and consumers products that meet the different needs and requirements of these divergent user groups. Certifications can offer valuable guidance for users in this regard and we want to push that forward.

- But raised awareness for issues of cyber security cannot be limited to industry. Sustainable, workable concepts have to address people in education and in vocational training, and must include the development of consumer protection rules for the use of digital media.

Cybersecurity and cybereconomic policy

Summary: The participants agreed that security of information technology is a key strategic success factor for companies. Digital business models only work and innovations are only accepted when customers trust that their data is secure. Businesses therefore have a vital self-interest in securing IT systems as much as possible through technical and procedural measures. Data as their “wards”. An increased level of security is a key differentiator, a competitive advantage and a sales argument. Cyber security policy is also economic policy because, in the globalized world, a high level of data protection and data security is an advantage for an economic region. We are confident that building up further competencies in cyber security will also pay off economically, because it creates technological superiority and contributes to the profile of a "reliable exporter" of high-end cyber-security products.

- We need to take further strategic and institutional steps to develop an orchestrated cyber security and cyber economic policy. Cyberspace needs a binding, concerted framework that balances legitimate security needs against fundamental rights and at the same time retains the basic concept of freedom in the Internet. Because different nations make differing assessments on the balance between freedom and security due to different cultures and experiences, we need an international discussion on values and ultimately a shared set of values that applies globally. It will be difficult to achieve an international consensus in terms of regulation, enforceability and sanctions in the foreseeable future.

- Information was more fleeting in nature in the past; digitization is increasingly creating a life-long memory. Once saved data that is never deleted can, over time, change a person's legal situation. Once something has been uploaded to

the network, it can be used to someone's detriment for decades to come. To safeguard human rights and the right to freedom in future, too, we need internationally implementable conditions for a “digital right to oblivion”.

- We need a sustainable international agreement on data protection. It must be evident which requests for information and surveillance measures are permissible for whom and under which circumstances. This also includes closer involvement of and improvement in the work, in particular, of parliamentary supervisory and controlling bodies that deal with surveillance issues. The aim must be the mutual renouncing of industrial espionage and the proscription of cyber sabotage.
- At European level, the draft General Data Protection Regulation and the new Directive on Network and Information Security must be pursued with determination. The re-negotiation of the Safe-Harbour-Agreement is indispensable since the requirements it makes in terms of data privacy and the possibilities for enforcement obviously do not comply with European law. This agreement will first have to be abrogated. Only then will it be possible to credibly begin re-negotiations in respect of European interests.
- We need a cooperative, trust-based cyber security strategy.
  Politics and business must work together to develop the most important cornerstones for this strategy. They include both security and economic-policy aspects such as security research, promotion of research, and a targeted strategy promoting expert development. At national level, political responsibilities need to be pooled in an interdepartmental coordinating body to create a unified basis for a cyber security and cyber economic policy.

Information exchange

Summary: Only comprehensive cooperation promises success. Only together are we strong in the battle to make cyberspace more secure. Awareness of the risks entails the global mapping of sources, quality and quantity of attacks to be as comprehensive as possible. We need to continuously update such an overview of the situation through voluntary international and cross-sectoral exchange between governments, business and society.

- We need a shared overview of the situation. We want to promote open exchange on attack scenarios on a voluntary basis, thereby creating a climate in which effective and sustainable measures for protecting against cyber attacks and products to protect against attacks are developed and shared more quickly. The objective must be to identify risks at an early stage, to develop solutions in good time, and thus to strengthen the security level overall.

- We need to establish an international security culture based on shared values, trust, transparency, exchange and cooperation.
- The necessary international networking of security experts can only succeed if they are acting within a consistent international framework. Politics must work toward such a framework and together with business, vigorously support exchange among experts.
- With this in mind, an obligation to report cyber risks as part of companies' risk management systems must not be taboo. Only then will it be possible to make necessary countermeasures transparent and to prioritize them.