Cyber Security Summit – Working party 3

Gaining trust, restoring trust

After the monitoring scandals of the very recent past, the industrial and political worlds face the challenge of creating a security culture based on trust, transparency, and cooperation. The problem of trust between states may possibly be solved if all sides declare openly and transparently what espionage activities they have indulged in.

It was not clear how the U.S. government could be persuaded to change its espionage activities. However, the discussion group agreed that the Europeans should avoid the search for a means of putting pressure on the U.S. to change its conduct. The suggestion of linking this to the negotiations for a transatlantic free trade agreement was rejected as absurd. In so doing, Europe would mainly harm itself.

Instead of a policy of escalation, diplomatic solutions were required. A possible no-spy agreement between the states should be given realistic consideration.

A Schengen Agreement against industrial espionage could serve as a model for an international agreement. However, there was disagreement within the working party. Considered realistically, such an agreement would not mean the end of espionage. Nevertheless, espionage would be more expensive for the governments concerned. A no-spy agreement might at best have a placebo effect. Some of the participants in the discussion stressed that protection against cyber criminality, which threatened the entire infrastructure, was more important than protection against espionage.

No-spy agreement not a solution

There was nevertheless agreement that phone-tapping activities undermined basic democratic rights, endangered freedom of speech and threatened freedom of information and protection of the private sphere. These issues did not just involve tapping the German Chancellor's phone, but affected citizens as a whole. It was the duty of politicians to restore trust among the population. Political espionage had to be restricted. States had to lay down red lines for mass monitoring. A simple no-spy agreement would not solve the problem. Every government had to fulfill a national duty to provide security. A public discussion about Big Data and the evaluation of mass data was necessary. There was unanimity on the need to create a joint, consensus-based understanding shared both by the NSA and the European secret services.

Balance between freedom and security required

Companies with international value creation chains required international regulations and standards. Participants pointed out that at the moment there were major national and cultural differences in data storage and the statutory obligation to pass on information. In Germany, the storage of personal data was only permitted under very strict conditions. In the U.S., almost all data was stored. The U.S. government made frequent requests to companies to provide information. These demands sometimes took place in a legal gray area. Companies always had a duty to check the legality of these requests. Sometimes a court order from the country where the data had been collected was required.

There were cases in which the U.S. government demanded the provision of data that had been collected in a different country. The basis for the demand was that the headquarters of the company collecting the information was in the U.S. In this case, the duty to provide the information conflicted with the legal rights of the country where the data had been collected. If the company provided the data demanded by the U.S., it had to pay a fine in another country. The customer required a convincing explanation of this situation. The participants in the discussion demanded that existing contradictions in international law should be resolved.

Thus the question had arisen of how an international Code of Conduct (CoC) could be implemented. The reply was – if all those involved are interested, an international Code of Conduct would be possible. For example, if data protection issues started to threaten the cost-effectiveness of American companies, this might create a basis for an international CoC. If governments developed legal systems that were mutually incompatible, they would obstruct international business, unless companies built up enormous reserves to cover fines. Prescriptive solutions, that is, those based on regulations demanded by governments, had to be able to be implemented. It had become clear that cyber security had to be reflected in politics and legislation – with international standards, including a uniform EU approach which also had to prevent the idea of informational self-determination from becoming mere empty words.

More security for critical infrastructures and companies

Industry assumed that governments were exposed to even greater security threats than major companies, because they provided less money for security. Small and medium-sized enterprises (SMEs) were at the greatest risk, because they had neither the expertise nor the financial means to make strong security arrangements. This group in particular required a central contact from whom they could request help. This also implied that iGovernance was required to orchestrate the process, including a central point of contact for the exchange of information. In principle, a joint approach by industrial and political leaders was seen as necessary to improve security. However, there were a series of approaches in the areas of critical infrastructures, consumers, and SMEs. The principal duty of government had to be to support SMEs with consultancy to increase their sensitivity on cyber security.

Industry expected specific assistance and that security vulnerabilities in products should be remedied more quickly. One topic for discussion was claims for damages against providers if companies suffered losses through security vulnerabilities in third party products, though the companies themselves had taken all necessary security measures. In order to be able to lay such claims, legal security would have to be created. It seemed likely to be particularly difficult to prove in court that the firm offended against had complied with all its duties to employ its own security measures. The industry saw the necessity to provide differentiated, adapted solutions rather than one-size-fits-all regulations that treated every company in the same way. However, when the issue was the protection of critical infrastructures, those wishing to protect the constitution demanded a national solution, perhaps in the form of a general registration requirement in all security incidents.