

Cyber Security Summit 2014 – Documentation

Panel discussion:

Data Protection and Cyber Security – How to Find Common Ground?

What actions by intelligent services are appropriate? What is the right balance to strike between the security interests of states and individual personal rights? On what might be seen as the first anniversary of the intelligence services scandals, Ben Wizner, attorney for Edward Snowden and Director of the American Civil Liberties Union, Clemens Binninger, Member of the German Bundestag [Parliament] and Chairman of the [German Parliament's] Parliamentary Control Board, and Klaus-Dieter Fritsche, State Secretary and Federal Intelligence Service Coordinator, German Federal Chancellery, looked for answers to these questions.

Much trust on the part of people, companies and governments was lost as a result of the Snowden disclosures. This has now reached the point where Internet companies such as Google have announced that they are going to use encryption to block all eavesdropping and data interception. Can this be in harmony with intelligence services' primary goal of protecting the security of their countries and citizens?

Damage to national and global security

Elmar Theveßen, Deputy Editor-in-Chief of ZDF German Television and intelligence service expert, expressed doubts as to whether intercepting enormous amounts of data is the right way to improve security: "Is this really about combating terror? I don't think so. It's about much more. It's about collecting as much data as possible in order to advance the economic, political and military interests of nations." The NSA and the GCHQ compromise the security of their own countries and of other countries, Theveßen stated. With backdoors, they weaken systems, destroy trust,

prepare the way for faulty and deceptive programs and help to spread new attack methods that can endanger others, he explained.

Unfounded data collection

Clemens Binninger confirmed that "a security strategy that focuses only on accumulating as much data as possible, in order to perhaps make it possible to find a hot trail, is not useful." Intelligence service coordinator Klaus-Dieter Fritsche agreed. The state must always uphold the principles of proportionality and human dignity, he added. Intelligence services must therefore be criticized when they unjustifiably accumulate enormous amounts of data and thereby impinge on citizens' freedom. "The services should not be doing everything that is technically possible," Fritsche said. Data privacy and data security are manifestations of freedom, he pointed out. Citizens want to be free from threats and free to determine what happens with their own personal data, he stated. "We need to find a balance between these two freedoms." For this reason, the Federal Government is seeking to ensure that the services function more transparently. "We need to build citizens' trust in our services and to expand parliamentary and executive control of the relevant legal foundations."

Citizens have not changed their behavior

Both Fritsche and Binninger expressed surprise at the way people reacted to the Snowden disclosures. "Citizens are concerned, but their behavior has not changed. The numbers of users of WhatsApp have increased, and behavior in social networks has not changed – the same carelessness is still there," noted Binninger, and Fritsche added: "I am more concerned about the data that citizens voluntarily disclose on the Internet. They don't see the dangers related to what can happen to that data." And, he added, this problem does not involve legal aspects of data privacy, since citizens themselves are allowing their data to be used.

Balancing national and personal interests

Snowden attorney Ben Wizner also expressed doubts regarding the effectiveness of accumulating enormous quantities of data. "It doesn't become easier to find a needle in a haystack when you make the world's biggest haystack." In general, a discussion is also underway in the U.S. about the right balance between data privacy and security, he added. That discussion has been swinging between two poles, he explained: Is the risk for society more important than the individual, personal risk involved if, for example, encryption completely blocked the actions of intelligence services? Or must personal freedom be placed above national security? "It's not a black and white issue. We have to precisely balance national and personal interests," Wizner explained.