

Cyber Security Summit 2014 – Documentation

Keynote speech by Andy Müller-Maguhn, Managing Director of the "Datenreisebüro" think tank and former member of the Board of the Chaos Computer Club (CCC)

"A complete failure of diplomacy"

In his keynote remarks, Andy Müller-Maguhn, Managing Director of the "Datenreisebüro" think tank and former member of the Board of the Chaos Computer Club (CCC), discussed interest conflicts in IT security and the importance of encryption. He pointed out that while we now see that our communication systems are being monitored almost constantly, there is good news: cryptography works.

Müller-Maguhn stated that Edward Snowden's successful escape to Russia is proof of the effectiveness of encrypted communication. At the same time, he expressed surprise at European countries' willingness to cooperate with the U.S. government. The U.S. government has violated the digital sovereignty of countries and individuals, he explained. Spying on citizens and countries does not fit with "our understanding of cyber security", he added. Müller-Maguhn spoke of a "complete failure of diplomacy."

The deception begins with terminology, he explained. For the U.S. government, "trustworthy systems" are systems that are under its control. One central problem is "default deniability," as seen in the ongoing denial of NSA activities. The denials put forth by technology companies should not be trusted, either. For example, the security risks in Windows 8 need to be openly discussed, he stated. The Chinese government has already prohibited use of that operating system on its public agencies' computers, he added.

Trustworthy encryption systems are needed

Müller-Maguhn called encryption the most important technology for the digital sovereignty of citizens, organizations and countries. Snowden's escape showed, he explained, that encryption works and offers foundational protection in cyber space. The problem is that the security of encryption systems is constantly being compromised. Mechanisms to review the trustworthiness of encryption systems need to be developed.

In closing, Müller-Maguhn called for greater sensitivity in use and handling of data. We need to think very carefully about what data are to be processed, and how, and about where they are going. A good way to start would be to minimize data production per se. In future, we need to keep information from being used for purposes of warfare. This also includes data from social networks, he added. He emphasized that "security and surveillance are not the same thing." Conflicts of objectives and interests need to be given greater attention in selection of IT security strategies and of security component providers.