Arne Schönbohm

President, Cyber Security Council Germany e.V.

What led to the establishment of the Cyber Security Council Germany in 2012 and what are the Council's main tasks and goals?

Policy makers recognized the importance of creating a think tank to bring together major players in the field of cyber security. The Cyber Security Council Germany was founded in August 2012 by well-known leaders across a variety of fields. The Berlin-based association is politically neutral and its purpose is to advise companies, government agencies, and policy makers about cyber security and to protect them against cybercrime.

The main tasks of Cyber Security Germany e.V. are to:

- Intensify cooperation between politics, public administration, industry, and science to improve IT protection
- Support initiatives and projects to promote the awareness of cyber security
- Construct a European and international cyber security network
- Build a knowledge platform and network for members of Cyber Security Germany e.V.

Unfortunately, the current EU Commission draft NIS Directive relies on an outdated regulatory approach that was originally designed to meet the challenges of the 18th century, and then later updated in the 19th and 20th centuries as technologies developed. These pre-existing models are too slow and cumbersome to manage the digital environment of the 21st century. They will probably not be effective and could even undermine our ability to create a sustainable cyber defense system.

Hence, we need newer, more flexible and dynamic models to address the enormous unfamiliar challenges that arise from the ubiquitous nature of digital technology and the inherent vulnerabilities that come with it. These challenges are simply too complex for governments to manage alone. We need to develop and leverage a new partnership between governments and the businesses that own and operate the critical infrastructures that provide the services essential to a modern economy and also hold the personal data of nearly every European citizen.

We also need to understand cyber threats in a broader context. These threats are not just about the (in)stability of technological infrastructures, but also about the significant economic and public policy implications of security breaches.

The Internet Security Alliance (ISA) and the Cyber Security Council Germany, for example, propose a modern "Social Contract" between industry, governments, and citizens. This "Social Contract" will leverage market economies to create a sustainable cyber security system while incentivizing innovation, investment, and economic development.

In your book on cybercrime, you describe cyberspace as a “fifth military battlefield.” Please elaborate on this.

Cyberspace is now seen as the “fifth military battlefield” next to land, air, sea, and space. Until recently, the objective of cybercrime was primarily technology theft or information dominance. While military attacks use bombs and rockets, cyberspace has its own virtual weapons. The advantages of cyber weapons are that they are anonymous and quite cheap. Cyber weapons have supported military objectives, as shown in 2010 by the worm Stuxnet, which targeted and paralyzed centrifuges for uranium enrichment in Iran. Similar incidents have also occurred in Estonia and Georgia. Nowadays, we are developing more and more into a cyber-dependent society and governments can use this dependency to either defend their assets or to attack others. However, it cannot be stressed enough: Cyberspace does not exist in a legal vacuum; rather, the contrary is the case: There are laws and regulations in place to govern and protect cyberspace.

What is the greatest danger that individuals face with regards to cyber security?

More and more individuals are using cyberspace for almost everything they do in their daily lives. In light of the continuing high number of potential risks and the increasing variation of attacks as well as the expected growth of such risks in the future, cyber security has become a national priority.

According to policymakers, privacy breaches, data fraud, and malicious software are some of the greatest potential risks for individuals on the Internet. However, the greatest danger facing the individual user is clearly identity theft, since it opens the door to many other criminal activities like fraud or credit card theft.

Another large obstacle for governments and international organizations to overcome is the speed at which technology advances, making it very hard for governments to adequately react to these changes in order to pass or adapt new laws in a timely fashion. In addition to these risks, there is also the challenge of managing the speed at which the government is acting or more likely reacting to cybercrimes and cyber security needs. It is like a race between a cheetah and a snail – the snail represents the government and the speedy cheetah stands for technological advancements in cyberspace, which is rapidly developing.

On your website you cite Wilhelm von Humboldt’s remark: “Without security, there is no freedom.” Many people, however, feel that they have to sacrifice freedom for the sake of security. What are your thoughts on this?

Von Humboldt argued that without security, man would not have the freedom to develop his life in a way he desires. On the flip side, too much freedom and no rules would endanger the security of the people. In this scenario, a few dominant people would repress the weaker ones, such as minority groups. Therefore, security and freedom have to be in sync. Over the past few years, the focus of many countries has been on national security, especially during the aftermath of the terrorist acts in New York, London, and Madrid. This priority resulted in a reduction in freedom and civil liberties. However, in the future, there has to be a greater balance between security and freedom, as one diminishes the other. The more security I want, the more freedom I have to sacrifice; conversely, the more freedom I desire, the more security I have to give up. A society with total security will not have true freedom and vice versa. Without security, we would not be living in the cyber society we are living in today, nor would we benefit from the wealth creation it enables for our society. E-Commerce and many other services that add value to our lives rely heavily on security, i.e. reliability, stability and accountability. However, this does not give organizations, countries, or companies the right to collect all possible data that they can get their hands on under the pretext of achieving security. This would only lead us to sacrifice our personal freedom in exchange for superficial security. The Cyber Security Council Germany has therefore made it its goal to work towards a working and sustainable balance of freedom and security in cyberspace.

What are the most common types of cybercrimes? How has this changed over the history of the Internet?

Cybercrime has increased dramatically over the past years. It is a relatively new field and refers to the perpetration of crime using information and communication technologies. This includes spying, data theft, the distribution of malicious software, identity theft, phishing, computer fraud, and many more. Additionally, cyberspace inadvertently enables many of the traditional types of crime, such as blackmail, gambling, narco- and human trafficking, money laundering, and counterfeiting.

The development of crime in cyberspace and the ways criminals are using information and communication technologies for their own benefit have changed considerably over the past decade. What started with Trojan web dialers has now evolved into advanced persistent threats unlike anything we have experienced in the past. Cyber criminals are usually the first ones to adapt to new developments and technologies in the field of cyber security and are the first ones to take advantage of newly discovered vulnerabilities. Since 2009 organized crime is earning more money with cyber crime than with drugs.

Firewalls. Anti-virus software. Encryption. What kind of protection should the average household user have?

The bare minimum should be an up-to-date anti-virus software and firewall. Encryption would be an extra “nice-to-have.” In addition to these programs, every private user should be aware of his or her “digital footprint,” such as personal data, sensitive data, or user statistics that he or she is leaving behind while using the Internet. Users should be careful and learn how to minimize this footprint in the future. Moreover, the private user should prioritize and categorize personal data based on which data are especially worth protecting. And as advice for everyone: Do not open any email you receive that looks suspicious, such as “Congratulations, you won $100,000.” Please also be sure to instruct your children about proper Internet use.