Cyber security and its strategic dimension

But cyber security is not only about technical implementation, it is also about strategic decision making. There is a need to discuss an integrated approach bringing all aspects together in the form of an EU cyber strategy – integrating also aspects like industrial policy – so that the EU can rely on secure components. A debate on an international a code of conduct for the internet is needed for example to protect humanitarian infrastructures like hospitals against cyber attacks from states and how to achieve a better framework internationally (the majority of States worldwide do not have any legislation criminalising cyber attacks).

In view of new developments like cloud computing, we also have to discuss threats and challenges. Cloud computing can help to better integrate data, to achieve more security, but it also creates risks. Sovereignty over data and applications, transparency and privacy are important issues to be preserved also in the cloud. We have to create a new security awareness to avoid being taken by surprise by new threats (as a possible amplified impact of malicious insiders in the cloud or an increased reliance on the general connectedness of the internet). These are concerns from a counter terrorism perspective but also far beyond. We have several EU initiatives to build on, but cyber-space will continue to challenge our EU policy making and coordination.

Born 1956 in Brussels, Gilles de Kerchove was Director for Justice and Home Affairs at the EU Council Secretariat from 1995 to 2007.

News: ESRT Conference on Cyber Security

On 14 June, the European Security Round Table (ESRT) organised a conference entitled "Shared Threats – Shared Solutions: Towards a European Cyber Policy", which was initiated by the Estonian Ministry of Defence. Keynote speakers included the Estonian Defence Minister, Mart Laar, as well as Cecilia Malmström, Commissioner for Home Affairs, and Richard Wright, Director for Conflict Prevention and Security Policy, European External Action Service. This initial conference in Brussels aimed to kick-start a discussion about a comprehensive policy approach to Cyber Security and to sharpen the awareness among EU-Institutions that have coordinated activities in a number of areas of EU competences.

Christoph Raab, Director of the ESRT, welcomes the Estonian Defence Minister, Mart Laar, at the Cyber Security Conference.
Photo: ESRT

More information: *www.security-round-table.eu*

Does the cyber threat usher us into an area of exister

Cyber crime and cyber w

by Arne Schönbohm, CEO, BBSG, München

Can the European Community withstand the new challenges of cyber crime and cyber war? How real is the new threat of cyber attacks? Estonia came under massive cyber attack in the spring of 2007, Georgia in 2008, Kyrgyzstan in 2009 and the Iranian nuclear programme in 2010. All these countries were, at the time of the attacks, involved in conflicts with other countries.

The Internet – a new domain of "warfare"

The Internet has been called the "fifth domain of warfare" alongside land, air, water and space. Cyber attacks are aimed at severely disrupting a country's social and economic life and damaging its economy. To illustrate our vulnerability and the extent to which we are interconnected, the trade in emission certificates within the European Union can serve as an example. In January 2011, hackers brought down the European Union Emission Trading System, in which 20% of all emissions certificates are traded. They penetrated several national registries, for example in Romania, stealing about 1.6 million certificates in November 2010 and an additional 2 million with a value of about € 30 million in January 2011. The Stuxnet worm attack on the Iranian nuclear programme in Bushehr similarly illustrates the severity of the new threat.

SCADA supervisory control programmes are used to monitor industrial processes in refineries, power stations and manufacturing plants and to control and display automated operations. An attack on such a programme could cause an accident with extremely serious consequences.

Flexibility versus vulnerability

With the number of cyber attacks on companies and governments increasing and the damage they cause on the rise, close NATO attention to the issue is fully warranted. A majority of the Member States of the European Union are members of NATO and are economically strong. The are generally highly networked, globally active and endowed with modern armed forces that can engage in network-centric operations and are interconnected via standardisation. Commercial off-the-shelf systems are increasingly being procured. These systems, already in widespread use in the business world, are less expensive and can be acquired more quickly than customised products; they can thus support more rapid adjustment to changing technology, providing much-needed flexibility. But commercial off-the-shelf products make users more vulnerable, since defects – so-called "trap doors" – that even experts have difficulty recognising can be deliberately designed and built into these software systems.

Under Article 5 of the North Atlantic Treaty, NATO calls for

pplications similar to the nuclear?

– we have to cease being passive

collective self-defence when an "armed attack" is carried out on one or more parties. Cyber attacks on states are, however, not included in this definition, even though they can cause damage far exceeding that caused by an armed attack. Article 5 should be extended to cover cyber attacks. The existence of "trap doors", mentioned above, also makes it necessary to continuously monitor the suppliers, developers and producers of security-critical goods to be procured as well as the integrity of employees and to provide ongoing training.

The line between cyber crime and cyber war

There is no longer a clear distinction between the two. The same viruses, Trojans and other attack programmes are used for both purposes. During the war between Georgia and Russia, Russian Business Network cyber crime organisation was apparently using to attack Georgia virtually at the behest of the government.

The purpose of cyber attacks

In most cases, cyber attacks are carried out to earn money. Last year for the first time more than 246,000 crimes perpetrated on the Internet were recorded across the Federal Republic as a whole, an increase of nearly 20% from the previous year. Examples of such crimes are counterfeiting, fraud and theft of development documentation, access codes, etc. According to Interpol, some 162 million credit card data sets were put up for sale or traded over the Internet in 2009, enabling the card to be used without restriction. Such credit card data are said to represent purchasing power of US$5.3 billion. Europol has reported that credit card information can provide a return of US$30 per card, bank data between $10 and $25 and even access to an e-mail account up to $10. Other data such as pension scheme numbers, telephone numbers and birth dates also constitute a lucrative market.

Lucrative business

Criminals gain access to the data by penetrating the data systems of networks such as hotel booking platforms and the Sony Playstation network, to give just two examples. Such cases have occurred in Germany. In 2009 alone, 100,000 credit cards that had been used in Spain during a particular period of time had to be exchanged. Businesses especially are suffering increasing losses. Analysts have calculated that organised crime generated more profits from cyber crime than from drug trafficking in 2009, for the first time. The German Ministry of the Interior, said that the potential damage to the German economy alone amounts to € 50 billion per year.

Arne Schönbohm
Arne Schönbohm is General Manager, BSS BuCET Shared Services (BSS AG).
Studies of International Management in Dortmund, London and Taipei.
1995-2008, DASA / EADS. Retired from EADS as Vice President Commercial and Defence Solutions. Mr. Schönbohm is editor of "Deutschlands Sicherheit – Cybercrime and Cyberwar" (2011)

Countermeasures require clear jurisdiction

What steps can be taken to effectively thwart cyber crime? Private-sector Internet users, companies, national governments and the European Union must henceforth optimise their security measures to combat cyber attack. Government has a duty to fully protect the country's economy and its external and internal security, including in cyber space. But jurisdiction remains a problem. The "Cyber Europe 2010" cyber security exercise carried out in November showed that 55% of the participants were not confident they would be able to quickly identify the right contact, in the event of a crisis, even with the available directories. Much remains to be clarified in this area. Yet the only way to limit damage to businesses and governments and to optimise security is to define areas of responsibility, ensure short communication paths and respond rapidly.

Security-focused business model

One of the main duties of every government is to ward off risks to public safety and public order and to safeguard the country's economy. One important aspect of this effort is the protection of the R&D systems of individual industrial sectors. Despite all the newly developed protective technologies and the ongoing improvement of security systems, espionage attacks still occur, as we have seen. These can result in loss of know-how and data. Hence there is a need to increase security spending as part of corporate risk reduction. Auditing firms should take this risk on board by performing crisis-management audits and insurance companies could sell policies covering such losses. The additional costs would have to be borne by companies, but the costs could be calculated in advance and would certainly be lower than the cost of a comprehensive loss. In addition, this business model could spawn new growth industries.
The introduction of preventive measures is a matter of political will on the part of the European Union and its Member States. They must cease to be passive and become pro-active in cyber space.