ENISA at the service of the EU's Cyber Security

Udo Helmbrecht

Executive Director

ENISA

SEDE speech

European Parliament

Brussels, 16th March 2015

Dear Ms Fotyga, members of the SEDE committee and representatives of other authorities present.

Thank you for the opportunity to address you here today, and provide you with an overview on securing the EU's cyber space, while at the same time demonstrate the contribution ENISA is making for Network and Information Security (NIS).

Information and communication technologies (ICT) are the backbone of every modern society. **An open, safe and secure cyberspace** is key to supporting our core values set down in the EU Charter of fundamental rights such as **privacy and freedom of expression. This is also essential** for the **smooth running of our economies within the European single market**. However, ICT technologies and business opportunities in cyberspace also present opportunities for crime and misuse[1].

Security of network and information systems is essential to the security of all the critical sectors in society. Disruptions on these infrastructures and services are becoming more frequent and are estimated to cost annually 260-340 billion EUR to corporations and citizens. The World Economic Forum's 2014 report on Global Risks, lists "failure to adequately invest in, upgrade and secure infrastructure networks" as a top threat to the global economy.

Various recent studies, including those of ENISA[2], demonstrate that the threat landscape will get worse, unless we take firm action. It is expected there will be a significant evolution in the top threats, with new, more sophisticated malicious attacks on critical services and infrastructures, with a dramatic increase in data and security breaches (25% increase over the same period last year).

Today I will present elements and activities in the global cyber security context and talk firstly about the taxonomy. Today we are still living in a tailorised world of the sailos of law enforcement, military, intelliegence service, public institutions, private companies etc. The attackers do not care about this separation and use the same tools and infrastructure to achieve their objectives. Therefore we have to distinguish between:

Cyber security means protection of information, information systems and infrastructure from those threats that are associated with using ICT systems in a globally connected environment. By deploying security technologies and security management procedures, a high level of protection of personal data and privacy can be achieved. A typical example, is ensuring the integrity and security of public communications networks against unauthorised access.

[1] Recently the German newspaper Süddeutsche Zeitung reported an increase in damages only for Germany arising from cybercrime from 37 M€ in 2008 to 42M€ in 2012 and in increase in reported cybercrime cases from 37.900 in 2008 to 63.595 cases in 2012.

[2] The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. ENISA supports the EU and the Member States in enhancing and **strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents.**

Cyber Crime Crime on the internet has a new dimension. The technology allows organized crime to scale their "business", especially outside the legal boundaries of states.

Cyber Espionage We had military espionage for thousands of years. The only difference between traditional espionage and cyber espionage is the use of technology and as long as we have civil intelligence agencies it will not stop. Another aspect is espionage because of philosophical disagreement[3].

Cyber Warfare We are facing a new type of asymmetric warfare with a new paradigm and no taxonomy.

Assessing the Threat Landscape Environment (ETL)

In 2014, major changes were observed in top threats: an increased complexity of attacks, successful attacks on vital security functions of the internet, but also successful internationally coordinated operations of law enforcement and security vendors. Many of the changes in cyber threats can be attributed exactly to this coordination and the mobilisation of the cyber community. However, the evidence indicates that the future cyber threat landscapes will maintain high dynamics.

I often say, identifying and understanding cyber threat dynamics can be the basis of a very important cyber security tool. The dynamics of the cyber threat landscape set the parameters for flexible, yet effective security protection regimes that are adapted to the real exposure. **Understanding the dependencies among all components of the threat landscape is an important piece of knowledge and an enabler towards active and agile security management practices.** With ETL 2014, ENISA continues its contribution to publicly available cyber threat knowledge[4].

CERTs and first response

CERTs - the EU's Computer Emergency Response Teams - respond to emergencies, new incidents and cyber threats that could affect vital computer networks or information systems.

These teams **assist public and private sector** organizations to provide an **adequate response to incidents and threats accross an EU wide network**. They exchange experience and expertise while developing 'baseline capabilities'. Furthermore, it raises the bar for non-Governmental teams to offer similar response to incidents across the EU.

[3] e.g. some countries see industrial espionage as part of their social behavior.

[4] The Emerging Technology that will impact the Threat landscape are: Cyber Physical Systems (CPS), Mobile and Cloud computing, Trust Infrastructure, Big Data, and Internet of Things. Cyber Physical Systems (CPS) - has an important impact within the protection of Critical Infrastructure Protection – and represents a distinct opportunity creating competitive advantages for European industry and research.

As part of ENISA's cooperation with CERTs, the Agency has updated and extended its training material in the area of Network Forensics, and has published a good practice guide on Actionable Information for Security Incident Response. The study is complemented by an inventory that can be applied to information-sharing activities and an accompanying new hands-on exercise scenario.

Pan-European Cyber Exercises

Over the past five years ENISA has supported the implementation of the Commission's policy initiatives, the CIIP Communication and the Digital Agenda, by developing ***cyber exercises*** and ***cooperation and*** *by* defining and testing ***operational procedures*** *(EU-SOPs)* for all cybersecurity authorities in the EU.

In 2010, there was only a table top exercise and no crisis management procedures at the EU level for dealing with cyber-events. Now Standard Operating Procedures are in place for handling cyber events. New policy initiatives such as the Cybersecurity Strategy and the NIS Directive have highlighted the importance of these successful activities**.**

Both activities will continue to contribute to the long-lasting impact of the EU Cybersecurity Strategy and the NIS Directive on the level of security in the EU. In this light, ENISA will need to **streamline its activities** in this area and further develop them to **support effectively the implementation** of this demanding policy context.

National Cyber Security Strategies (NCSS)

Around twenty (20) MS have now developed a National Cyber Security Strategy (NCSS). The remaining eight (8) Member States are also developing strategies. ENISA has established an expert group with representatives from the Member States to exchange good practices and to analyse specific topics of interest to the group. Last year the Agency developed a good practice guide for the evaluation of National Cyber Security Strategies. This year ENISA co-operates with Member States on PPPs (Public Private Partnerships) and how they can be used in the context of a National Cyber Security Strategy, while in May a workshop is planned on National Cyber Security Strategy development.

Criticial Information Infrastructure Protection (CIIP)

The Agency has worked for many years in the Criticial Information Infrastructure Protection (CIIP) area and has assisted the Member States in implementing the EU's CIIP action plan. Currently our focus is only on a few areas namely the Telecom Sector, Energy sector and Finance sector. In the future we plan to extend our efforts in the area of health, transport and cover more aspects within the energy sector.

In the Telecoms and Smart Grids area we have developed minimum security measures. In Telecoms, we have also developed a harmonised incident reporting framework (due to article

13a). This work could provide a strong basis for assisting in implementing similar requirements in the NIS Directive once it is adopted.

Incident Reporting

All EU National Regulatory Authorities now use ENISA's guidelines and recommendations for incident reporting. The last four (4) years we have issued four (4) annual incident reports covering the area of Telecom operators. In the context of Article 4, which covers *Data* Breach Notification, ENISA brings together National Regulatory Authorities and Data Protection Authorities to develop a common approach to incident reporting in Europe. Additionally the Agency has been called in the eIDAS (Electronic identification and trust services) Directive to assist National Regulatory Authorities to implement the incident reporting scheme for trust providers. The work has just started and is expected to finish in June 2016.

Cryptography research and tools and 'security by design'[5]

Cryptographic tools are widely used to protect our information infrastructure from malicious users. Today cryptography is mainly used to protect the access to services and to protect communication of individuals and groups (e.g. virtual private networks and message encryption, end-to-end encryption).

A good approach to secure our personal data is to "*reduce, protect, detect*". However, as with any quality measure, it poses a burden for implementers. Hence, EU legislation needs to support privacy by requiring systems' developers and service providers to build in data protection measures from the design phase on, what is also known as **'security by design'**[6].

Digital sovereignty

For the EU to become the single market of choice for governments and industry, it is necessary to have trusted core NIS technologies and services for industry and citizens (i.e. Trust in EU products and services).

Furthermore, there is a need for an innovative business model for EU companies producing cybersecurity products and services. Currently there is no properly coordinated EU industry policy in place specifically for the IT security sector. In addition, it is critical to ensure that the cost of implementing NIS legislation and policy does not penalise EU companies in a global market.

There are a number of solutions in this direction, for example in the area of standardisation, certification, public procurement and research.

[5] See report on "Privacy and Data Protection by Design" http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design

[6] This should be done in a proactive manner and not simply secured after the event, on a case by case basis. This is a two-sided coin as information technology should also provide the capabilities for implementing the protection mechanisms foreseen by legislation. **It also signals the importance of encouraging standardisation and certification activities with industry.**

Challenges for the future

There are different aspects to cyber security and cyber attacks. But all current security approaches tend to make use of the same technology, making it difficult to judge who is attacking what and why. We are facing a new type of asymmetric warfare with a new paradigm and no taxonomy. This brings cyber security to a new level, making its scope more critical for the EU's security. The protection of information, information systems and infrastructure from those threats associated with the use of ICT systems in a globally connected environment, is inevitably linked with effective security policies and robust and resilient cyber defence capabilities within a common (= taxonomy) EU policy.

To enable the EU to address this, **cooperation** among Member States, EU Institutions and other relevant bodies, is a top priority. Within this scope, collaboration or so- called 'Service Centres' for special tasks can be created between agencies, e.g. ENISA and Europol including Member States' National agencies.

We need European Prevention, Detection and Response capabilities. This includes harmonization of European and international legislative frameworks and procedures as well as collaboration models to ensure adequate policy implementation. Citizens need to be able to trust the EU to create a legal framework and to prosecute those who break the law. Furthermore, we need to implement **early warning systems** to support detection. Some of the current decisions will have an impact on the EU's future over the next few decades.

ENISA is strategically well positioned to address the technical and organisational elemements of these challenges and threats, provide solutions and the knowledge that will support investment and deployment of electronic services in the EU internal market. ENISA is here to actively contribute to a high level of network and information security within the Union, and use its expertise to stimulate broad cooperation between actors from the public and private sectors, and deliver its agenda on cyber security for the European Union and its citizens.

Thank you for your attention.