International Perspectives on Cybersecurity

Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht - 2018 Potsdam conference for national cybersecurity

POTSDAM, GERMANY
JUNE 2018

1. Cybersecurity in the EU

In the last few years, there have been many new developments in the cyber world. We continue to witnessthe digitalisation of our daily lives, the development of new technologies, new threats and new stakeholders. The words cybersecurity, cyber warfare, cyber espionage, cyber terrorism and cyber defence are increasingly referred to in daily conversation by our citizens and politicians. Some new concepts that have emerged in the last few years include fake news, cyber ethics, cyber diplomacy and digital sovereignty.

The ENISA Threat Landscape Report of 2017 highlighted the growth in the traditional cyber challenges where we have witnessed the increased complexity of cyber incidents, the monetisation of cybercrime such as growth in ransomware, cyber espionage, advanced persistent threats and attacks on critical infrastructure.

Are we prepared to address the challenges arising from new threats and the new hybrid threat landscape in cyber space? To name a few, we are witnessing development and deployment of new technologies such as Robotics, growth in Artificial Intelligence. From a technical perspective, we have new technologies changing the cyber landscape. The Internet of Things/ Internet of people is now being deployed with an estimated 20 Billion devices expected to be operational before 2020. Industry 4.0, Robotics, Artificial Intelligence and BlockChain technologies are emerging as disruptive technologies and are beginning to affect our daily lives. These technologies will have a significant societal impact. Europe and its digital single market needs to be ready to adopt, explore and apply the benefits from these technologies in a safe and secure cyber environment. Traditional approaches to security will have to be adapted in order to cope with issues of scalability and modified timelines.

EU cybersecurity market grows slower than other regions in the world.

In 2016, the EU cybersecurity market was estimated at €20.1bn and compares favourably with the cybersecurity market of other global regions. The CompoundAnnual Growth Rate (CAGR) of the EU market however is 6%, whereas the average growth rate is around 8%, and is growing slower than all other major regions.

We see an increase in monetisation of cyber crime, crime as a service and of targeted attacks.

Targeted attacks, like ransomware, entered the top ENISA 2016 cyber threats. According to the ENISA Threat landscape, in 2016, ransomware was the primary element for the manifestation of monetization of the activities of cyber-criminals, with an estimated loss of one billion US $ for the entire year 2016. More recently, the WannaCry ransomware campaign caused chaos due to its massive distribution, affecting more than 150 countries and infecting over 230,000 systems. Next to ransomware, information theft is the main area of ‘malware innovation’ in 2016. Targets affected included political organisations and democratic institutions.

We become more aware that our rights online and even our democracy are at risk.

The scandal of hacked emails in the US election in 2016 and the measures taken in Europe to prevent interferences in elections cannot be ignored and are other examples that show us that there is more to be done to address the continuous changing landscape of threats and challenges in cyber space.

Small devices, which we sometimes forget are connected to Internet, are used to build very large cyber attacks affecting targeted businesses and infrastructures. In October 2016, the Mirai botnet compromised IoT devices and household routers, where cases are documented that life was at risk because normal emergency telephone calls were not accessible. This raises the question of who is liable in such events.

Cyber space can be used for sabotage, espionage and warfare.

Hybrid warfare (adding cyberwarfare to conventional and unconventional warfare tools) is evolving without necessarily using the word 'war' in describing the attacks. Some countries are already taking steps to combat these threats. We see specialized institutions and bodies investing in activities related to cybersecurity. I would say that

at this time, at least at the institutional level there is a relatively good understanding of the need for strong cybersecurity. However, given the limited resources and budgets a coordinated approach is required to make sure we do not fail in our mission. Now it is a good moment to ask ourselves some questions, and based on the replies to see how we can improve the context and go to the next stage/level of preparedness and readiness to address the emerging challenges.

Cooperation and exchange of information

In the majority of countries, private companies own critical infrastructure and critical services are provided by the private sector. Therefore, a high degree of communication and cooperation can be an effective way for governments to understand the needs and challenges of private companies, but also to ensure that the necessary measures are implemented to achieve a sufficient degree of cybersecurity. For this reason, **public-private partnership (PPPs), information sharing and analysis centres (ISACs) and cyber security exercises** can be an effective tools to ensure that a nation's essential industries have the best protection possible.

ENISA has worked towards this direction offering incentives and actual recommendations on how to setup and run PPPs and ISACs. Moreover, ENISA organises cybersecurity exercises like Cyber Europe, which are **simulations of large-scale cybersecurity incidents that escalate to become cyber crises**.

More specifically:

- For PPPs, trust has been recognised as the basic element between public and private sector in order to have the best possible protection between them. PPPs can cover topics like policy making, funding and collaboration options and best practices on cybersecurity.
- For ISACs, open communication and knowledge sharing is the corner stone for building collaboration between the private sector stakeholders. The government can act as a facilitator bring all key players together.
- Cyber security exercises enable competent authorities to test existing emergency plans, target specific weaknesses, increase cooperation between different sectors, identify interdependencies, stimulate improvements in continuity planning, and generate a culture of cooperative effort to boost resilience. Cyber exercises are important tools to assess preparedness of a community against natural disasters, technology failures, cyber-attacks and emergencies.

2. Cybersecurity Taxonomy

Cybersecurity operates on many different levels and one of the functions of the strategy should be to address coherently all the different levels of cybersecurity needs.

The following image draws on the Maslow's Pyramid of needs approach to categorising cyber space and cybersecurity needs in a hierarchical way. Any EU strategy must cover all aspects of the cybersecurity to ensure a comprehensive approach to addressing the cyber challenges of tomorrow.

Figure 1: Layers of cybersecurity needs.

Figure 1 presents ENISA's perspective on cybersecurity needs, starting with EU core values at the top, and, working the way down, to the basic citizens' needs. The following paragraphs provide a short description of the pyramid and the layers as cybersecurity requirements.

Layer 1. Basic security protection. Safety and security of citizens in cyber space is not a matter of debate. Under no circumstances, the safety of users should be at risk due to actions in cyber space. Furthermore, preventive measures should be applied; education, awareness and cyber hygiene are very important. As you wash your hands to protect your health, or lock the door of you home to protect your properties, in the cyber space, you also have to be aware of the risks. Thus, every user should be aware and should be using minimum-security protection actions: firewalls, malware detection, apply updates and patches to safeguard devices and IT systems.

Layer 2. Critical asset protection. The Network and Information Security (NIS) directive brings new security requirements for protecting essential services and digital services in the EU. These requirements are the most recent ones; since past decade, several communications addressed the need for Critical Information Infrastructure Protection (CIIP). The implementation of NIS directive is an important step in protecting EU CIIP, the cooperation of CSIRTs via the CSIRTs network, the improvement of EU collaboration via the Cooperation Group, etc. Secure infrastructures in sectors like energy, transport, banking etc. provide bases for the society to function and for economy to grow.

Layer 3. Digital single market protection. The cyber space and technology evolution provide many opportunities for business development. Besides critical infrastructures, all business needs to be protected as their reliance on cyber space is increasing. The exposure to cyber space related threats like cyber attacks, cyber crime, cyber sabotage and/or cyber espionage becomes more visible every day and is visible in media almost daily. Security measures should be deployed and an EU approach is needed to address and support business in general and SMEs in particular in their cybersecurity needs.

Layer 4. Global stability protection. Espionage and war have millenniums of history. Cyber space associated terms are already in place; several actions during the past decade were assessed as cyber war, cyber espionage etc. There are several discussions on the need for cyber norms and cyber diplomacy. Cyber defence activities are funded and developed across the globe. Given the nature of cyber space, adequate measures and international agreements need to be in place to guarantee global stability in front of risks. The EEAS activities, the Tallinn manual, etc. are good examples of activities at this level that need to be supported and extended.

Layer 5. Democracy and human rights protection. Safety vs security balance is changing in the global physical world. Some emerging technologies (autonomous vehicles, etc.) – require new discussions on the ethical aspects. Human rights protection online is not an easy objective to achieve. Protection of the core EU values online needs to be guaranteed in the cyber space. Impact of new technologies, products and services needs to be assessed and adequate measures should be in place – i.e. any new technology should preserve rights, liberties and democracy. There are interdependencies between the layers described above. Protection of the critical assets, i.e. critical information infrastructures provides a good base for other businesses, part of the digital single market, to flourish while supporting citizens' needs as well. Cybersecurity for citizens, infrastructures and business, in current context, cannot be achieved without addressing the challenges associated with globalisation. In the globalized context, cyber diplomacy needs to be in place, as well as the means to prevent, defend and protect the EU, its citizens, infrastructures and businesses. Furthermore, it should be noted that core EU values and norms, ethics, need to be applied to all levels in the cyber space: to all products and services available for EU customers, independent of their place of production/development in the world.

3. EU Legislation

In 2009, the European Commission published the Communication on Critical Information Infrastructure Protection (CIIP)[1]. In the following years, COM launched several strategic level documents that address challenges of the cybersecurity domain:

- the EU Cybersecurity strategy in 2013, introducing a directive on security of network and information systems;
- the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS regulation) in 2014**;**
- the European Agenda on Security[2] in 2015, the Digital Market Strategy, and the Directive on payment services in the internal market (PSD2)[3].

In 2016, a Joint Framework on countering hybrid threats was published and the cPPP initiative was launched. In 2016 the European Parliament and Council adopted the General Data Protection Regulation (GDPR), Law Enforcement Authorities (LEA) data protection Directive, the Passenger Name Records Directive and the Directive on security of network and information systems (the NIS Directive).

The NIS Directive is the first piece of legislation at the EU level that addresses network and information systems and the essential services playing a vital role in society, from ensuring the supply of electricity and water, to the provision of healthcare and transportation. These initiatives demonstrate that political awareness results in political action.

Furthermore, a connected Digital Single Market has been identified as one of the top priorities in the roadmap for a More United, Stronger and More Democratic European Union. The Cyber-Security package was announced by the President of the European Commission Mr Jean-Claude Juncker at the State of the Union letter of intent to the European Parliament on 13 September 2017.[4]

The Cyber-Security package sets concrete measures to respond to the changed cyber-threats landscape including:

- a proposal to strengthen the EU Agency for Network and Information Security (ENISA), including a proposal to harmonise cybersecurity certification approaches at the European Union level;
- an implementation toolkit for the Network and Information Security Directive;
- a blueprint for effective response in case of cyber-attacks affecting several Member States;
- enhancing the Union's strategic autonomy by boosting research capacity and building effective cyber-defence, cyber-hygiene and the right skills both inside Europe and with partners worldwide, including NATO.

In addition to the above, it should be noted that several proposals are being discussed between the European Parliament and the Council that address cybersecurity issues:

- Proposal for a regulation Cybersecurity act COM(2017)0447 final/2;

[1] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
[2] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366
[4] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_en.pdf

- Proposal for a Directive establishing the European Electronic Communications Code COM/2016/0590 final;
- Proposal for ePrivacy Regulation and repealing Directive 2002/58/EC COM(2017)10final;
- Proposal for a regulation on a framework for the free flow of non-personal data in the European Union COM(2017) 495 final;
- Proposal for directive on copyright in the digital single market COM(2016) 593 final.

On the implementation side, the EU agency for Network and Information security (ENISA) was established in 2004 to support the security of network and information systems across the EU, and its mandate was renewed in 2009 and 2013 respectively.

Even with its limited resources, of about €11 million/year, ENISA has published and covered nearly every upcoming topic relevant for cybersecurity and cyber space. Examples of published reports include the ENISA Threat Landscape, pan European cybersecurity exercises, reports on Smart Airports, Smart cities, eHealth, to name a few.

It is known that any cyber security incident could have a cross boarder effect on Member States. To improve preparedness of the EU to cyber attack, in July 2016 the Directive on Security of network and information systems (the NIS Directive) has been adopted giving Member States 21 months to implement the Directive into their respective national laws. The NIS Directive aims to raise levels of the overall security and resilience of network and information systems across the EU.

In amongst other measures, the NIS Directive requires the EU Member States to adopt and implement a national strategy on the security of network and information systems (national NIS strategy). On this task, the Directive requires ENISA to support Member States by providing expertise and advice and by facilitating the exchange of good practice.

Since 2012 ENISA has supported Member States creating their national NIS strategy through so called Article 14 requests[5] and indirectly through sharing of good practices. ENISA has also developed guidelines to support the individual objectives of the strategies (the most highly implemented objectives of the EU strategies are Critical information infrastructure protection, establishing public-private partnerships, addressing cybercrime, establishing incident reporting mechanisms, organising cyber security exercises, establishing cyber response capability and engaging in international cooperation).

Currently all 28 MS have a National NIS Strategy. With the adoption of the NIS Directive, many Member States realised that their strategy needs to be updated to reflect the specific requirements of the Directive.

In September 2017, the European Commission proposed the Cybersecurity act[6], a Regulation that aims at further increasing EU cyber resilience, deterrence and defence. The Regulation proposal, which is currently under discussion at the Council and the Parliament, builds on two pillars:

1. A permanent and stronger mandate for ENISA **to assist Member States** in effectively preventing and responding to cyber-attacks; and
2. The creation of a European cybersecurity certification framework to ensure that cybersecurity products, services, and possibly processes meet certain cybersecurity requirements.

Further analyses on the new proposal are made available in Chapter 5 of this document.

[5] Article 14 of the Regulation (EU) No 526/2013
[6] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN

4. Challenges ahead

1. How do we adapt current security approaches to deal with the timescales and scale of deployment of new technologies such as IoT?
2. Are our human rights respected online? Are we as citizens protected enough?
3. Are our critical infrastructures well prepared for the threats in cyber space?
4. Do we have enough human and financial capacity to address the threats to the digital single market? The EU's access to the cybersecurity skills is limited since a shortage of 350.000 professionals have been reported by the industry.
5. Programs should be put in place, at the earliest opportunity, to prepare and assess the likely impact of new disruptive technologies. Specific assessments need to be made in respect of each technology from a technical, political and societal perspective. Following these assessments, the need for new policies and legislative initiatives needs to be addressed.
   European industry, governments and citizens should have access to competitive secure and trustworthy products and services that allow data and service portability and do not depend on single (monopolistic) service providers.
6. Member States should further invest in security awareness training and cyber hygiene. This includes promoting cybersecurity as a career choice in schools and universities, encouraging industry to develop cybersecurity training schemes that are aligned with established career paths and encouraging the retraining of adults and long life learning programs in this area.

5. Cybersecurity act: A proposal to harmonise cybersecurity certification approaches at the European Union level

Harmonising cybersecurity certification approaches at European level can **increase the transparency of information on the security level of ICT products, processes and services** in the digital single market for all its participants.

The proposed certification framework will provide **EU-wide certification schemes** as a comprehensive set of rules, technical requirements, standards and procedures. This will rely on agreement at EU level for the evaluation of the security properties of specific ICT-based products, services or even processes. By undergoing a certification process, we will be able to **attest** that ICT products and services **meet specific cybersecurity requirements**.

The resulting certificate will be **recognized in all Member States**, making it easier for businesses to trade across borders and for purchasers to understand the security features of products and services. Should these cybersecurity requirements are based on internationally accepted standards, the resulting certificate would also provide a certain level of assurance outside EU.

ENISA is expected to contribute to the emerging EU framework for the certification of products and services and carry out the **drawing up of certification schemes** in line with the Cybersecurity Act **providing stakeholders** with a sound service that leads to efficiencies and value in the EU.

Under its 2018 programming document[7], the Agency seeks to **explore how existing schemes could be transposed** to the European cybersecurity certification framework proposal while also **collect high-level requirements** for an industry-led lightweight certification scheme or labelling.

[7] https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2018-2020

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu