Adequate and effective cybersecurity: state of play

Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht – Cybersecurity Conference organised by the Austrian Presidency of the Council of the European Union.

VIENNA, AUSTRIA

3RD DECEMBER 2018

Ladies and gentlemen,

On behalf of ENISA, I kindly thank you for this opportunity to share our views about cybersecurity and its state of play.

Before I begin, let me thank **the Presidency trio – Estonia, Bulgaria, and Austria** – for their success in promoting a culture of network and information security in Europe.

Back in September 2017, we have welcomed the publication of the proposal of the European Commission on the future role and mandate of ENISA with great pleasure and look forward to entering into force in 2019.

I hope to see in the next two weeks a successful conclusion of trialogue negotiations in respect of the proposed cybersecurity act and its entry into force in 2019.

I believe that cybersecurity, in terms of secure products, services and processes will serve as the key differentiator that will support the European citizens and industry.

Cybersecurity in the EU

In the last few years, there have been **many new developments in the cyber world**. We continue to witness the 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, Quantum Computing, and BlockChain technologies are emerging as **disruptive technologies** and are beginning to affect our daily lives.

These technologies are beginning to a **significant societal impact**.

Europe and its digital single market needs **to be ready adapt and reap 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 these new challenges.

Research is indicating that the 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 Compound Annual Growth Rate (CAGR) of the EU market however is 6%, whereas the average growth rate is around 8%.

We are seeing an increase in monetisation of cybercrime, crime as a service and targeted attacks. Targeted attacks, like ransomware, are now listed as top cyber threats in the ENISA Threat Landscape report of 2017.

The scale of cyber incidents can be seen in the WannaCry ransomware incident caused which caused chaos due to its massive distribution which affecting more than 150 countries and infecting over 230,000 IT systems.

Our rights online and democracy are now matters of public debate. The incident relating to hacked emails in the US election in 2016 and the measures taken in Europe to prevent interferences in elections cannot be ignored. The more we look at this issue the more we realise that there is more to be done in continuous changing landscape of threats and challenges in cyber space.

Cooperation and exchange of information

In the majority of the EU countries, **private companies own critical infrastructure and critical services are provided by the private sector.**

Consequently, a high degree of communication and cooperation is necessary. And this can be an effective way for member states not only to understand the needs and challenges of private sector but also to ensure that the necessary measures are implemented to achieve a sufficient degree of cyber security.

For this reason, **public-private partnership (PPPs), information sharing and analysis centres (ISACs) and cyber security exercises can be an effective tools** to assist in managing cyber threats.

ENISA has worked towards this direction by offering incentives and actual recommendations on how to setup and run PPPs and ISACs. Moreover, ENISA organises **cybersecurity exercises every two years**. **This ENISA's flagship activity "Cyber Europe" has simulated large-scale cybersecurity incidents.**

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.

ENISA has developed a **so- called "Maslow's Pyramid of needs approach" to categorise cyber space and cybersecurity needs in a hierarchical way ranging from basic cyber hygiene to cyber ethics.**

Any EU strategy must cover all aspects of the cybersecurity to ensure a comprehensive approach to addressing the cyber challenges of tomorrow at every level.

Policy Context - certification

Technological transformation affects all areas of modern life, from education and jobs to the welfare system. Change is already happening, and at a fast pace. Europe needs to embrace these changes in order to protect its citizens as well as to allow them to seize new opportunities for industry.

Securing network and information systems in the European Union is essential to keep the online economy running and to ensure prosperity of our society. **Under this prism, on September of 2017 the Commission adopted a cybersecurity package.** The package builds upon existing instruments and presented new initiatives to further improve EU cyber resilience and response.

One of the main elements **is the Cybersecurity Act Proposal, which includes provisions on a European Cybersecurity Certification Framework.**

The proposed cybersecurity certification framework, which is currently with the co-legislators) will aim to provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. This will be based on an agreement at EU level for the evaluation of the security properties of a specific ICT-based product, service or process.

The certification framework will ensure that **ICT products, services and processes that have been certified in accordance with such a scheme comply with specified 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 the product or service.

It is evident that businesses across the EU will **benefit** from the provisions of the Cybersecurity act and the proposed certification framework in particular.

Firstly, new markets will open up for industry.

Secondly, the harmonised **EU wide certification framework** will inherently promote the cross-border flow and exchange of secure ICT products and services. Businesses will be able to work with more homogeneous systems and should therefore require less resources in dealing with diverse compliance schemes.

Thirdly, the level of consumer **trust** will increase the confidence in EU products, services and processes.

Currently, **the landscape** of security certification of ICT products and services **in the EU is quite sparse**. This proposal should greatly increase the level of certification across Europe.

The role of ENISA

Throughout 2018, ENISA has worked alongside the European Commission and Member State authorities to assist in **planning a course of action for the transition to the new EU framework known as Cybersecurity Act.**

Furthermore ENISA **has engaged** with the industry (e.g. manufacturers, health care, IoT) and conformity assessment bodies alike to document their priorities and promote the merits of the framework.

ENISA **has also further developed its relationship** with the standardisation organisations in the EU (CEN and ETSI) and internationally (IEC) in an effort to provide a solid basis of cooperation that is likely to support the development of the certification schemes.

Closing Remarks

The EU has an opportunity to become a **global leader**.

By putting cybersecurity at the forefront of our efforts, the EU has the potential to set the scene and serve as the yardstick for other markets to compare against **by leveraging the collective experience and expertise** of the Member States and European industry.

ENISA, **since 2004**, acts as a centre of expertise dedicated to enhancing network and information security in the Union and supporting capacity building of Members States.

Ladies and gentlemen

In 14 years of its activity ENISA has become an entity in the EU cybersecurity landscape that brings the cybersecurity actors together,

ENISA is ready to begin work in earnest on the new Cybersecurity Certification Framework. The Agency can start preparatory work as soon as the Cybersecurity Act is adopted.

Ideas for initial schemes have already been suggested by the different stakeholders and the Agency is prepared to define a timeline with the Commission and the European Cybersecurity Certification Group (ECCG).

Over the past year, ENISA has been working with all its stakeholder communities to prepare them for contributing to the first schemes and we believe that the majority of these communities are also up-to-speed and ready to contribute.

The Agency has put together a recruitment plan to enable us to grow the certification activity in a consistent manner and is proactively recruiting for reserve lists so as to have additional skill sets in house at the earliest moment.

In conclusion, we have established the momentum in our stakeholder communities that is necessary to ensure an efficient start-up of this activity and are looking forward to a positive outcome from the political process in order to start.

I believe that acting together we will make Europe a better place.

Thank you for your attention.

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 9710
info@enisa.europa.eu
www.enisa.europa.eu