Keynote speech at the Digital Society Conference 2017

Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht - The Digital Society Conference 2017

BERLIN, GERMANY
NOVEMBER 2017

Thank you for the opportunity to address you here today in Berlin.

On 13 September 2017 the new cybersecurity package, was announced by President Juncker in his State of the Union speech. The newly proposed package indicates that political leaders are committed to building the future wealth of the EU by leveraging the opportunities of the digital society.

In the last few years, there have been many new developments in the cyber world, including the digitalisation of our daily lives, new technologies, new cyber threats, and new cyber stakeholders.

New technologies are changing the cyber landscape. The Internet of Things (IoT) is increasingly deployed, with approximately 20 billion devices expected to be deployed before 2020. Robots, Artificial Intelligence (A.I.), and Blockchain are emerging as disruptive technologies that are beginning to affect our daily lives.

New technologies bring benefits and challenges as is the case with cryptocurrencies, on which the European Union Agency for Network and Information Security (ENISA) published a paper earlier this year.

As a result, traditional approaches to security have to be revisited to cope with issues of scalability and modified timelines.

In current perspective, cybersecurity is becoming an increasing challenge for our societies.

This trend is demonstrated by an increase in monetisation of cybercrime, crime as a service, and of targeted attacks. There is an increasing awareness that our rights online, including democracy, are at risk, and of the potential of using cyber space for sabotage, espionage, and warfare.

Without significant improvements to cybersecurity in Europe, the risk of a severe negative impact continues to increase.

However, cybersecurity also presents an opportunity to promote a new of generation products and services that incorporate security and privacy by design. It is proposed that this goal will be achieved by:

- Strengthening ENISA, the EU Cybersecurity Agency by providing it with additional financial and human resources that better position the Agency to assist Member States, EU institutions, businesses, and citizens in achieving a higher level of cybersecurity, and to support effective implementation of the Network and Information Security Directive (NISD).
- Developing an EU cybersecurity certification framework as a voluntary framework that builds on existing national certification schemes and aims to enhance trust and confidence in the digital products and devices available on the European market.

The Cybersecurity Act proposed by the Commission presents a chance for the European legislator to increase IT security based on a voluntary and market-driven approach.

Just to say a few words about the Internet of Things:

The onset of IoT presents several challenges to our contemporary societies. Rapid technological developments are not matched by proactive regulation, certification, or standardisation. Additionally, IoT entails a market-driven ecosystem, where functionality and low cost rather than security and safety are

seen as the main drivers. I believe this is an explosion waiting to happen and, when it does, end users will cry about the lack of security and privacy by design

ENISA has provided recommendations on:

- Smart homes;
- Smart cars and autonomous driving;
- Smart hospitals and eHealth;
- Smart cities and intelligent public transport;
- Smart airports;
- Smart grids.

Clearly, there is work to be done.

Standard security techniques and practices need to be reconsidered in light of the IoT due to its inherent particularities. Additionally, the impact of two fundamental pieces of legislation need to be re-visited in the light of the extraordinary growth in IoT devises including those deployed in our critical infrastructure.

ENISA has contributed to developing IoT solutions in a number of ways.

For example, ENISA set up an IoT Expert Group that aims at giving initial advice before the end of 2017. Furthermore, the agency drafted a common position paper on cybersecurity with select semiconductor industry representatives calling for minimum security requirements for the IoT. ENISA has also been active in developing baseline security measures for the IoT.

However, several outstanding issues remain.

In particular, it is necessary to address the question of legal liability in the context of the IoT. It is also important to incorporate cyber security in all stages of the lifecycle of products and services. The NISD and GDPR have to be implemented and interpreted in the light of the IoT development and deployment. IoT standardisation and certification of products are currently lagging behind demand.

The consideration of ethics by design is a more recent concept that gains importance as technology is increasingly deployed at closer proximity to humans.

Artificial Intelligence and Robotics will undoubtedly lead to societal changes of great magnitude across the spectrum of human activities. The TEU (Treaty on European Union) sets the legal framework for our core values and principles in Europe. Emerging and disruptive technologies are raising new challenges and there is a need to interpret existing legislation in the context of these new technologies.

This has special relevance considering that software now needs to be programmed to make the same decisions as humans have made intuitively for centuries.

An example of a possible difficult decision is how an autonomous driving vehicle would be programmed to react to a potential head on collision with another vehicle. Will the vehicle maintain its path or will it swerve to avoid a collision but potentially putting other road users at risk?

These technological developments raise questions about software liability and how liability will be addressed in this type of situation.

It is of vital importance that security by design, privacy by design, and ethics by design are addressed in the cyber world of today and tomorrow.

ENISA envisages a new way forward for Europe's digital society, where the security, as well as the profitability of European digital products and services are ensured.

The EU institutions, MSs, civil society, and industry – all stakeholders – need to work together to address cyber challenges and ensure that policies are in place that prepare the European economy to embrace emerging technologies and benefit from the opportunities they provide.

The world of interconnected objects brings with it many new opportunities but also new risks. It is our job to maximise opportunities while keeping the risks under control.

As the EU cyber security agency, ENISA will work together with policy makers and industry to ensure that cybersecurity is an enabler of, and not a barrier to, economic progress.

Thank you for your attention.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu