Security Challenges and best practices in the IoT Environment

Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht - Public Hearing on Security Challenges and best practices in the IoT Environment

EUROPEAN PARLIAMENT, BRUSSELS
7TH NOVEMBER 2017

Members of the European Parliament, Ladies and Gentlemen, thank you for the opportunity to address you on this important topic at this opportune time.

The importance of cyber security in Europe is evidenced by the recent proposals of President Juncker in his State of the Union Address on the 13th September 2017, the publication of the new European cyber security strategy 2017 and the Cybersecurity Act[1], the Commission's proposal for the new and strengthened EU Cybersecurity Agency ENISA (the European Union Agency for Network and Information Security) which includes a proposal for regulating certification. On this basis it is clear that our political leaders are committed to building the future wealth of the EU by leveraging the opportunities of the Digital Society.

However, 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 cyber security, cyber warfare, cyber espionage, cyber terrorism and cyber defence are becoming increasing referred to daily discourse by our citizens and politicians.[2] Some new concepts that have emerged in the last few years include fake news, cyber ethics, cyber diplomacy and digital sovereignty.

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 deployed before 2020. Robots, Artificial Intelligence and Blockchain technologies are emerging as disruptive technologies and are beginning to affect our daily lives. New technologies can produce benefits as well as security challenges, as is the case with cryptocurrencies, on which ENISA published an opinion paper earlier this year.[3] Traditional approaches to security will have to be modified in order to cope with issues of scalability and modified timelines.

In 2016, the EU Cyber Security 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%, and is growing slower than all other major regions.[4]

Before we explore the way forward we need to reflect on some specific examples as to why cyber security is becoming an increasing challenge for our society.

We see an increase in monetisation of cyber crime, crime as a service and of targeted attacks. Targeted attacks, like ransomware, have entered the top ENISA 2016 cyber threats. According to ENISA Threat

---

[1] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*, COM(2017) 477, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:477:FIN

[2] ENISA, *ENISA Overview of Cyber Security and Related Terminology,* October 2017, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

[3] ENISA, *ENISA Opinion Paper on Cryptocurrencies in the EU,* September 2017, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-opinion-paper-on-cryptocurrencies-in-the-eu

[4] ENISA, *Cybersecurity as an Economic Enabler*, 2016, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler

landscape[5], 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 ransomware campaign, which became known as the WannaCry Outburst, caused chaos due to its massive distribution, affecting more than 150 countries and infecting over 230,000 systems[6]. Next to ransomware, information theft are the main areas of 'malware innovation' in 2016. Targets affected included political organisations and democratic institutions[7].

We become more aware that our rights online, including our democracy, are at risk. The scandal of hacked emails[8] in the US election in 2016 and the measures taken in Europe to prevent interference to elections[9, 10, 11] cannot be ignored and are other examples that show us that there is more to be done to address the continuously changing landscape of threats and challenges in cyber space.

Small devices that sometimes we even forget that they are connected to Internet serve and 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..[12]

An upgraded variant of the malware targeted[13] Deutsche Telekom Voice over IP Routers[14] and almost one million landline subscribers lost service on Sunday 26 November 2016 in Germany. Cases are documented and described where life was considered to be 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 necessary using the words 'war' in describing the attacks. Some countries are already taking steps to combat these threats[15]. Current efforts

---

[5] ENISA Threat Landscape Report 2016, ENISA publications covering threat landscape are available at: https://www.enisa.europa.eu/topics/threat-risk-management?tab=publications

[6] ENISA, *WannaCry Ransomware Outburst*, May 2017, available at: https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

[7] German parliament foiled cyber attack by hackers via Israeli website, Reuters, 29/03/2017, available at: http://www.reuters.com/article/us-germany-cyber-idUSKBN1701V3

[8] Hillary Clinton Email Archive on WikiLeaks, available at: https://wikileaks.org/clinton-emails/emailid/30373

[9] Russian cyber-attacks could influence German election, says Merkel, The Guardian, available at: https://www.theguardian.com/world/2016/nov/08/russian-cyber-attacks-could-influence-german-election-says-merkel

[10] France's Hollande seeks 'specific measures' against election hacking, Politico, 15/02/2017, available at: http://www.politico.eu/article/frances-hollande-seeks-specific-measures-against-election-hacking-russia-putin/

[11] Dutch will count all election ballots by hand to thwart hacking, The Guardian, available at: https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking

[12] Dyn, *Dyn Analysis Summary Of Friday October 21 Attack,* 26 October 2016, available at: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[13] ENISA, *"Mirai" Malware Attacks Home Routers,* 14 December 2016, available at: https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

[14] Deutsche Telekom probes potential hacking after router issues, Bloomberg, 28/11/2016, available at: https://www.bloomberg.com/news/articles/2016-11-28/deutsche-telekom-probes-potential-hacking-after-router-issues

[15] European Centre of Excellence for Countering Hybrid Threats established in Helsinki, Finnish government site, Government Communications Department, on 11.4.2017, available at: http://valtioneuvosto.fi/en/article/-/asset_publisher/10616/eurooppalainen-hybridiuhkien-osaamiskeskus-perustettiin-helsinkiin

at EU level include the cyber diplomacy toolbox.[16] The application of international law in cyber space was addressed in the Tallinn Manual[17], which was updated and expanded in the Tallinn Manual 2.0[18].

The message is clear – unless Europe substantially improves its approach to cyber security the risk of a significant impact on our lives continues to increase. However, cybersecurity should not only be seen as a negative obstacle but as an opportunity to promote a new generation of products and services that are made and or delivered in Europe with security by design as a central component to the products and services.

It is proposed that this goal will be achieved in a number of ways.

Firstly, by the **strengthening** of the European Union Agency for network and Information Security (**ENISA**). The proposal from the Commission which is now being considered by the Council and the Parliament proposes to increase the financial and human resources of the Agency in order to put the Agency in a stronger position to support Member States, EU institutions, businesses and citizens in achieving a higher level of cyber security. The Network and Information Security Directive (NISD) which comes into force next year, places requirements on Operators of essential services and Digital Service Providers to have minimum level of cyber security in their networks and to report on certain levels of incidents so that the EU industry and service sectors can learn from the experiences and to avoid similar incidents.

It is proposed that ENISA with its greater resources will be better positioned to have a stronger role in policy development and implementation including helping the Member States meet the requirements of the NISD. It is also proposed that ENISA will act as a focal point for information and knowledge sharing and play an important role in both operational and crisis management across the EU. In addition, the proposal to organise annual cyber exercises should enhance the European preparedness to manage cyber incidents.

Secondly

As Europe strives towards a single cybersecurity market there is **a need to build trust and confidence into the digital products and devices that are being used**. To achieve this ambition **an EU cybersecurity certification framework is being proposed** where ENISA would be at the heart of the framework. It is proposed that this policy will result in products and services being put on the market that will be certified and provide the necessary assurance to their users that the products and services are fit for purpose. The EU framework should bring a clear benefit for producers and service providers in that they will only need to be certified in one Member State so as to be made available in the entire EU market. This approach should increase speed to market, reduce the financial burdens of achieving national certification in each Member State and facilitate standardisation across the EU market.

This approach draws on an analogy from the telecommunications market developed in the 1990's where once there were many different mobile phone standards operating across the EU, which did not allow for interoperability when citizens crossed borders. Today, Europe has the GSM mobile phone standards implemented in all member states and where users can cross borders seamlessly and obtain service in a

---

[16] Council of the EU, *Cyber attacks: EU ready to respond with a range of measures, including sanctions*, 19/06/2017, available at: http://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[17] Schmitt, Michael N., ed. *Tallinn manual on the international law applicable to cyber warfare*, Cambridge University Press, 2013, available at: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

[18] Schmitt, Michael N., ed. *Tallinn manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2017.

standardised way. The success of the GSM standardised process put Europe in the lead globally for the provision of cross border mobile telecommunications services.

Given the complexity of the market, it is proposed **that this framework is voluntary and would build on existing national certification schemes**. It is also proposed to subdivide the market into a number of areas to include

1. critical and high risk areas
2. widely deployed digital products and
3. low cost mass market products such as the Internet of Things (IoT).

While some concerns have been expressed by some Member States in relation to this proposal, that there are existing schemes in place to meet the needs of the market, I believe that none of the few existing international (like common criteria) or national schemes serve the full 28 member states and that Europe needs to push forward for a European solution for all of Europe. I believe there is a compromise solution where some very sensitive equipment that are designed for national use only could be managed by way of an exception to this framework, while most products and services are manufactured or delivered with the intention of reaching the 500 million EU citizens and the global export market. With this approach, I believe that Europe should immediately address the widely used and mass-market goods and services that need to be certified and realise the economic opportunity as well as the confidence and trust building that this certification framework will bring.

Most importantly, there is a chance to build up a new European, globally standardised and accepted, Ecosystem of Certification Labs which will for the benefit of the European Citizens increase significantly the IT security of products and services.

In the long term, the question of regulating product liability will stay, as the Mirai or WannaCry cases have shown. Certification is a start to build a trustworthy Cyberspace. My message is: take the Cybersecurity Act as a chance to increase IT security based on a voluntary and marked driven approach.

Turning more specifically to the IoT environment, ENISA, the EU cyber security agency, has been working for some time in identifying security threats and risks in the Internet of Things and on providing recommendations to strengthen its security. ENISA has already provided recommendations on securing:

- Smart homes;[19]
- Smart cars and autonomous driving;[20]
- Smart hospitals and eHealth;[21]
- Smart cities and intelligent public transport;[22]
- Smart airports;[23]

---

[19] ENISA, *Security and Resilience of Smart Home Environments,* December 2015, available at: https://www.enisa.europa.eu/publications/security-resilience-good-practices
[20] ENISA, *Cyber Security and Resilience of Smart Cars,* January 2017, available at: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
[21] ENISA, *Cyber Security and Resilience for Smart Hospitals,* November 2016, available at: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
[22] ENISA, *Architecture Model of the Transport Sector in Smart Cities,* January 2016, available at: https://www.enisa.europa.eu/publications/smart-cities-architecture-model
[23] ENISA, *Securing Smart Airports,* December 2016, available at: https://www.enisa.europa.eu/publications/securing-smart-airports

- Smart grids.[24]

The IoT world will result in everything being connected everywhere. And it needs to be secure.

There are numerous challenges and issues concerning the security of the Internet of Things. We are witnesses to rapid technological developments in the area. We have not so far witnessed equally responsive efforts in terms of regulation, certification or standardization. Consumer Internet of Things devices are usually low-cost, with security being seen not as a necessity but as an added-value service by many developers and manufacturers alike. It is thus a market-driven ecosystem, where security and safety are not seen as the main drivers.

Standard security techniques and practices need to be reconsidered in the light of Internet of Things due to its inherent particularities. Consider the case of security updates. We have recently witnessed an enormous ransomware campaign targeting computing systems. The most significant recommendation provided by ENISA was to update the software on their computers. But when talking about the Internet of Things, how would such updates be enforced? Smart locks, light bulbs and home appliances, connected and autonomous cars, smart medical devices. How can we be sure that all of these smart devices are always up-to-date in terms of security?

The existing security issues and concerns over the Internet of Things should not be seen as a hindering factor for its deployment and the grasping of the numerous associated benefits. From these challenges, opportunities arise that will lead to secure, safe and prosperous deployments of Internet of Things across Europe and the world.

The European Union has two fundamental pieces of legislation to assist in this direction. The Network and Information Security Directive (NISD) and the General Data Protection Regulation (GDPR). The special intricacies of the Internet of Things need to be carefully examined in light of the legislation.

Clarifications and possible extensions and/or amendments might be necessary in order to achieve the goal of security and privacy of the Internet of Things.

In order to identify solutions ENISA has set up an Internet of Things Security Expert Group that aims at delivering initial advice to the Commission and the MS by the end of 2017 through its active engagement in this year's activities.

Along with select semiconductor industry representatives, ENISA has published a common position paper on cybersecurity[25] calling for minimum security requirements for connected devices and has been encouraging the development of mandatory staged requirements for security and privacy in the IoT.

ENISA is also in the process of defining baseline security measures for the Internet of Things in critical information infrastructures.

Despite these efforts, there are a number of outstanding issues that need to be addressed. These include:

---

[24] ENISA, *Communication Network Interdependencies in Smart Grids,* January 2016, available at: https://www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids

[25] ENISA, *Infineon – NXP – STMicroelectronics – ENISA Common Position on Cybersecurity,* December 2016, available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

- Addressing he question of legal liability in the context of the Internet of Things
- Addressing security in all stages of the life cycle of products and services. Accordingly, there is a need to develop a harmonized scheme and define baseline security requirements to ensure and promote security in the Internet of Things.
- The NISD and GDPR have to be implemented and interpreted in light of the features of the Internet of Things.
- Standardization and certification of Internet of Things are lagging behind demand.
- Holistic approaches are needed due to the diverse nature of the IoT.
- Raising awareness in regard to Internet of Things security is a fundamental first step forward.
- The delivery of ethics by design in the world of the IoT

The consideration of ethics by design is a more recent concept. As technology is deployed increasingly closer to humans, Artificial Intelligence and Robotics will undoubtedly lead to societal changes of great magnitude across the spectrum of human activities. The Treaty on European Union (aka Lisbon Treaty) sets the legal framework for our core values and principles in Europe. There is a clear need to protect our fundamental rights, which includes freedom of expression, personal data and privacy. Emerging / disruptive technologies are now raising new challenges and there is a need to interpret existing legislation in the context of these new technologies.

Imminent commercialization of autonomous systems (i.e. robots) and Artificial Intelligence are competing to deliver many functions until now reserved for humans. Software now needs to address and needs to be programmed to make the same decisions as humans have done for centuries.

Where humans are held responsible for their decisions and actions in a court of law the next generation of robotics and autonomous machines, which will be executing the actions of tomorrow, will have to be examined in a different way. 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 technology developments raise questions about software liability and how liability will be addressed in this type of situation or when software is compromised by malware, which is subject to exploiting a vulnerability or a deliberate sabotage of the software.

The European Parliament, together with the EU institutions, MS, civil society and industry need to work together, to address these type of challenges and put in place policies to ensure that our economy is ready to embrace these emerging technologies and benefit from the economic and social opportunities from the deployment of IoT.

In summary, the world of interconnected objects brings with it many new opportunities but also new risks. Our job is to maximise the opportunities whilst keeping the risks under control. In this speech, I have outlined some actions that need to be undertaken in order to achieve this goal. As the EU cybersecurity agency, ENISA will support this process and will work together with policy makers and industry to make sure 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