Security and Liability in the Internet of Things

Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht

BRUSSELS

7TH JUNE 2017

Ladies and gentlemen,

Thank you for the the opportunity to address you today on **Security and Liability in the Internet of Things (IoT)**.

Estonia 2007[1], Georgia 2008[2], Iran (Stuxnet) 2010[3], the Snowden[4] revelations of 2013, are only a few examples of the new virtual Wild West in cyber space.

In the past, you needed a gun to rob a bank, today an equivalent amount of damage can be achieved from the action of a fingertip on a keyboard. This exercise can be performed from any place in the world. Crime, espionage, sabotage and even international conflicts move from the so-called real world into the virtual cyber world. On top of this, **the terrorists' attacks in Brussels and Berlin last year resulted in a new debate on the use of cryptography**[5] linked to criminal justice in cyber space[6].

The **scandal of hacked emails**[7] in the **US election in 2016 and the measures taken in Europe to prevent interferences in elections**[8, 9, 10] cannot be ignored and are further examples that show us that there is more to be done to address the continuous changing landscape of threats and challenges in cyber space. Political organisations and **democratic institutions like national parliaments**[11] **have been also affected by cyber incidents**.

A few years ago, cyber and cyber incidents were unknown to the wide public. Now they are part of our everyday life. Listen please to the next **three real life stories** from recent past.

Let us step back in time to Friday October 21, 2016, after 11:10 UTC. If you typed the URL of some well-known US internet service providers into your browser there was no response[12], and no online services

---

[1] 2007 cyberattacks on Estonia, available at: https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[2] Cyberattacks during the Russo-Georgian War, available at: https://en.m.wikipedia.org/wiki/Cyberattacks_during_the_Russo-Georgian_War
[3] Stuxnet, computer worm, discovered in June 2010, available at: https://en.m.wikipedia.org/wiki/Stuxnet
[4] Edward Snowden, American whistleblower and former National Security Agency contractor, available at: https://en.m.wikipedia.org/wiki/Edward_Snowden
[5] Encryption: Challenges for criminal justice in relation to the use of encryption - future steps, November 2016, Presidency progress report no. 14711/16, available at: http://data.consilium.europa.eu/doc/document/ST-14711-2016-INIT/en/pdf
[6] Outcome of the 3508th Council meeting on Justice and Home Affairs, 15391/16, December 2016, page 7, available at: http://www.consilium.europa.eu/en/meetings/jha/2016/12/st15391_en16_pdf/
[7] Hillary Clinton Email Archive on WikiLeaks, available at: https://wikileaks.org/clinton-emails/emailid/30373
[8] 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
[9] 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/
[10] 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
[11] German parliament foiled cyber attack by hackers via Israeli website, 29/03/2017, available at: http://www.reuters.com/article/us-germany-cyber-idUSKBN1701V3
[12] 2016 cyberattack, available at: https://en.m.wikipedia.org/wiki/2016_Dyn_cyberattack

available. The reason - the Mirai botnet[13] had hacked millions of mainly Linux-based Internet-Of-Things devices and collectively performed a Denial-Of-Service attack on the Domain-Name-Service provider DYN with the result that the IP-addresses of hundreds of company services could not be accessed anymore. It was like removing the telephone number of these organisations in a way that customers could not contact them.

Few months ago, on Sunday 26 November 2016, a friend of mine, fell off the stairs at his home and broke his leg. He was home alone and with big pain, he tried to find the closest phone. He crawled to the VoIP based fix phone. He tried to call emergency services but the phone did not work. His mobile was outside, in the car, and he could not reach it. He had to wait several hours until the phone was operational again. This incident was due to an attack targeting Deutsche Telekom Routers[14] where almost one million landline subscribers lost service on Sunday 26 November 2016 in Germany.

One day, in the middle of May, this year, *let's call him, Mr. Smith* wanted to shut down his notebook, as he noticed a strange symbol on his monitor: two shaking hands and a curious file name have popped up on his desktop. He immediately cut internet connection off. He thought that an infection has just took place. He could not figure out why: he was very careful with clicking on links and mails of unknown origin and visiting suspicious web sites. By assessing the situation in the home WLAN network the other day, it became clear through ransom-messages that other PCs were already infected. As the family declined paying the ransom, family pictures, videos, other personal data went lost. Until then, Mr Smith thought that this would never happen to him. This incident had to do with WannaCry attacks few weeks ago, the ransomware campaign targeting a vulnerability of the Windows OS that caused chaos due to its massive distribution, affecting more than 150 countries and infecting over 230,000 systems[15]. Between these systems affected by WannaCry where many in hospitals, where surgeries could not be performed neither other medical evaluations like X-rays.

You will understand that **any day now this could be the destiny of millions of citizens using digital services and devices**.

We are not 100% secure and it is difficult to be so. The trust in the digital ecosystem is at risk now and even if experts expressed their concerns in the past, their opinions were not listened to. Today we need to do more.

[13] Dyn Analysis Summary Of Friday October 21 Attack, October 26th, 2016, available at: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[14] https://www.bloomberg.com/news/articles/2016-11-28/deutsche-telekom-probes-potential-hacking-after-router-issues
[15] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

Ladies and gentlemen,

Everything is interconnected.

The era of ubiquitous connectivity is upon us, manifested by the ongoing prominent technological developments. What was once futuristic scenarios of Internet-enabled objects, connected vehicles and intelligent decision-making systems, is nowadays an emerging reality. The Internet of Things coupled with Artificial Intelligence and Robotics constitute the foundations of a technological paradigm shift, bringing along major changes in society itself.

The Internet of Things is not a stand-alone technology. It is rather an amalgamation of technologies that aim at reducing or even extinguishing the barriers between the physical and digital worlds in order to facilitate and empower our daily activities. *The Internet of Things is a cyber-physical ecosystem of interconnected sensors and actuators, which enable and support decision-making.* Information lies at the heart of the Internet of Things, feeding into a continuous cycle of sensing, decision-making, and actions. Systems are thus able to understand their surroundings (sensing), process relevant information (for decision-making purposes) and act or react accordingly (acting) changing the status of things.

With the advancements in Artificial Intelligence and the ever-increasing connectivity of everyday objects, it becomes evident that the Internet of Things is progressively permeating and affecting all human activities. We can witness it around us:

- In smart homes, with almost all home appliances offering advanced, Internet-enabled functionalities (smart locks, lights, alarms, coffee machines);
- In smart factories, with the ongoing fourth Industrial Revolution (Industry 4.0);
- In eHealth, with personalized and remotely controlled medical devices (insulin pumps, pacemakers);
- In robotics, with semi-autonomous and autonomous robots being able to perform more and more complex tasks (drones, personal assistance, manufacturing);
- In smart transport, with connected and autonomous vehicles being prepared for widespread deployment;
- In critical infrastructures, with smart grids;
- In everyday life, with wearables monitoring vital bodily functions in real-time and any object being offered Internet of Things features (Internet of Toys, smartphones).

Ladies and gentlemen

Everything is interconnected. But is it secure?

The security threats and risks related to the Internet of Things are manifold and they evolve rapidly. While one can argue that this has always been the case with any new technology, the features of the Internet of Things are such that need to be taken seriously into account.

With the Internet of Things, the digital and the physical worlds are no longer kept apart from one another.

- A hand gesture may control a smart car;
- Patterns of information can be used to regulate the insulin intake of a patient for instance;
- Network relayed commands can control operations in smart factories and energy plants.

Therefore, any security breach in the Internet of Things cannot only severely affect the digital world, but more importantly might lead to grave safety issues in the physical world. Security and safety are tightly integrated, exacerbating relevant threats and risks.

Information and data collection is fundamental to the Internet of Things. The manner in which this takes place is not always transparent to the end users. Whereas informed consent is possible in standard scenarios (consider the case of cookies in the browser), it is not straightforward to envisage how this would be applied in the case of connected toys, smart light bulbs and other devices without a dedicated user interface, for example.

With great impact on citizens' health, safety and privacy, the security threat landscape concerning the Internet of Things is extremely wide. And it is not a theoretical one. During the last year:

- The Mirai botnet comprised of hundreds of thousands of compromised devices was used to take down major Internet services and operators;
- Smart toys were exploited to eavesdrop on children and record their activities unbeknownst to their parents;
- Pacemakers and other medical devices proved to be susceptible to hacking;
- People were refused access to their residences due to ransomware attacks on their smart locks;
- Adversaries were able to remotely affect the driving behaviour of connected vehicles;
- Smart grids and other infrastructures were targeted by malicious cyber-attacks.

Ladies and gentlemen

Everything is connected. And it needs to be secure.

There are numerous challenges and issues concerning the security of the Internet of Things. Largely, it is unchartered territory. 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.

Moreover, security concerns are exacerbated by the complexity of the Internet of Things ecosystem, which is unparalleled. The sheer number of devices (in their billions), their inconceivable and dynamic interconnections, their widespread deployments, as well as the numerous appropriations of technologies by end users, all form a level of complexity that is difficult to manage. Holistic approaches are called for.

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 we provided to citizens 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 question of liability naturally emerges.

Should we consider Internet of Things devices as standard commercial products and apply the same liability rules? Or do the inherent particularities of such devices call for special attention?

There is a great number of stakeholders involved in every IoT device or system. To name a few, hardware manufacturers, network operators, software providers, digital service providers, providers of algorithmic solutions, cloud providers, operators of essential services, end users. Lack of clear assignment of liabilities might lead to ambiguities and conflicts in case of security incidents. It might also lead to the exposing of legislative gaps. Consider the case of an industrial robot or a smart device causing an accident. Who should be held liable? The robot, the hardware manufacturer, the software developers or the regulators, for failing to enforce certification and standardization schemes?

Ladies and gentlemen

Everything is interconnected. And we are working to secure it.

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). While of immense significance, the special intricacies of the Internet of Things need to be carefully examined in light of said legislation. Clarifications and possible extensions and/or amendments might be called for in order to achieve the goal of security and privacy of the Internet of Things.

ENISA, the EU cyber security agency, has been working for several years on identifying security threats and risks in the Internet of Things and on providing recommendations to strengthen its security. We have already provided recommendations on securing:

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

In this, we are not alone.

We are working closely with the European Commission, Member States and many other stakeholders from the industry, public sector and academia on a host of policy areas and we support standardisation and certification actions.

We have 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.

We are developing a portfolio of demos[16] in the context of Internet of Things security with the aim to strengthen our expertise and knowhow and engage with the community, as well as to validate the recommendations stemming from the different studies.

Along with select semiconductor industry representatives, published a common position paper on cybersecurity calling for minimal security requirements for connected devices and encouraging the development of mandatory staged requirements for security and privacy in the IoT.

We are in the process of defining baseline security measures for the Internet of Things in critical information infrastructures.

Ladies and gentlemen

Everything is interconnected. And it has to be secure and safe.

The challenges ahead for the Internet of Things are many. Security is paramount, since in the context of the highly interconnected Internet of Things security is tightly linked to safety.

However, the road that we need to follow still has a number of open issues and uncertainties.

- The question of liability in the context of the Internet of Things remains challenging. We welcome the relevant recent open consultation initiatives of DG CONNECT and eagerly anticipate further developments.
- It is important to ensure 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. In the context of the Digital Single Market strategy and the European Commission's priorities, noteworthy contributions are being made in this direction.
- Holistic approaches are called for due to the diverse nature of the problem. Public Private Partnerships might pave the way for secure Internet of Things deployments.
- Raising awareness in regard to Internet of Things security is a fundamental first step forward.
- The upcoming review of the European Cyber Security Strategy is a great opportunity to underline and address relevant challenges.

Ladies and gentlemen

The benefits and opportunities that the Internet of Things brings are numerous and of paramount significance for the entire society. Together with Artificial Intelligence and Robotics it will undoubtedly lead to societal changes of great magnitude across the spectrum of human activities.

[16] ENISA at Bitkom 2016, https://www.enisa.europa.eu/news/enisa-news/enisa2019s-at-bitkom-hub-conference-feeling-secure-about-your-smart-device

It is our duty to ensure that this is done in a secure, safe and reliable manner. It is not only an enabler of a connected digital society, but a prerequisite.

The time to act for Internet of Things security is now.

Ladies and gentlemen

Final remarks: We need ethics! We need cyber ethics!

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.

The basic principles of security by design, privacy by design and ethics by design need to be addressed in the cyber world of today and tomorrow.

Consumer's rights should also be well addressed in the cyber world.

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, all stakeholders, 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 their deployment.

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 the 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.

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