# EU strategies to secure the EU cyber space and critical infrastructure against hackers

Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht - AECA Round-Table Conference-Luncheon

BRUSSELS, BELGIUM
NOVEMBER 2017

Thank you for the opportunity to address you today on **the EU strategies to secure the EU cyber space and critical infrastructures against hackers.**

This topic has been high on the agenda of the European legislators; In September 2017, the European Commission **presented the Joint Communication on resilience, deterrence and defence**: Building strong cybersecurity for the EU[1]: **The new EU cybersecurity strategy**. This Communication aims at building a strong digital single market

- through an EU cybersecurity certification framework,
- through a blueprint plan for operationalising cybersecurity response,
- through investing in strong encryption and protection of fundamental rights,
- through strengthening ENISA's role and developing international cooperation for EU leadership on cybersecurity.

The **Communication recognises ENISA's role** in the implementation of the NIS Directive and addresses a stronger role for the Agency through a proposal for a permanent mandate.

To counter existing and emerging cyber security threats, EU Member States are required to adopt cyber security strategies. **The national cybersecurity strategies** are the main documents of MS to **set strategic principles, guidelines, and objectives** and in some cases specific measures to mitigate risk associated with cyber security. Following a high-level top-down approach, NCSS set the strategic direction for subsequent actions.

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**[2] linked to criminal justice in cyber space[3].

The **scandal of hacked emails**[4] in the **US election in 2016 and the measures taken in Europe to prevent interferences in elections**[5, 6, 7] 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

---

[1] http://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PD
[2] 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
[3] 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/
[4] Hillary Clinton Email Archive on WikiLeaks, available at: https://wikileaks.org/clinton-emails/emailid/30373
[5] 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
[6] 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/
[7] 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

organisations and **democratic institutions like national parliaments**[8] **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[9], and no online services available. The reason - the Mirai botnet[10] 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.

A 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 in considerable 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[11] where almost one million landline subscribers lost service on Sunday 26 November 2016 in Germany.

During the eHealth Week 2017, organised by the Maltese presidency of the EU Council, ENISA was reaching out to hundreds of healthcare practitioners about cyber security in the healthcare sector. And then the news came through: more than 40 Hospitals in the UK shut down operations due to a cyber-attack! More specifically terminals in numerous organizations across the globe received the same ransom-message resulting into loss of data; medical data. This incident had to do with WannaCry attacks a 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[12]. Amongst these systems affected by WannaCry there were many in hospitals, where surgeries could not be performed neither other medical evaluations like X-rays.

I am sure that you will all agree with me 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.

**Everything is connected. And it needs to be secure.**

---

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

[9] 2016 cyberattack, available at: https://en.m.wikipedia.org/wiki/2016_Dyn_cyberattack

[10] 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/

[11] https://www.bloomberg.com/news/articles/2016-11-28/deutsche-telekom-probes-potential-hacking-after-router-issues

[12] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

The EU is already working towards this direction in many ways: however, now it is the **time to streamline and synchronize all efforts**. In 2013, the EU set out a Cybersecurity strategy launching numerous work streams to improve cyber resilience. The main goals of this strategy were to foster a reliable, safe and open cyber ecosystem for all, goals that still remain valid. But the continuously evolving threat landscape calls for more effective measures.

As already mentioned last September, the EU announced the Joint Communication on resilience, deterrence and defence **for building a strong cybersecurity for the EU**. The EU MS have all tools and policies required to address cybersecurity; even though cybersecurity still remains a national priority, **the scale and the cross border nature of the threats** (like WannaCry) **show that cybersecurity is a joint responsibility**. All actors - the EU, the Member States, industry and individuals – should work together to give cybersecurity the priority it needs to deliver a better EU response to cyber-attacks.

In 2016, the European Union adopted the Network and Information security directive. **It is the first piece of EU legislation specifically aimed at improving cybersecurity throughout the Union**; a very significant step towards more secure EU information systems. The Directive focuses on protection for Critical Information Infrastructures or national essential services namely through setting **baseline security measures** and implementing cyber **incident notification**. **Full implementation of the Directive by all Member States by May 2018** is imperative for ensuring resilience in the Union.

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). National cybersecurity strategies are the main documents of MS to set strategic principles, guidelines, and objectives and in some cases specific measures in order to mitigate risk associated with cyber security. Following a high-level top-down approach, national cybersecurity strategies set the strategic direction for subsequent actions like a national cybersecurity roadmap. Based on the priorities set on this roadmap the states establish agencies, public entities, action plans, academic curricula and many other activities to achieve making the state more cyber resilient.

There are commonalities in the objectives a national cybersecurity strategy should include. The most important are to develop national cyber contingency plans; to protect critical information infrastructure; to organise cyber security exercises; to establish baseline security measures; to raise user awareness; to strengthen training and educational programmes; to address cyber-crime and to engage in international cooperation. ENISA is supporting the EU MS in implementing all these objectives of the strategies.

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

**ENISA has a major role in the implementation of the NIS Directive. ENISA has a major role in supporting the MS to create their national strategy and to implement it.** In 2012, only 12 Member states had developed a NCSS. Currently, all 28 Member States have published a national cybersecurity strategy. ENISA is supporting the EU Member States and EFTA countries since 2012 to develop, implement and evaluate their National Cyber Security Strategies. With the NIS Directive in place, a lot of Member States are considering revising their strategies with the goal to create new versions that will include the provisions of the NIS Directive into their strategic objectives.

Critical information infrastructure protection is an integral part of a NCSS. The NIS Directive also names seven critical sectors like Energy, Banking, Transport and Health, which EU Member States should consider when planning and implementing cyber security measures. We **recommend aligning policy requirements with the national cybersecurity strategy** to avoid ambiguities relating to lines of responsibilities, duplication of structures and measures, and waste of resources. Some sectors are more cyber-mature than others.

A **focused approach rather than a "cover everything" approach can provide several advantages**. EU Member States can make fast progress by rolling out cyber security measures in sectors, which are already in an advantageous position. These sectors can provide a positive example, when approaching stakeholders of other critical sectors at a later stage.

One of the priorities of the national cybersecurity strategies, but also of the Directive, is **cooperation and information sharing between the public and the private sectors**; a behaviour that even though it is prioritised in all cyber security strategies still faces a number of obstacles.

The September 2017 Communication by the European Commission states: 'At European level, Sectoral Information Sharing and Analysis Centres (ISACs) **can play a key role in preparing for and responding to cyber incidents**. To ensure effective information flows on evolving threats and to facilitate the response to cyber incidents, ISACs should be encouraged to engage with all relevant bodies.'[13] How is this suggested cooperation even possible, when only several ISACs on EU level exist, or are still in development? Here ENISA's role becomes a necessity; a role that positions the agency in a central spot as a facilitator. **ENISA already positions itself as an expert or facilitator in the existing sectorial EU-level ISACs**. The existing EU-ISAC Members welcome ENISA's participation because of its status as an independent expert (not a regulator), its overview of current developments within the sector on EU level, and its network.

Policies and strategies are just preparing the ground; actual hands-on experience is sorely needed in this cyber hostile environment. The first Pan European exercise that brought 30 European countries against a common enemy that wanted to bring chaos in the Information systems in the EU, was organized in 2010 by ENISA. Since then a major exercise is organized every 2 years. A fast and effective response relies on the cyber readiness and the swift information exchange between all key players. Cyber Europe is testing standard operating procedures on cross border information exchange focusing each time on a different crisis scenario, like for example targeting the energy sector or air transport. Experience from these drills resulted into the recently announced EU Blueprint[14] that **explains how cybersecurity is addressed in existing Crisis Management mechanisms** and sets objectives and modes for cooperation between MS.

In our days, cyber capabilities need to be developed earlier on in our lives; **ENISA brings together young talents competing under the European Cybersecurity Challenge.** Fifteen competing national teams recently took part in this major competition, to showcase their technical skills and teamwork capabilities to a large participating audience, including experts, judges, observers, industry actors and media.

However, cybersecurity strategies should only depict the past, but should also pave the way for a cybersecure future: many MS have already started creating strategies on emerging technologies like Big Data, Internet of Things (IoT- Industry 4.0), Cloud Computing as they could support critical systems. **The national cybersecurity strategies should not only cover the existing landscape but also have a vision for a secure use of ICT in the borders of the country**. Moreover, cybersecurity is not only a priority for the public or the private sector; start-ups and SMEs (the backbone of the EU economy) are also affected from the national strategy. Thus it would be beneficial to include this long term vision and need for investment early on in the strategy.

As discussed, **cybersecurity is a shared responsibility** and ENISA is stepping forward and is already assuming its share of this responsibility. Accordingly, ENISA is working towards making collaboration and information

[13] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16546
[14] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:450:FIN

and knowledge sharing stronger and more reliable. The multi-faceted efforts of ENISA across the cybersecurity spectrum are supporting and empowering a more cyber secure and safe Europe.

**Everything is interconnected. And it has to be secure and safe. ENISA is present and strong to support this cause.**

**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