Introductory Speech to the Ramboll Event on the future of ENISA

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

BRUSSELS
22ND MARCH 2017

Ladies and Gentlemen,

Thank you for giving me the opportunity to address this workshop on the future contribution of ENISA to EU cyber security.

I would like to acknowledge the support of the Commission in organising this workshop and for engaging the many stakeholders and experts to contribute to the debate on the future of ENISA.

I know that the workshop will be divided into two parts, the first looking at the backward evaluation of ENISA and what has been achieved between 2013 and 2016 and the second looking at the future NIS challenges and EU Priorities.

The mandate of the European Union Agency for Network and Information Security (ENISA) expires on 18th of June 2020. The renewal of the mandate will require the bringing forward of a proposal by COM and the agreement of the Council and the Parliament. Here today, you are part of this process in providing input for the drafting of the proposal by the Commission.

In the pursuit of an open, safe and secure cyber space, ENISA supports the EU and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents. ENISA also supports the development and implementation of European Union policy and law on matters relating to network and information security (NIS).

ENISA is the European cyber security agency, which determines and addresses network and information security issues, thereby contributing to the proper functioning of the internal market. It also aims to exploit the full potential of the internal market from the widespread use of information and communications technologies (ICT) in a safe and secure cyber space.

While ICT technologies present business opportunities in cyber space they also present opportunities for crime and misuse, which need to be considered and addressed.

Cyberspace can be considered in terms of cyber attack, cyber sabotage, cyber espionage, cyber terrorism and cyber warfare. International conflicts move from the real world into the virtual cyber world.

Estonia 2007, Georgia 2008, Iran (Stuxnet) 2010, the Snowden revelations of 2013, the scandal of hacked emails in the US election in 2016 are only a few examples of the new virtual Wild West in cyber space.

In some countries more economic loss is now being attributed to cyber crime than to traditional crime.

Other recent types of cyber attacks in Europe include:

1. the compromising of routers in a number of countries where VoIP emergency 112 calls were affected leaving citizens without access to the emergency services,
2. the hacking of hospital IT systems with ransomware, the effect of which the hospital operations had to be shut down and a ransom paid to the criminals,
3. the hacking of autonomous driven cars putting citizens at risk,
4. the hacking of the door locks of hotels leaving the owners and customers of the hotel without access to their rooms,
5. the detection of malware in nuclear plants in Europe.

The main difference between the good guys and the bad guys is that the good guys have to be successful every time while the bad guys only have to be successful once. It is only a matter of time before the criminals will score a catastrophic cyber attack in Europe.

Cyber security is one of those subjects that never stays still. Every month new issues arise to challenge the digital ecosystem which continues to grow. Despite these challenges, the Member States continue to encourage and invest in the use of the internet. The EU Digital strategy is based on a single digital market that will generate the wealth and jobs of the future. Reflecting the pace of change, I also understand that the existing cyber security strategy adopted in February 2013 which is four years old is now the subject of review.

According to Eurostat the percentage of the EU population using the internet now exceeds 80%. However, when the figures are analysed on a member state level, the percentage of the population using the internet varies from 57% to in excess of 96%.

It is reasonable to assume that this variance also applies to the investment and preparedness of different Member States in the area of cyber security. Some countries declare publicly investment levels of Billions of Euros in national cyber security while other countries are more silent on their levels of investment in cyber security.

One of the reasons for the creation of ENISA in 2004 was the different levels of cyber security preparedness across the EU member states. ENISA is in a position to support all Member States across Europe and has been and is well positioned to narrow the cyber preparedness gap.

Europe continues to be increasingly integrated at a political, economic and infrastructure level. Cyber security knows no borders and infrastructure outages in one country can easily impact other countries.

ENISA also needs to be in a position to address the geopolitical aspects of cyber security which supports the EU foreign security and defence policy.

In my opinion, to face the technological, economic and geopolitical challenges in the EU, three essential things need to be addressed:

1. The EU Commission, together with the MSs need to continually examine and adjust where necessary the current **European governance structure** regarding roles and responsibilities in ICT and cyber security, and
2. A **permanent mandate** with a significantly **strengthened role for ENISA** to allow for better long term strategic vision, and
3. A **significant increase in its budget** with **the allocation of additional high level expert positions.**

The current evaluation of ENISA and the envisaged new ENISA mandate proposal of the Commission is a unique opportunity to address the challenges mentioned above.

As you are aware, ENISA has produced a draft position paper on the future of ENISA[1]. I hope you have found this paper engaging and a good basis for the discussions we will have today.

The main findings of this paper are as follows:

[1] ENISA, Cyber Security Beyond 2020 – ENISA's Input to the mandate renewal discussion, 20th February 2017: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cyber-security-beyond-2020

1. ENISA's current tasks and product **portfolio** shall be **retained.**
2. ENISA be granted a **permanent mandate.**
3. A number of existing tasks and service offerings by ENISA needs to be reinforced and several new tasks and orientations should be considered to address the c**omplete cyber security life cycle in other words the detection, mitigation and response to cyber attacks.** ENISA shall have the power to act on its **own initiative** and to engage in the complete security life cycle.
4. The future mandate should be scoped more broadly to allow for a coherent approach to EU cyber security and give greater consideration to the **economic and societal aspects** of cyber security where ENISA could also play a role.
5. In scoping ENISA's role and tasks, it would be important to define clearly the scope of different other actors in the EU cyber security space.
6. A **new governance structure** along the lines being considered by other agencies could be suggested to improve the decision-making process.

Issues and themes that were identified by ENISA for the future include:

1. **Organic growth:** continuing the evolution of the functions of the Agency to address the latest cyber security challenges,
2. **Policy advice:** provision of strategic policy advice to the EU institutions and MS in relation to cyber security; ENISA should also be in a position to produce its own initiative policy advice,
3. **Information** and **capability-building:** ENISA as the EU Cyber security Information Hub offering high quality cyber security analysis and training,
4. **Economics of cyber security:** including better engagement with industry to leverage economic opportunities in the EU from cyber security,
5. **Standards and certification:** ENISA developing and promoting cyber security standardisation and certification.

As a **closing remark**, ENISA has contributed to the EU cyber security landscape since 2004. Despite the importance of this topic, ENISA's mandate has had to be renewed in 2009 and 2013. ENISA's budget has remained relatively static in the last few years at around €11M per year. Given this relatively modest resource, ENISA has produced reports on a wide variety of cyber security issues including the annual Threat Landscape report, Smart Transport and Cities, Cloud Services, Encryption, Blockchain to name a few as well as designing and delivering the most comprehensive cyber exercises in Europe.

ENISA is addressing and hopefully will continue to address the cyber security challenges while supporting the political goal of harnessing the opportunities of the Digital Society. ENISA's role needs to be further developed and strengthened to adequately contribute to the EU cyber security world post 2020.

It is against this background, I present and hope that you **share my vision for a stronger European cyber security Agency** that will meet the cyber security challenges of the future.

Thank you for your attention and I look forward to a constructive debate over the next few hours.

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