ENISA today and in the future

Udo Helmbrecht
Executive Director
ENISA

COMMITTEE ON INDUSTRY, RESEARCH AND ENERGY
MINI-HEARING on ENISA

European Parliament,
Brussels, 26 May 2011

For Publication

Dear Mr Chairman,
Dear Members of the Parliament,
Ladies and Gentlemen,

Thank you for the invitation to speak here today. I am very pleased that you have given me the opportunity to talk to you about ENISA's work and how it might evolve in the future to meet the needs of Europe.

Network and Information Security Today

ICT dependencies

Information and communication technologies (ICTs) are the backbone of today's global information society: for governments, for businesses and for citizens. Since 1995 the Internet has become a vital medium of our economy and our social life: online-shopping, social networks, mobile communication, cloud computing are all examples of technologies that have come to play an important part in our daily lives.

Vice-President Commissioner Kroes has put forward the Digital Agenda for 2020, with the objective of improving the quality of life through, for example, better health care, safer and more efficient transport solutions, a cleaner environment, new media opportunities and easier access to public services and cultural content[1].

Threats & opportunities

Unfortunately, the significant benefits that ICTs afford us are accompanied by a number of new threats. These threats are not only due to vulnerabilities associated with new technological developments – they are also due to the fact that these technologies are being used to attack systems. ICT is increasingly used in cybercrime and politically motivated attacks. This fact was recently referred to by the German Minister of the Interior, who noted that during 2010 there had been an increase of 8.1% in criminal acts associated with the Internet[2].

The evolving threat landscape

ICTs are vulnerable to threats which no longer follow national boundaries and which have evolved with technology and market developments. As ICTs are global, interconnected and interdependent with other infrastructures, their security and resilience cannot be secured by purely national and uncoordinated approaches. There is a need for a comprehensive framework at the EU level that will enable us to

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF
[2] http://www.dw-world.de/dw/article/0,,15093336,00.html

stay ahead of the threats, or at least be up to speed, throughout Europe. Network and Information Security (NIS) is vitally important to modern communications, economic growth and development, and to social cohesion.

NIS threats are evolving in many different areas:

- man-made attacks such as cybercrime, cyber-espionage, or attacks on critical infrastructure,
- natural disasters and
- technical failures.

I will briefly mention three examples of fairly recent attacks, each of which highlights different aspects of the types of threats we are facing and their consequences. They all illustrate the seriousness and global dimension of network and information security issues.

- Stuxnet[3]: a virus which targets industrial software at, for example, nuclear facilities. It was specially created for the SCADA[4] systems that these facilities use. Doing this requires special knowledge of the control systems as well as a great deal of resources to develop. So we have highly capable and resourceful attackers that go after critical infrastructure. The major concern about Stuxnet however is not the technical mechanisms that the software implements, but the fact that the target has changed – the ability to interrupt or modify the operations of industrial control systems could result in the loss of life.
- Another recent and well publicised attack is the theft of close to 30 million euro-worth of emissions allowances from the national registries in the EU Emission Trading Scheme.[5] This was a cross-border attack with serious financial impact.
- Last month, Sony's online gaming platform, the PlayStation Network, was attacked and information about more than 100 million users was stolen[6]. It is still not known how much the attack will cost Sony, but it is likely to be considerable and one estimate is as high as $2 billion[7]. This shows how an attack on one company can seriously affect and undermine the trust of users across the globe. More generally, it illustrates how attacks can affect entire businesses.

[3] http://en.wikipedia.org/wiki/Stuxnet

[4] http://en.wikipedia.org/wiki/SCADA

[5] http://en.wikipedia.org/wiki/European_Union_Emission_Trading_Scheme

[6] http://www.ft.com/cms/s/2/e13be04a-80af-11e0-85a4-00144feabdc0.html#axzz1MiIfi8HH

[7] http://www.reuters.com/article/2011/05/05/us-sony-insurance-idUSTRE74472120110505

Of course it is not only threats that are evolving. The countermeasures to tackle them have also changed. These developments include improvements to networking best practices, more focused policies, regulations and directives, increased insight into multi-sector implications of security issues and the recognition of the importance of having a global perspective on NIS.

Organised crime

In the recently released organised crime threat assessment from Europol, it is noted that the Internet is "a facilitator for organised crime". They note that "A new criminal landscape is emerging marked increasingly by highly mobile and flexible groups, operating in multiple jurisdictions and criminal sectors, and aided, in particular by widespread, illicit use of the Internet."[8]

Improving the capability for dealing with cyber-attacks is part of the objectives of the EU Internal Security Strategy, which states that, "Europe is a key target for cybercrime because of its advanced Internet infrastructure, the high number of users, and its Internet-mediated economies and payment systems."[9]

ENISA acknowledges the importance of the fight against cybercrime as well as the need for a strong collaboration between Computer Emergency Response Teams (CERTs) and law enforcement because we need the CERTs in the fight against cybercrime. The important role of ENISA is to provide an interface between Law Enforcement and the cyber security community.

Building the community

It is precisely because the technologies, networks and information systems which we have come to rely so heavily upon in our everyday lives can be used against us, that we need to continue to improve and strengthen our prevention, detection and response capabilities.

As I have already demonstrated, we are increasingly aware of how sensitive and how vulnerable to attack our infrastructures are. Unfortunately, we lack adequate information by which to be able to recognise and react to dangers in due time. Here, I see a real opportunity for Member States to use ENISA more effectively, by asking the Agency to collect and analyse data relating to information security in a

[8] http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA_2011.pdf

[9] http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf

cross-border context. Such an approach is likely to reveal trends that are not visible at present.

Our tasks are made all the more difficult if barriers are set up to which our adversaries are not subject. It is important that on a European level we have a holistic approach to NIS – and that we pursue opportunities for international collaboration and dialogue. One of the biggest obstacles we face here is the fact that communication between different communities within Europe is far from being optimal. As an example of this, it is important to note that the public and private sectors are working actively in the area of Critical Information Infrastructure Protection (CIIP), but lessons learnt are not being shared. By ensuring that these efforts are aligned, we can greatly increase the effectiveness of the overall approach.

This brings me on to the Lisbon Treaty, which gives us the opportunity to take a more holistic approach towards NIS. The treaty is a second opportunity for ENISA, which is ideally placed to support the Member States and the EU institutions in improving the level of dialogue between these communities in the area of NIS. The Agency could sensibly be considered as an interface between different operational communities in general. The objective would be to ensure that the overall approach to improving information security throughout Europe is both coherent and efficient, by identifying synergies and eliminating duplication of work.

Ensuring a coherent pan-European approach

Any future approach to securing Europe's ICT systems must be coherent across geographical borders and communities and consistent in time. This is clearly not the case at the present time, where different approaches to securing information and systems are developed independently in different Member States and in different communities.

Even at a more technical level, there is evidence that the approaches we have defined to date need to be improved. As an example, it is clear that it makes little sense to separate the protection of infrastructure from the applications which run on top of it. Those who choose to attack systems do not make the distinction between the two – they simply exploit the weakest link. For example, with botnets[10] home users' computers can be infected with malicious software, such as a Trojan horse[11]. The computers can then be remotely controlled to attack governmental websites

[10] http://en.wikipedia.org/wiki/Botnet

[11] http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29

and online services. An example of this was seen in the 2007 cyber-attacks against Estonia[12].

ENISA has developed a network of contacts across Europe that includes all Member States and that spans many different communities. ENISA will continue to strive for an approach to securing our systems and information that is coherent across all of these dimensions, and that is aligned with what is happening in other international communities.

Building on progress

In summary, whilst it is clear that threats will not cease to develop, each new development brings with it corresponding opportunities for improvement.

As the recent communication on CIIP[13] shows, we have, on a pan-European level, already made several important first steps to improve our approach to cyber security and our ability to respond effectively to other forms of disruptive events. ENISA is playing a key role in facilitating much of this activity, and we expect to improve the impact of our activities even further with the strengthened role associated with the new mandate.

ENISA's current Work Programme

Our Work Programme[14] is currently divided into three Work Streams:

- ENISA as a facilitator for improving cooperation
- ENISA as a competence centre for securing current and future technologies
- ENISA as a promoter of privacy and trust

Together they contain thirteen work packages. It would be too ambitious to try to cover all of these in this speech. I will therefore give you a summary of some of the more important elements of the Work Programme.

[12] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[13] http://eur-lex.europa.eu/Notice.do?checktexts=checkbox&val=493232:cs&pos=1&page=1&lang=en&pgs=10&nbl=1&list=493232:cs,&hwords=&action=GO&visu=#texte

[14] http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/enisa-work-programmes-general-reports

ENISA as a facilitator for improving cooperation

Work Stream 1 is essentially dealing with two distinct areas: CIIP and the strengthening of CERTs in Europe. I will return to these activities later.

ENISA is also supporting the establishment of an EU institutional CERT and has Agency representatives both within the 'pre-configuration team'[15] and the Steering Committee.

ENISA as a competence centre for securing current and future technologies

In Work Stream 2, we are working with the public and private sectors to correctly secure new technologies and business models such as those arising from the adoption of cloud computing. In this, we are collaborating closely with other areas of the European Commission, notably DG INFSO Directorate F, where we will be involved in an advisory role in the next call for research projects under Framework Programme 7 (FP7).

ENISA as a promoter of privacy and trust

In Work Stream 3, ENISA is working with a number of other EU institutions and bodies (the Commission, the European Data Protection Supervisor and the Article 29 Working Group) in order to ensure that EU privacy laws can be implemented in a realistic and meaningful way on modern IT systems.

The work that ENISA is performing in Work Stream 1 is directly supporting the CIIP Action Plan, as laid down in the Commission Communication of March 2009 - “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”[16]. It is therefore worthwhile to explain this work in a little more detail.

CERTs in Europe

Since 2005, ENISA has run a programme dedicated to reinforcing national and governmental CERTs. The goals of this programme are to support the EU Member States in establishing and developing their national and governmental CERTs according to an agreed baseline set of capabilities, and to generally support and

[15] The team is tasked with establishing the operational CERT for EU institutions within approximately one year.

[16] http://eur-lex.europa.eu/Notice.do?checktexts=checkbox&val=493232:cs&pos=1&page=1&lang=en&pgs=10&nbl=1&list=493232:cs,&hwords=&action=GO&visu=

reinforce CERT cooperation by making available good practice. There are 21 Member States that have already established official national/governmental CERTs. But there are others which either do not have such a team, or have one that is not yet fully operational. Besides this, there are national/governmental CERTs which participate in well-functioning networks. For example, some national/governmental CERTs participate in the European Government CERTs Group (EGC), partly on a voluntary basis with informal CERT communities. Finally, there are Member States which have national/governmental CERTs that are either not integrated in informal structures (TF-CSIRT[17] and FIRST[18]) or are unknown to CERTs in other Member States.

ENISA seeks to reinforce this type of cooperation by analysing barriers for cross-border cooperation and proposing measures to tackle them. An example of how this is being achieved in practice is the development and further deployment of the activities around information sharing and the alerting of citizens in the Member States, such as the European Information Sharing and Alert System (EISAS).

The ultimate goal of these activities is to help CERTs to improve the effectiveness and the efficiency of their response mechanisms, particularly where cross-border incidents are concerned.

A recent development here is the work that ENISA is doing to facilitate dialogue between CERTs and other communities in cyber security.

The EU institutional CERT

The Digital Agenda for Europe is a flagship initiative under the EU 2020 Strategy. Key Action 6 of the Agenda is to: “Present in 2010 measures aimed at a reinforced and high level Network and Information Security Policy.” One of the measures identified is the implementation of a CERT for the EU institutions.

In August 2010, European Commission Vice-Presidents Neelie Kroes and Maroš Šefčovič established a “Rat der IT Weisen”. This was asked to provide the Commission and the EU institutions with advice regarding the establishment of a CERT for EU institutions. A CERT for the EU institutions will deliver strong value as it would inter alia increase protection against attacks and facilitate swifter reaction to threats, ensure efficiency through shared resources, protect EU competitiveness and be consistent with EU policy.

[17] Task Force – Computer Security Incident Response Teams http://www.terena.org/activities/tf-csirt/
[18] Forum of Incident Response and Security Teams http://www.first.org/

ENISA, in its position as an independent, experienced and – above all other things – trusted body in Europe is uniquely positioned to play the key role in the coordination of the incident response capabilities of the EU institutions. Experts from ENISA are established members of FIRST and TF-CSIRT, and maintain vital relationships with all other CERT communities around the globe. Furthermore, ENISA's experts have extensive experience in assisting CERTs in the provision and coordination of NIS incident response.

The Rat der IT Weisen's final report resulted in an action to take the first steps towards a CERT for EU institutions, by setting up a pre-configuration team. This will start operations on June 1st of this year. ENISA is actively supporting the establishment of the EU institutional CERT.

Cyber EU-Exercise

In 2010, ENISA facilitated the first pan-European cyber security exercise. This took place on 4th November 2010 and involved the participation of all 27 Member States and 3 EFTA countries (Switzerland, Norway and Iceland). Of these participants, 22 acted as players and eight as observers. One of the most important conclusions of this exercise was that procedures to handle cyber incidents do not yet exist on a pan-European level and that there is a need to improve response collaboration across Europe[19]. Following on from this work, ENISA has recently been asked to facilitate the planning of the first EU-US cyber security exercise, which will happen before the end of the year. This exercise represents an important development in international cooperation and we are happy that the Agency's expertise is being called upon to support this effort. Despite the fact that such a project is a great challenge for the Agency, we are confident that we can work together with the Member States in order to meet the deadline.

ENISA's role

As the technology and threat landscape has evolved, we have fortunately also improved our network and information security capabilities. In some ways we can more easily define the issues and what is at stake. However, we do not know what tomorrow brings. It is a constant race to keep up with new technologies and business models and the opportunities they create.

[19] http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report/view?searchterm=cyber+europe+report

ENISA’s role is to support the Commission and the Member States in advancing network and information security. I see it as one of our main tasks to perceive and understand the needs of the Member States and the strategic interests of the EU. On this basis we will promote extensive cooperation and facilitate efficient and effective collaboration to advance cyber security in Europe.

In summary, ENISA is in a unique position to be a focal point for NIS in the EU.

The Agency can achieve this in a number of different ways. By acting as a **neutral** European platform for **information sharing** - and for establishing and maintaining networks and communities - we promote dialogue and help Member States to align their approaches to specific issues. This role is also important in a more general context, where ENISA facilitates dialogue between European actors and their international counterparts.

The Agency also provides expertise and advice to a variety of stakeholders, particularly in the area of development and implementation of standards and best practices. As such, the Agency plays an important role in bridging the gap between policy and operational requirements. Finally, we are active in the area of risk assessment and management, particularly where emerging threats are concerned.

The future of ENISA

It is increasingly clear that information security is a global issue, requiring a global solution. Not only are approaches to security that are confined within national boundaries liable to failure, any European approach that does not take account of the international dimension will also not work. By acting as a focal point for Network and Information Security within Europe, ENISA assists Member States in aligning their approaches and, in close collaboration with the European Commission, in ensuring consistency with international developments.

At present, ENISA is the only public institution with a pan-European focus that is mandated to work closely with operational communities in order to respond effectively to the threats I have outlined above. Past experience teaches us that working closely with operational communities is critical to introducing significant improvements in this area and we have an opportunity to take this model one step further with the new mandate.

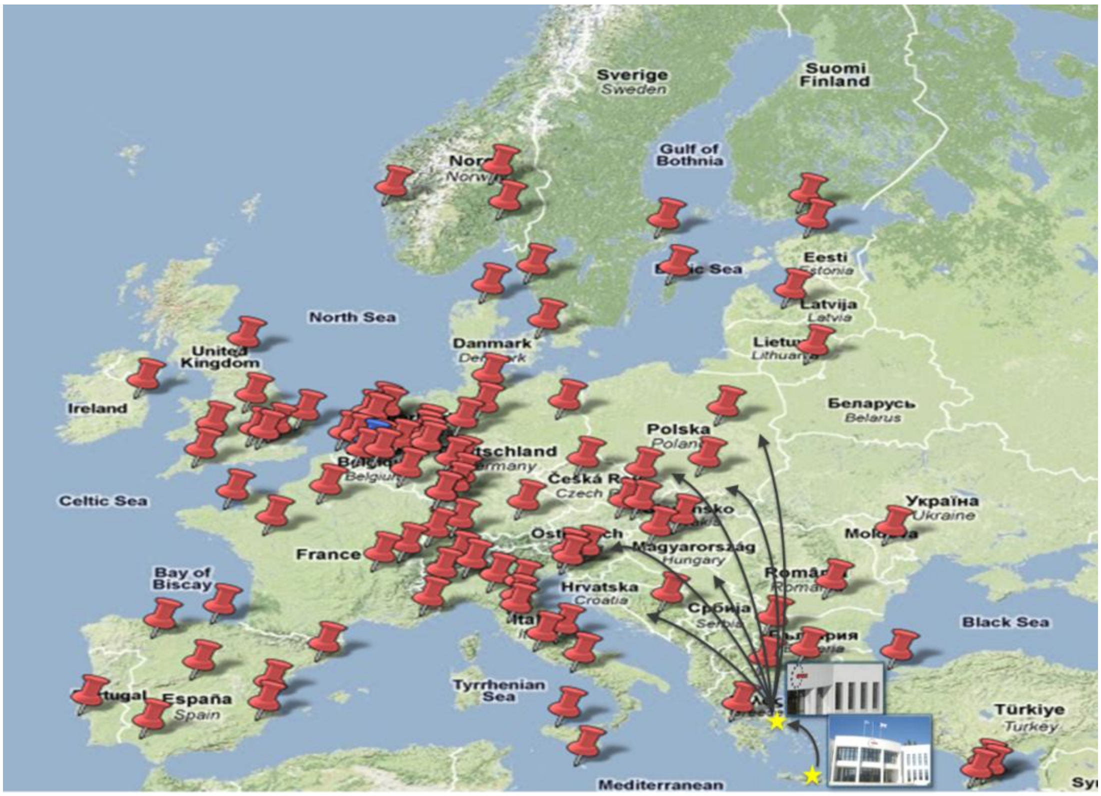
Commission’s proposal and our comments

In September 2009 Vice-President Neelie Kroes announced the Commission’s proposal for the extension of ENISA’s mandate.

We very much appreciate the additional tasks, especially the fact that the proposal already takes steps towards overcoming the Pillar structure by including a reference to how ENISA can support other institutions in the fight against cybercrime.

The Commission's proposal for the ENISA budget was not done for post-2014 and will be presented by the Commission in the context of its proposal on the MAFF (Multiple Annual Financial Framework). As you have seen from the introduction on IT dependencies and threats, the budget of ENISA has to be aligned with the mandate's tasks lists. Therefore I am calling for your support in achieving this.

ENISA also needs more flexibility to face the current and future challenges in ICT. The modernised mandate of ENISA must have the necessary adaptability to respond to the challenges of the continuously evolving NIS environment.



Above: The yellow stars show ENISA's seat in Heraklion on Crete and the Agency's branch office in Athens. The pins indicate ENISA's mission destinations across Europe.

The Agency must be enabled to fulfil the expectations and needs of our stakeholders, both today and in the future. It should be strengthened in its capacity and scope, as a centre for information sharing and exchange of best practices to achieve a pan-European approach to cross-border issues. In these ways, ENISA can assist in achieving a more coordinated and thereby more effective approach to cyber threats, as well as better cooperation on response to cyber-attacks in order to increase the overall level of cyber security to protect the European information society.

In a nutshell, ENISA is all about achieving stakeholder engagement. Our operating model is to maximise contact with stakeholders at all levels and to be present where the issues need to be resolved. We know that this approach is supported by our stakeholder community, but we also recognise that being continually present throughout Europe is a significant operational challenge. In this respect, we would ask the Parliament to support the efforts of the Agency to improve the flexibility of its working environment and to create an operating model that allows the Agency to attract qualified staff as employees and to attract all relevant stakeholders.

Conclusion

ICT developments bring with them considerable benefits for modern society – they are a key economic driver and contribute to the competitiveness of the European economy. Such developments however are accompanied by associated risks, and controlling such risks is essential if we are to realise the true benefits.

As the European Agency for Network and Information Security, ENISA already plays an important role in supporting the EU institutions and the Member States in securing the ICT infrastructure of the future. In particular, by acting as a neutral European platform for information sharing and for establishing and maintaining networks and communities, we promote dialogue and help Member States to align their approaches to specific issues. We also provide advice to stakeholders, bridging the gap between policy and operational requirements.

I have mentioned a number of areas where the tasks assigned to the Agency could sensibly be extended. Firstly, by asking the Agency to collect and analyse data relating to information security in a cross-border context, there is an opportunity to discover trends that are not visible at present. Secondly, I have noted that the coming into force of the Lisbon Treaty is a second opportunity for ENISA, which is ideally placed to support the Member States and the EU institutions in improving the level of dialogue between communities in the area of information security; and the Agency could sensibly be considered as an interface between different operational communities in general. I have also made extensive reference to the work that ENISA is doing in the area of resilience and CIIP, which is bringing valuable results to the community.

I have also mentioned the need to optimise the working environment of the Agency. Given that our operating model is to maximise contact with stakeholders at all levels and to be present where the issues need to be resolved, we would ask the Parliament to support the efforts of the Agency to improve full mobility and the flexibility of its working environment, and to ensure that we can place our resources where they are most efficiently mobilised throughout the EU – with the Member States.

Thank you.