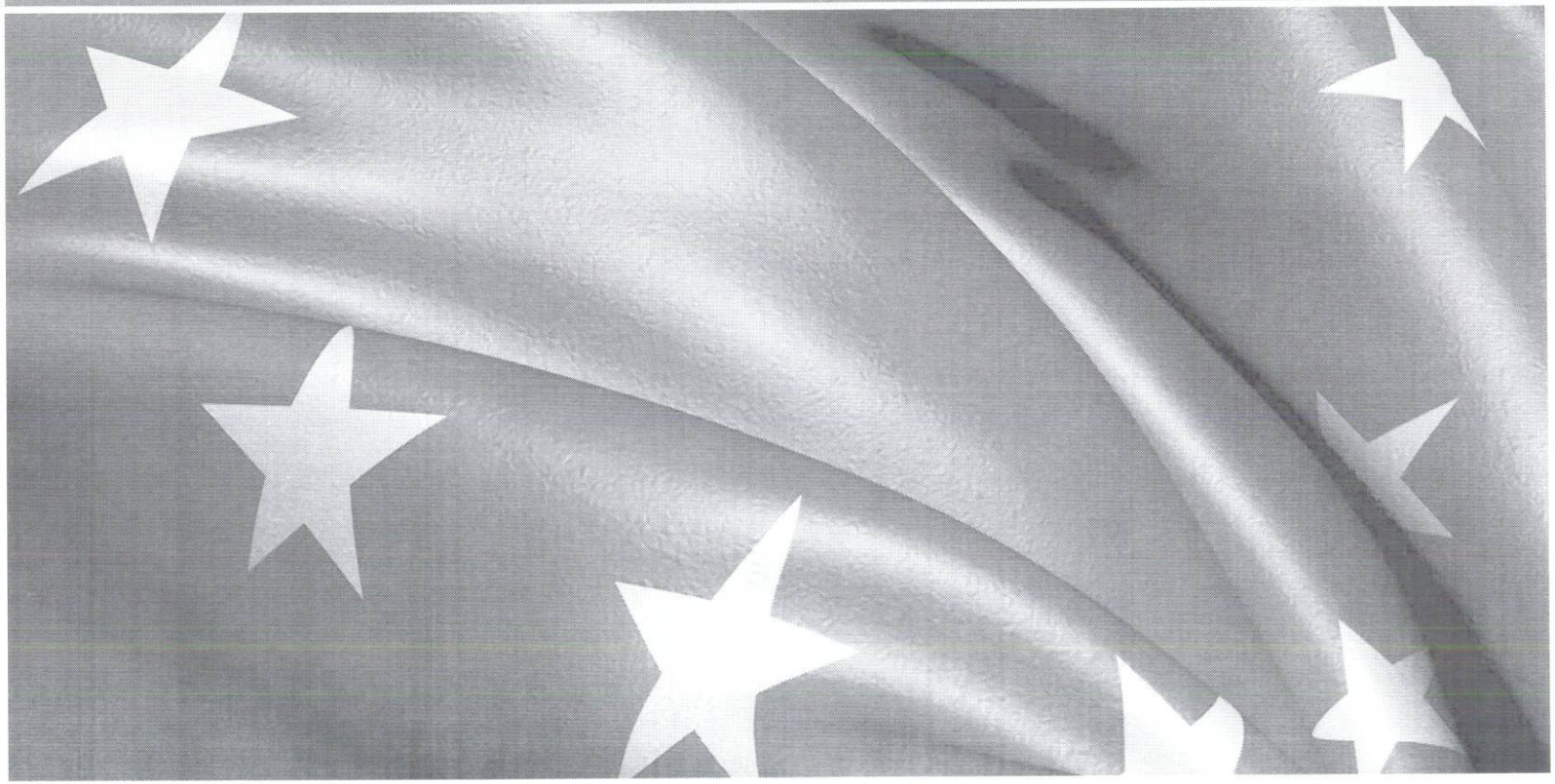
Cyber security: future challenges and opportunities

enisa
European Network and Information Security Agency



Cyber security: future challenges and opportunities

Authors:
Prof. Udo Helmbrecht
Dr. Steve Purser
Maj Ritter Klejnstrup

Contact details
For contacting ENISA or for general enquiries about this publication, please use the following details:
E-mail: info@enisa.europa.eu
Internet: http://www.enisa.europa.eu

Contents

Executive Summary

Our society has become irreversibly dependent on Information and Communication Technologies (ICTs). Unfortunately, whilst these technologies have brought many benefits, the increased adoption of them has also been accompanied by the development of a new set of cyber threats which are developing in ever more rapid, sophisticated and sinister ways.

This means that the protection of critical infrastructure, and the applications that run on top of it, is not just about technology and security, it is closely connected to the European Union's competitiveness and prosperity.

Any future approach to securing Europe's ICT systems must be coherent across geographical borders and pursued with consistency over time. This is 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. However, without a coordinated global approach to major incidents on the internet, Member States could find themselves in a situation where local systems cannot function correctly due to issues that are outside their control.

ENISA believes international coordination is essential to achieve a holistic approach to network and information security. This includes cooperation throughout Europe as well as worldwide in both the public and private sectors. In many ways, it is this global dimension that distinguishes cyber security from what we have referred to in the past as information security.

The EU institutions and bodies should provide the support and the framework for Member States to achieve a coordinated global approach.

One of ENISA's tasks is to bridge the gap between policy and operational requirements, it does so by being an impartial European platform for information sharing amongst EU Member States, and also globally.

The main contributions of ENISA to enhancing cyber security are in the following areas:

- *Identification and analysis of emerging trends and threats*
- *Awareness of network and information security risks and challenges*
- *Early warning and response*
- *Critical information infrastructure protection*
- *Adequate and consistent policy implementation*
- *Actions against cybercrime*
- *International cooperation*
- *Information exchange*
- *Building communities*

There are a number of areas where the current approach to improving cyber security in the EU could sensibly be extended. For example, there is a clear need to collect and analyse data relating to information security in a cross-border context which could reveal trends that are not visible at present. Also, the coming into force of the Lisbon Treaty is an opportunity to improve the level of dialogue between communities in the area of network and information security. A proactive approach to building these new cross-border communities will bring great benefits both in terms of the effectiveness of its approach and efficiency in use of its resources.

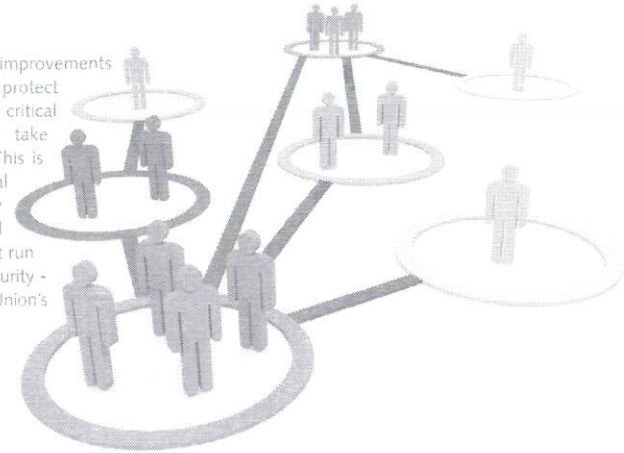
It is important that our efforts to protect and facilitate the development and prosperity of the European Information Society do not lose momentum. These efforts are addressed on many fronts with multiple stakeholders – all are increasing in numbers and scope along with the pervasiveness and economic importance of ICTs. It is important that ENISA is modernised and further developed to allow the Agency to respond to these changes and provide support and expertise for stakeholders across Europe.

Introduction

Information and Communication Technologies (ICTs) have become the backbone of our economy and society. In today's world, geographically separated societies are interconnected by information technology – and are irreversibly dependent on it. Unfortunately, whilst it has brought many benefits, the increased adoption of information technology has also been accompanied by the development of a new set of threats. These threats reflect the global nature of the systems they target and their mitigation often requires international collaboration. In many ways, it is this global dimension that distinguishes cyber security from what we have referred to in the past as information security. The propagation and implications of threats such as malware (and botnets in particular) mean they are no longer just an issue for people to deal with individually, but are increasingly a social and civic responsibility.

European Commission Vice President Neelie Kroes has put forward the Digital Agenda for Europe, 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] This is a major step towards the creation of the Digital Society. However, cyber-attacks complicate the deployment of ICT solutions used by citizens in their day-to-day lives, such as online payment and e-government services. ICT is increasingly used in crime and politically motivated attacks. For example Germany saw an increase of 8.1% in criminal acts associated with the internet during 2010, as noted by the German Minister of the Interior.[2]

To fully achieve the potential for improvements through ICTs, it is necessary to better protect citizens, businesses, governments and critical infrastructure from criminals who take advantage of modern technologies. This is also recognised in both the Digital Agenda and the Internal Security Strategy.[3] The protection of critical infrastructure, and the applications that run on top of it,[4] is not just about cyber security - it is closely connected to the European Union's competitiveness and prosperity.



1 COM(2010) 245 final/2
2 http://www.dw-world.de/dw/article/0,,15093336,00.html
3 COM(2010) 673 final
4 An insecure application running on secure infrastructure is still insecure. A secure application running on insecure infrastructure can still be secure as long as we can ensure availability and performance.

The Evolving Threat Landscape

The development of information technology in the past 40 years has been rapid. However, it is not only ICT that has developed and become increasingly pervasive, so have the threats against it.

This is a major challenge for all of those involved in securing the European information society and protecting European citizens and their fundamental rights. Not only are new technologies and business models continuously being introduced, the use of old technologies is being extended in ways that were never envisaged when they were first developed. A good example of this is SCADA[5] industrial control systems, which were initially designed to be independent without connectivity to other systems, but are now increasingly being connected to the internet. SCADA systems were targeted in the Stuxnet[6] attack which is described below.

At the same time, new business models seriously push existing concepts and regulation to their limits. Cloud computing and other technologies where data is decentralised and spread out over virtual and physical locations is a prime example. Our concepts of data, data protection and data sharing are often difficult to apply in these settings, which is problematic given the rate of uptake of these new technologies. An illustrative example of this is the difficulty experienced by a Danish municipality in rolling out Google Apps[7] to teachers. The Danish Data Protection Agency challenged the municipality's initial assessment that confidential and sensitive data about students and parents can be processed in Google Apps. Among other issues, the Data Protection Agency had concerns about the physical location of data as well as the municipality's ability to maintain control with the cloud solution provider (Google).[8] In this case there is a potential conflict between the benefits of the new business model, such as economies of scale and standardized services, and the possible negative impact on citizens' rights to privacy and data protection. ENISA is currently looking at the use of such new technologies. The Agency has highlighted some of the possible risks and provided guidance on how these risks could be mitigated. As part of their recommendations to the municipality, the Danish Data Protection Agency recommends the use of ENISA's cloud security risk assessment.[9]

As well as issues created by the fast pace of development, we are faced with deliberate attempts to cause harm. These include increasingly complex attacks, which may benefit from the backing of rogue states and organised crime, such as for example the Stuxnet attack. This, and four other recent attacks, are described below. Each of them 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 (NIS) issues.

- *Stuxnet: malware which targets industrial software at, for example, nuclear facilities. It was specially created to attack the SCADA systems that these facilities use. Developing Stuxnet required special knowledge of the control systems as well as substantial resources to develop. Thus 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.*

5 http://en.wikipedia.org/wiki/SCADA
6 http://en.wikipedia.org/wiki/Stuxnet
7 http://en.wikipedia.org/wiki/Google_Apps
8 http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/
9 http://www.enisa.europa.eu/act/application-security/rm/files/deliverables/cloud-computing-risk-assessment

- *Since 2008 the EU Emission Trading Scheme has been the subject of several attacks. At the beginning of January 2011 close to 30 million euro-worth of emissions allowances were stolen from the national registries.[10] This was a cross-border attack with serious financial impact.*

- *In March 2011, the security firm RSA[11] issued a statement that there had been an attack against their infrastructure which they categorised as an Advanced Persistent Threat (APT). This means that for some time they had been under a sophisticated attack which seems to have had the purpose of extracting specific information on their SecurID two-factor authentication products, probably as preparation for future attacks.*

- *In April 2011, Sony's online gaming platform, the PlayStation Network, was taken offline after it was attacked and information about more than 100 million users was stolen.[12] 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.[13] 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.*

- *Diginotar, an SSL certificate authority, recently suffered a cyber-attack which has led to its subsequent bankruptcy. Fox IT reports that the first traces of the cyber-attack date from the 17th of June 2011. The attacker was able to create fraudulent SSL certificates for hundreds of sites, including Google and Skype. Fake SSL certificates can be used to intercept encrypted web browsing, machine-to-machine communications (web services) and to fake electronic signatures. DNSSEC also relies on SSL certificates to validate the link between IP addresses and domain names.*

(footnote: http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html)

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. It is important to maintain and adapt these efforts to improve NIS to keep pace with the continuous evolution and increasing pervasiveness of ICTs.

10 http://en.wikipedia.org/wiki/European_Union_Emission_Trading_Scheme
11 http://www.rsa.com/node.aspx?id=3872
12 http://www.ft.com/cms/s/2/e14be04a-80af-11e0-86a4-00144feabdc0.html#axzz1MiffI8HH
13 http://www.reuters.com/article/2011/05/05/us-sony-insurance-idUSTRE74472120110505

Mitigating the Threats - A Fragmented Approach

Despite the above mentioned improvements, it is essential to achieve a holistic approach to cyber security, including cybercrime, on a pan-European level. Much of the current debate (and flow of information) on cyber security is taking place within specialised communities. Military communities are discussing subjects such as cyber war and cyber-defence; law and enforcement communities are analysing threats and solutions related to cybercrime; and intelligence communities are concerned with cyber espionage. In the information society, we are concerned with the way in which new threats affect infrastructure, applications and data related to internal market activities, both within the public and private sectors.

This document adopts the following classification of areas that are typically considered to fall into the general category of cyber security:

Cybercrime: Criminality is on a new scale on the internet. In conventional crime the perpetrator has to be at the scene of the crime. In a bank robbery he has to enter the bank. On the internet the time and place of the crime are not dependent on each other. If I am phishing, I can take money illegally from a person's bank account at any place in the world and at any time. This also means that I may find myself in different legal systems. It may be impossible for the prosecution authorities in country A to arrest a criminal in country B.

Cybercrime often also allows organised crime to scale up its illegal operations.

Cyber espionage: Espionage has been around for a long time and will continue to be present as long as there are national state interests and intelligence services.

However, whereas in the past the spy had to run the risk of having his cover blown at the crime scene, today he can spy unseen from afar using technology (for example Trojan horses[14]).

Cyber security: This refers to the protection of information, information systems, infrastructure and the applications that run on top of it from those threats that are associated with a globally connected environment.

Cyber warfare: In the past, troops from opposing countries confronted each other on a battlefield, and "rules" for warfare were written if not always followed. The Geneva Convention,[15] for example, describes rules for the protection of people who do not take part in the fighting.

Outside these rules, terrorist organisations seek to achieve mainly political aims by operations which, under state legislation, are assessed as criminal acts.

With internet technology it is possible for an individual, group or state to carry out remotely controlled, often covert, cyber attacks on critical infrastructures[16] of a state. Therefore the line between soldier, terrorist and criminal becomes blurred.

These terms are not mutually independent and there are many overlaps of scope when discussions take place, especially at a more detailed level, where similar issues and problems are discussed by many communities in both the public and private sectors. Unfortunately, information and experiences are often not shared across communities. This represents a significant challenge for Europe over the next decade and can also be seen as an opportunity. A truly effective approach to dealing with the issues underlying all these related areas will require close collaboration between different communities and a corresponding alignment of approaches.

Finally, our efforts to protect the European information society must not be restricted by definitions of words and artificial barriers to communications, which our adversaries are not subject to - and which they may actually benefit from if our responses are not coordinated across sectors and national borders.

14 http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
15 http://en.wikipedia.org/wiki/Geneva_convention
16 http://en.wikipedia.org/wiki/Critical_infrastructure

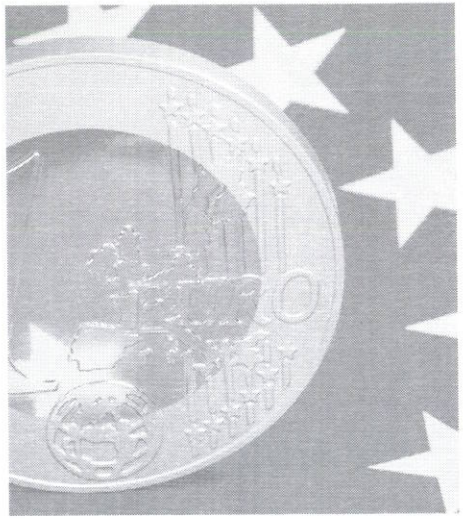
Ensuring a Coherent Pan-European Approach

Any future approach to securing Europe's ICT systems must be coherent across geographical borders and pursued with consistency over time. This is 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. In such an environment, the principle of the weakest link applies; for example weaknesses in one Member State could easily be used to compromise other Member States. Thus, in a global networked environment, there will only be an optimal response if issues that transcend national boundaries are managed and controlled correctly. Without a coordinated global approach to major incidents on the internet, Member States could find themselves in a situation where local systems cannot function correctly due to issues that are outside their control.

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[17] home users' computers can be infected with malicious software, such as a Trojan horse.[18] The computers can then be remotely controlled to attack governmental websites and online services. An example of this was seen in the 2007 cyber-attacks against Estonia.[19]

The EU institutions should provide the support and the framework for Member States to achieve a coordinated global approach. These efforts to improve NIS must involve the private sector: as users of ICTs, as implementers of ICT based business models, as producers of technologies and as operators of services and infrastructure. Last but not least, citizens must be involved and not left to fend for themselves.

17 http://en.wikipedia.org/wiki/Botnet
18 http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
19 http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia



ENISA's Role

ENISA is working together with the Member States to secure Europe's information society. A significant part of this effort is concerned with protecting our infrastructure and applications, and ensuring that we are prepared for incidents when they do happen by reinforcing incident response capabilities across Europe. The focus of ENISA is on cross-border issues, helping Member States to identify dependencies and to decide on the most appropriate way to deal with them.

The Agency achieves 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 good 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.

Where cyber security is concerned, the main contribution of ENISA is in the following areas:

- *Identification and analysis of emerging trends and threats*
- *Awareness of NIS risks and challenges*
- *Early warning and response*
- *Critical information infrastructure protection*
- *Supporting the international CERT community*
- *Adequate and consistent policy implementation*
- *Actions against cybercrime*
- *International cooperation*
- *Information exchange*
- *Building communities*

Identification and analysis of emerging trends and threats

These are explored in more detail below.

On the one hand we are increasingly aware of how sensitive and how vulnerable to attack our IT infrastructures are and on the other hand we lack adequate information by which to be able to recognise and react to dangers in due time. An example of this is botnets.[20] This is a very complex problem to solve because there are so many parties involved – the owners of infected PCs, ISPs, the victims of extortion or click fraud[21], law enforcement, software vendors etc. To make the most of the limited funds available for fighting botnets it is essential to have accurate assessments of the relative size and impact of different botnets. However, the current estimates of the extent of infected machines and botnet activities vary wildly by up to a factor of seven.[22] More generally, we need to move from a situation in which we are making decisions based on information about attacks to a situation in which we are able to refer to discrete data.

ENISA can support the European Commission and Member States by providing them with information on trends, emerging threats and by providing guidance on risk management and appropriate preventative and response measures. For example, ENISA has produced a report on Botnets entitled "Botnets: Measurement, Detection, Disinfection and Defence" which is a comprehensive report on how to assess botnet threats and how to neutralise them.[23] At the moment ENISA does not collect and analyse data on cyber-attacks. However, this could be useful as it would enable ENISA to identify pan-European trends and to report these back to the Member States. ENISA can also facilitate dialogue on NIS across communities and with different international counterparts. We believe that this dialogue is a critical precursor to any long-term action plan for protecting information services that benefit EU citizens.

20 http://en.wikipedia.org/wiki/Botnets
21 http://en.wikipedia.org/wiki/Click_fraud
22 http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence
23 Ibid.

Awareness of NIS risks and challenges

Much of the work that ENISA carries out on a daily basis can be considered as awareness raising. Most of this activity is directly associated with the different work packages that constitute ENISA's annual work programme. For instance, we are examining whether the Computer Emergency Response Team (CERT) community could function as a channel for communicating with businesses and citizens across Europe about NIS issues.

In addition to this ongoing effort, the Agency undertakes specific projects that are concerned with awareness raising as an activity its own right. At present, the Agency is exploring the possibility of a European Cyber Security Awareness Month, which would bring stakeholders together to support and reinforce NIS awareness across Europe. In parallel, we are also working together with certain Member States to see to what extent it is possible to introduce the basic elements of information security into the school curriculum. Achieving this vision would put Europe amongst the leaders in terms of correctly preparing the next generation for dealing with the cyber security issues of tomorrow.

Early warning and response

Early warning

It is critical to have a proactive approach to threats in order to be able to anticipate, counter and attribute them. This approach much be a collaborative effort and cannot be limited only to the boundaries of an industry or of a country. Information collection on attacks, techniques, methods and vulnerabilities needs to be constant and vigilant. ENISA has devised a high-level roadmap for a development of a European Information Sharing and Alert System (EISAS).[24] The Agency has the expertise to support the Member States in implementing it and developing the interoperability services enabling national Information Sharing and Alert Systems (ISAS) to be functionally integrated into EISAS.

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 reinforce CERT cooperation by making available good practice.

ENISA seeks to reinforce this type of cooperation by analysing barriers to cross-border cooperation and proposing measures to tackle them. 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 such as law enforcement, which is important for the fight against cybercrime. As part of this work, the Agency is currently exploring ways in which we can collaborate with Europol.

CERT for EU institutions

The Digital Agenda for Europe[25] is a flagship initiative under the EU 2020 Strategy.[26] Key Action 6 of the Agenda is to: "Present in 2010 measures aimed at a reinforced and high level Network and Information Security Policy."[27] One of the measures identified is the implementation of a CERT for the EU institutions.

A CERT for the EU institutions will deliver strong value as it would, among other things; increase protection against attacks and facilitate swifter reaction to threats; ensure efficiency through shared resources; protect EU competitiveness; and be consistent with EU policy.

24 http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/?searchterm=eisas
25 http://ec.europa.eu/information_society/digital-agenda/index_en.htm
26 http://ec.europa.eu/europe2020/index_en.htm
27 COM(2010) 245 final/2

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 European institutions.

The first steps towards establishing such a CERT have already been taken by the setting up of a pre-configuration team in the summer of 2011.[28] ENISA is supporting the establishment of the EU institutional CERT and has representatives both within the pre-configuration team and the steering committee.

Critical Information Infrastructure Protection

As the communication on Critical Information Infrastructure Protection (CIIP) 'Achievements and next steps: towards global cyber-security' shows, we have, on a pan-European level, already made several important first steps to improve our cyber security. ENISA is facilitating much of this activity, and will continue to do so. In the future, we hope to increase our contribution on the basis of the new mandate for the Agency because, as the communication recognises, "strengthening and modernising ENISA will help the EU, Member States and private stakeholders develop their capabilities and preparedness to prevent, detect and respond to cyber security challenges."[29]

Cyber exercises

In 2010, ENISA facilitated the first pan-European cyber security exercise. This exercise took place in November and involved all 27 Member States and three 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.[30] 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 2011.

This exercise represents an important development in international cooperation and ENISA appreciates 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 and the USA to enhance transatlantic cyber security and cooperation.[31]

Adequate and consistent policy implementation

The cross-border nature of threats today means that there is a need for alignment of European and international legislative frameworks and procedures as well as collaboration models to ensure adequate policy implementation. More importantly, operational measures need to be designed to be capable of delivering results in a cross-border environment.

ENISA is supporting the Member States in the implementation of article 13a of the telecommunications directive.[32] This is important because it is the first attempt to collect data on security breach notifications at the pan-European level. In addition to supporting the Member States with implementation, we are also working on the broader concept. In particular, we are looking into how this data could sensibly be used to provide Member States with a more complete understanding of security breach trends at the pan-European level. By necessity, we consider this as a long-term goal, as it is critical that Member States fully support any model for exploiting the data that has been provided and that they agree on an overall concept for the use of such data.

28 IP/11/694
29 COM(2011) 163 final
30 http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report/view?searchterm=cyber+europe+report
31 MEMO/11/246
32 http://www.enisa.europa.eu/media/news-items/agency-initiative-to-implement-art.-13-of-telecom-package?searchterm=article+13a

Supporting the community in the fight against cybercrime

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."[33]

Improving the capability for dealing with cyber-attacks is one 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."[34]

ENISA acknowledges the importance of the fight against cybercrime as well as the need for a strong collaboration between CERTs and law enforcement. Since its inception, ENISA has sought to foster a good working relationship with relevant communities in both areas. ENISA already acts as a facilitator and information broker for CERTs.[35] The Agency does not, itself, respond to cybercrime, but can assist bodies that do.

ENISA will continue to work together with the CERT community as well as law and enforcement agencies to assist CERTs in their efforts against cybercrime and to work for better protection and resilience of ICT in Europe. For this reason, ENISA appreciates the European Commission's proposal to extend its task list by giving the Agency a role in supporting the fight against cybercrime.

Cybercrime centre

ENISA supports the establishment of a cybercrime centre, as called for in the Internal Security Strategy[36] and recognises the importance of setting up a structured approach to information exchange between this centre and ENISA. ENISA can help the centre set up a dialogue with the CERT community and provide the centre with access to its other stakeholder communities as needed. Furthermore, ENISA can act as a centre of expertise on tools, methods and trends.

The cooperation between the cybercrime centre and ENISA will initially focus on improving awareness about trends and emerging threats, as well as concerns and possible barriers to collaboration and information exchange across sectors and national borders. With the different knowledge, focus and expertise of the centre and the Agency, the exchange of methods and information will help in improving skill sets and achieving a more holistic approach to preventing and tackling cybercrime.

International cooperation

The cross-border nature of threats and the associated mitigation mechanisms make it essential to focus on strong international cooperation. This requires major efforts at national level, at pan-European level and globally. There should be close cooperation with international partners to prevent and to respond to cyber incidents.

At the EU-US summit[37] in November 2010, held in Lisbon, it was agreed to set up a working group on cyber security and cybercrime to evaluate and coordinate opportunities for enhanced collaboration. ENISA will contribute to three Expert Sub-Groups (ESGs). These are looking at Public Private Partnerships, Cyber Incident Management and Awareness Raising.

ENISA expects that international coordination in the area of information security will grow in importance throughout the next decade as countries become increasingly dependent on ICT functions that are offered and maintained in locations outside national boundaries. The recent phenomenon of cloud computing is highly illustrative of this trend.

33 http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA_2011.pdf
34 COM(2010) 673 final
35 And for Computer Security Incident Response Teams (CSIRTs).
36 http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf
37 MEMO/10/597

Information exchange

Information exchange is a fundamental component of any global initiative to improve security. Without effective information exchange mechanisms, European Member States will not be in a position to correctly assess global threats and may therefore put in place procedures and mechanisms that do not address the most important risks.

Similarly, poor information exchange mechanisms are likely to result in a duplication of effort and a slower implementation of approaches, processes and technology for mitigating the key risks once they are understood.

ENISA has significant experience in promoting the exchange of information related to information security between Member States. In the area of CIIP for instance, the approach has been to work together with Member States in order to identify lessons learned from national approaches and to enable Member States to learn from each other. As a concrete example, one of the preparation activities in the cyber security exercise was the exchange of experience at the national level on preparedness exercises.

Building communities

Given the global nature of ICT, and the growing and ever more sophisticated forms of cyber security threats, international coordination and appropriate networks are indispensable. This includes cooperation throughout Europe as well as globally in both the public and private sectors.

Much of our critical information infrastructure is owned and operated by the private sector. As such, addressing threats and strengthening security in the digital society is a shared responsibility – of individuals as much as of private and public bodies. A good example of an initiative to build bridges between the public and private sector is the EP3R (European Public-Private Partnership for Resilience) initiative. Since 2009 ENISA has facilitated and supported the activities of the working groups in the EP3R on security and resilience objectives, baseline requirements, as well as good policy practices and measures.

The Future

With the Lisbon Treaty in force the EU is better placed to take a more holistic approach to cyber security and to exploit synergies in our efforts to improve it. ENISA's mission is to support the Member States and the EU institutions in improving dialogue between 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.

ENISA was established in 2004 with the purpose of contributing to a high level of network and information security "for the benefit of citizens, consumers, business and public sector organisations in the European Union, thus contributing to the smooth functioning of the internal market," as set out in the founding regulation of the Agency.[38] Since then, the challenges related to NIS have evolved alongside technology and market developments. Therefore, the decision has been taken to modernise and further develop ENISA as an efficient body which serves as the EU's centre of expertise in NIS. The intention is to agree on a new mandate for the Agency, which reflects the constantly evolving NIS environment and will give the Agency more flexibility to interact with and respond to the needs of stakeholders across Europe.

38 Regulation (EC) No 460/2004

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.

The success of the EU Internal Security Strategy "is dependent on the combined efforts of all EU actors, but also on cooperation with the outside world. Only by joining forces and working together to implement this strategy can Member States, EU institutions, bodies and agencies provide a truly coordinated European response to the security threats of our time."[40]

ENISA's role is to support the Commission and Member States in facilitating dialogue on Network and Information Security across communities and with different international counterparts. 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, the Agency promotes dialogue and helps Member States to align their approaches to specific issues. The Agency also provides advice to stakeholders, bridging the gap between policy and operational requirements.

There are a number of areas where the current approach to improving cyber security in the EU could sensibly be extended. For example, there is a clear need to collect and analyse data relating to information security in a cross-border context which could reveal trends that are not visible at present. Also, the coming into force of the Lisbon Treaty is an opportunity to improve the level of dialogue between communities in the area of network and information security. A proactive approach to building these new cross-border communities will bring great benefits both in terms of the effectiveness of its approach and efficiency in use of its resources.

It is important that our efforts to protect and facilitate the development and prosperity of the European Information Society do not lose momentum. These efforts are addressed on many fronts with multiple stakeholders – all are increasing in numbers and scope along with the pervasiveness and economic importance of ICTs. It is important that ENISA is modernised and further developed to allow the Agency to respond to these changes and provide support and expertise for stakeholders across Europe.

40 COM(2010) 673 final p. 16

PO Box 1309 71001 Heraklion Greece
Tel: +30 2810 391 280 Fax: +30 2810 391 410
Email: info@enisa.europa.eu
www.enisa.europa.eu