Cybersecurity cooperation

Defending the digital frontline

October 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Udo Helmbrecht, Steve Purser, Graeme Cooper, Demosthenes Ikonomou, Louis Marinos, Evangelos Ouzounis, Marco Thorbruegge, Andreas Mitrakas, Sarah Capogrossi.

Contact

For media enquires about this paper, please use press@enisa.europa.eu.

Executive summary

Securing Europe's Information and Communication Technology (ICT) systems is an important policy goal in the European Union (EU), and ENISA works to support network and information security in the EU's internal market. The Agency works with European bodies and the EU Member States in preparing to respond to challenges raised by Network and Information Security (NIS) threats. It does so by bridging the gap between policy and operational requirements in the Member States and by making available a European platform for information exchange and sharing - amongst Member States and beyond. In particular, ENISA works together with operational communities to ensure that EU NIS policy is implemented in an effective manner, enabling organisations to meet their business goals whilst still benefiting from a high level of security. To meet its policy goals, ENISA acts at three levels: supporting policy and governance, facilitating cross-border collaboration and contributing to preparedness and knowledge.

The recently published Cybersecurity Strategy for the EU (EUCSS)[1] and the associated NIS Directive[2] have proposed a set of actions that will enable Member States to build on accomplishments in NIS to date. They bring separate policy areas into a single coherent policy for the future. The Commission calls upon ENISA to contribute directly to strategic objectives 1 and 4 of the EUCSS ('achieving Cyber resilience' and 'develop the industrial and technological resources for cybersecurity' respectively), whereas the Agency has an indirect role in objectives two and five ('drastically reducing cybercrime' and 'Establish a coherent international cyberspace policy for the European Union and promote core EU values'). ENISA welcomes this opportunity to increase the level of support it is providing to Member States.

In 2013, the Agency also received a new mandate.[3] The new Regulation builds on ENISA's achievements in areas such as supporting Computer Emergency Response Teams (CERTs) in Member States and facilitating pan-European cybersecurity exercises. It provides ENISA with a strong interface with Europol's European Cybercrime Centre (EC3) to enable the Agency to contribute to the fight against cybercrime, focusing on prevention and detection. It also foresees a more proactive role for the Agency in supporting the development of EU cybersecurity policy and legislation. This is also true for the areas of research, development and standardisation, where EU standards for risk management and the security of electronic products, networks and services are cited as key aspects. Finally, ENISA is also given a stronger role in cooperating with third countries.

[1] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Join (2013) 1 final.
[2] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final.
[3] Regulation (EU) No 526/2013 of the European Parliament and the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004

Contents

Executive summary iv

Introduction 1

The threat landscape 4

Figure 1: Overview of Trends assessed in 2012 vs. 2013 mid-year 5

The regulatory landscape 7

Cybersecurity Strategy 7

Draft Directive on Network and Information Security 8

ENISA's new mandate 9

Other regulatory initiatives 9

Responding to policy challenges 11

Support for policy and governance 11
Supporting the CERT for the European Institutions (CERT-EU) 11
Support for Europol and the European Cybercrime Centre (EC3) 12
Requests for advice and assistance 12

Cross-border collaboration 13
Cyber Incident Reporting in the EU 13
Cyber Crisis Cooperation and Exercises 13
The European Cyber Security Month 14
Securing Smart Grids 14
EP3R and NIS Platform 15
Supporting the CERT community 15
CERT / Law Enforcement collaboration 16
Cooperation in the standardisation process 16

(Continued overleaf)

Preparedness and knowledge **17**
Cyber crisis cooperation in Europe 17
Industrial Control Systems Security 17
Cloud computing 17
Resilience of European network interconnections 18
Resilience of European mobile networks 18
ICT Security of inter-bank transactions 18
Baseline capabilities - harmonised approach towards incident response 19
CERT training and good practice 19
Good practice Guides for CERTS: Improving information sharing 19
Network and Information Security driving licence 19

Moving ahead with ENISA **20**

References **22**

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. As societies interconnect with the help of ICT, a new set of opportunities opens up in terms of developing their economic capabilities. However, the increased adoption of information technology has also triggered the development of a significant new set of threats that could negate the promise that ICT holds in terms of economic and societal development. These threats are global in nature and are constantly proliferating, shifting in focus and intensity and exploiting opportunities presented by technology. Adopting mitigation measures is a way to respond to these evolving threats, but it is often the case that technological means need to be accompanied by cross-border collaboration to be effective. Digital boundaries do not coincide with national frontiers, making international collaboration an essential part of the response mechanism. Furthermore, the propagation and implications of threats such as malware (and botnets in particular) illustrate that they are no longer an issue for people to deal with individually, but are increasingly a social and civic responsibility that affects all sectors of the digital society.

In this paper, a distinction is made between 'cybersecurity', 'cybercrime', 'cyber espionage' and 'cyber defence' or 'cyber warfare'. Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization, and users' assets. Organization and users' assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment[4]. Cybercrime is the collective term for criminal activities carried out by means of computers or the Internet[5]. Cyber espionage is the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments or enemies, for military, political, or economic advantage using illegal exploitation methods on the Internet, networks, software and/or computers[6]. Finally, cyberwarfare is a form of information warfare sometimes seen as analogous to conventional warfare[7]. It is important to note that ENISA was established '*with the purpose of contributing to the goals of ensuring a high level of network and information security within the Union and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administrations*'[8]. ENISA's activities are therefore in the area of cybersecurity and the Agency plays no role in the areas of cyber espionage and cyber warfare. ENISA does however support the European Cybercrime Centre in its activities by facilitating communication with other communities and exchanging relevant information related to cybersecurity.

In Europe the response framework contains numerous established policy initiatives in place from the early days of ICT development. The European Commission's Digital Agenda for Europe[9] aims at improving citizens' quality of life through, for example, better healthcare, safer and more efficient transport solutions, a cleaner environment, new media opportunities and easier access to public services and cultural content. 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-

[4] http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
[5] Oxford Dictionary
[6] http://lexicon.ft.com/Term?term=cyber%20espionage
[7] http://en.wikipedia.org/wiki/Cyberwarfare
[8] REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004
[9] A Digital Agenda for Europe, COM(2010)245, May, 2010.

day lives, targeting areas such as online payment and e-government services. ICT is increasingly used in crime and politically motivated attacks. According to the Eurobarometer on Cybersecurity,[10] 29% of EU citizens do not feel confident in using the Internet for banking or purchases, and 12% said they had been victim to online fraud.

Securing Europe's ICT systems must be coherent across geographical borders and pursued with consistency over time. This is work in progress, but it is clear that recent EU policy developments are starting to bear fruit, as approaches that have varied across different Member States and communities have started to converge. Indeed, much of ENISA's work is aimed at facilitating this convergence by encouraging exchange of information, methods and results so as to avoid unnecessary duplication of work and to enable Member States to learn from each other in an optimal fashion.

Initiatives such as the Pan-European Cybersecurity Exercises, the work done in implementing Article 13a of the Telecommunications Framework Directive and the establishing of national and governmental Computer Emergency Response Teams (CERTs) has shown that EU bodies are capable of providing the support and the framework for Member States to achieve a coordinated global approach, under the umbrella of a dependable network and information security policy. [11]

ENISA continues to support the European Institutions and the Member States in preparing to respond to challenges raised by network and information security threats. ENISA bridges the gap between policy and operational requirements in the Member States by providing a European platform for information exchange and sharing amongst EU Member States and beyond. To meet its goals ENISA acts at three levels: supporting policy and governance, facilitating cross-border collaboration and contributing to preparedness and knowledge sharing. ENISA's main tangible contributions are the following:

- Identification and analysis of emerging trends and threats
- Publishing network and information security risks and challenges
- Early warning and response
- Cybersecurity strategies and capacity building
- Critical information infrastructure protection
- Incident Reporting in the EU
- Supporting adequate and consistent policy implementation
- Supporting actors in other communities (for example, industry, law enforcement and academia) in actions against cybercrime
- Supporting the European Commission and the Member States in international cooperation
- Encouraging structured information exchange
- Building communities
- Promoting private public partnerships (PPPs) in the area of cybersecurity

[10] http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

[11] Throughout in this document the terms cybersecurity and network and information security are used interchangeably. While the latter is much more accurate to describe ENISA's area of operation, which is the EU Internal Market, the term cybersecurity is often used to describe situations that require the involvement of law enforcement agencies, falling *inter alia* within the penal law domain.

This paper presents the current operational context for network and information security by summarising the threat landscape. It then presents the recent developments in EU policy and the regulatory framework on network and information security. Furthermore it presents ENISA's concrete contributions in assisting Member States in attaining increasingly higher levels of cybersecurity preparedness.

The threat landscape

The threats we encounter in cyber space evolve rapidly. New methods to compromise data, to gain illegal access to valuable information, to obtain information about user behaviour or to achieve similar objectives are constantly emerging. Such targets are - and will remain - a focus for malicious individuals and organisations acting in cyberspace. In order to develop defences, it is necessary to understand the cyber-threats and the methods used to deploy them.

In the race for primacy between attackers and defenders in cyber space the ability to respond to the evolving cyber-threat environment appears less like a destination and more like a journey. Understanding the components of the evolving cyber-threat landscape is a task that became a major focus for ENISA in 2012 and has been developing rapidly since then. Painting the cyber-threat landscape and keeping up with the dynamics behind it requires an on-going analysis of cyber-incidents reported. Priority lists of cyber threats, threat agents, attack methods and threat trends are all elements that need to be taken into consideration. This information is useful for cybersecurity experts assessing risks to various systems and developing cybersecurity policies for defending valuable information, although care should always be taken when analysing such data – the fact that an event has happened frequently in the past is not a guarantee that it will continue to happen. An example of this is provided by the Stuxnet cyber-attack of 2010, which represented a paradigm shift not so much because of the advanced methods it used to infect and damage industrial control systems, but because it unexpectedly changed the target. There was a new realisation that critical infrastructure, such as nuclear power systems, were susceptible to cyber-attack.

At the end of 2012 ENISA identified top cyber threats and trends for emerging areas of Information Technology that are consolidated in the table, below, with the updated position for mid-year 2013:

Top Threats	Trends assessed in 2012	Current trends mid 2013
Drive-by exploits		
Worms/Trojans		
Code Injection		
Exploit Kits		
Botnets		
Denial of Service		
Phishing		
Compromising Confidential Information		

Top Threats	Trends assessed in 2012	Current trends mid 2013
Rogueware/ Scareware	➲	↑
Spam	↓	↓
Targeted Attacks	↑	↑
Physical Theft/Loss/Damage	↑	↑
Identity Theft	↑	↑
Abuse of Information Leakage	↑	↑
Search Engine Poisoning	➲	Unable to assess trend!
Rogue Certificates	↑	↑

Legend: ↓ Declining, ➲ Stable, ↑ Increasing, ⚠ Warning

Figure 1: Overview of Trends assessed in 2012 vs. 2013 mid-year

As long as the cyber-threat landscape continues to show this very dynamic development, the challenge is to capture the trends as early as possible. The areas that ENISA has kept its main focus on throughout 2013[12], are the following:

Drive-by-exploits: There is a shift from botnets to malicious URLs as the preferred means to distribute malware. An advantage of URLs as a distribution mechanism lies in the fact that they are not such an easy target for law enforcement takedowns.

Code Injection: A notable issue with regard to this threat is attacks against popular Content Management Systems (CMSs). Due to their wide use, popular CMSs make up a considerable attack surface that has drawn the attention of cyber-criminals.

Botnets: Although not new, an interesting aspect of botnet activity reported is the use of botnet infrastructure to mine the "virtual currency" Bitcoins. Another important development is the increased use of peer-to-peer (P2P) botnets that are difficult to locate and take down. Moreover, in Internet Census 2012[13], it has been demonstrated how easy is to create botnet infrastructures by misusing weaknesses in the security of massively deployed devices.

[12] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013

[13] http://internetcensus2012.bitbucket.org/paper.html

Denial of Service: After the 2013 Spamhaus attack,[14] Domain Name System (DNS) reflection attacks have gained in popularity. Moreover, attack bandwidths achieved have reached impressive levels: the rate of 2-10Gbps attacks has doubled, and the level of 300Gbps attack was reached in 2013.

Rogueware/Scareware: In 2013 there was an increase in rogueware/scareware reported. One reason for the growth is the expansion of ransomware and fake Antivirus distribution to mobile platforms, such as Android.

Targeted Attacks: In the first half of 2013, targeted attacks demonstrated their effectiveness in achieving their objectives. In particular, cyber espionage attacks reached a dimension that went far beyond expectations[15].

Identity Theft: This threat led to some of the most successful attacks by abusing SMS-forwarders to commit significant financial fraud. These attacks were based on known financial trojans (e.g. Zeus, SpyEye, Citadel) that have been implemented on mobile platforms and attack two-factor authentication. A significant source for applying this threat remains social media.

Search Engine Poisoning: Search Engine Poisoning has also gone mobile: some reports on malicious mobile apps performing Search Engine Optimization poisoning have been found.

These developments lead to the conclusion that attackers remain one step ahead; quite often it suffices to exploit simple and well known weaknesses to cause havoc. The key message of ENISA is to transfer knowledge from the cybersecurity community to the user groups for the purpose of strengthening cyber-defence.

[14] http://www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability/at_download/fullReport

[15] https://www.enisa.europa.eu/publications/flash-notes/cyber-attacks-2013-a-new-edge-for-old-weapons/at_download/fullReport

The regulatory landscape

Since its inception in 2004, ENISA has contributed 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,"[16] as it was set out in the then founding regulation of the Agency. The current mandate of ENISA in the area of Network and Information security has been based on Article 114 of the Treaty on the Functioning of the European Union (TFEU) and it is in accordance with decision C-217/04 of the European Court of Justice.[17] Under the Lisbon Treaty, Article 114 of the TFEU describes the internal market responsibility and it continues being the applicable legal basis for adopting measures to improve Network and Information Security.[18]

A significant part of the Agency's work is concerned with supporting the protection of infrastructure and applications, and ensuring preparedness to counter threats and reinforce 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. While the focus of the Agency remains on the internal market, with ENISA's new mandate, received in 2013, it has the ability to collaborate in other relevant areas such as law enforcement, lending it support and expertise. Following up on the policy priorities of the Digital Agenda, in 2013 the European Union laid out a Cybersecurity Strategy, and proposed a Directive on Network and Information Security, acknowledging the renewal and expansion of ENISA's mandate.

Cybersecurity Strategy

A new comprehensive Cybersecurity Strategy for the European Union[19] comprises the internal market, justice and home affairs and foreign policy aspects of cyber space issues. The Cybersecurity

16 ENISA was founded by Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. The mandate was firstly extended by Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration and secondly by Regulation 580/2011 of the European Parliament and of the Council of 8th June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration. The new and current, basic ENISA Regulation is Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013, concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

17 ECJ 02.05.2006, C-217/04, United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union.

18 The Internal Market responsibility is a shared competence between the Union and the Member States (Article 4(2)(a) TFEU), which allows the Union and the Member States to adopt binding measures. The Member States will act if the Union has not exercised its competence or has decided not to act any more (Article 2(2) TFEU).

19 Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Join (2013) 1 final

Strategy offers clear priorities for the EU's international cyberspace policy, in terms of freedom and openness, outlining the vision and principles of EU core values and fundamental rights in cyberspace. This complements the role of the EU in the physical world. Furthermore, cybersecurity capacity building means that the EU will engage with international partners, the private sector and civil society to support capacity building in third countries. It will include improving access to information and to an open Internet, and preventing cyber threats. Finally, there is the aim to foster international cooperation in cyberspace issues, with the goal of preserving open, free and secure cyberspace. This is a global challenge, which the EU will address together with relevant international partners and organisations, including the private sector and civil society.

In the Cybersecurity Strategy the Commission has envisaged a key role for ENISA, with the Agency supporting cyber resilience, i.e. ensuring that critical information infrastructure and network structures in general are adequately protected.

Moreover ENISA supports the Commission in developing the industrial and technological resources necessary for cybersecurity, in cooperation with relevant stakeholders. In this regard ENISA will promulgate technical guidelines and recommendations for the adoption of network and information security standards and good practices in the public and private sectors.

Additionally, ENISA will be directly involved in reducing cybercrime by developing its relationship with Europol's European Cybercrime Centre (EC3) to identify emerging trends and needs in view of evolving cybercrime and cybersecurity patterns, to develop appropriate digital forensic tools and technologies.

In 2013, ENISA has been assessing the implementation of a roadmap for a "Network and Information Security driving licence" and it supports the organisation of a yearly cyber-security month.

ENISA works to make sure that the implementation of policy and strategy is firmly based on operational experience, that policy is aligned with industry expectations and that it is economically viable. ENISA will seek to implement scenarios in close collaboration with industry and the public sector to define good practices in an efficient and market-oriented way.

Draft Directive on Network and Information Security

The Draft Directive on Network and Information Security[20] (hereafter, the proposed Directive on NIS), aims at ensuring a high common level of network and information security, by improving the security of the Internet and the private networks and information underpinning the functioning of societies and economies in the EU. The proposed Directive on NIS requires Member States to increase their preparedness and improve their cooperation with each other in the areas of critical infrastructures e.g. energy, transport, information society services, public administrations etc. Additionally it requires Members States to adopt appropriate measures to manage security risks and incidents reporting.

The proposed Directive on NIS also aims at creating a collaboration framework, within which the Member States and the European Commission can share early warnings on risks and incidents. Sharing is facilitated by a secure infrastructure that can be managed by the European Commission.

[20] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final.

Additionally, market operators and public administrations alike have to adopt a risk based approach in reporting major security incidents in their core services.

The proposed Directive on NIS foresees a role for ENISA in terms of facilitating collaboration and managing security risks and information with Member States. Additionally, the proposed Directive helps to establish common minimum requirements for network and information security at national level. It requires Member States to designate national competent authorities for NIS, and draw up strategies on network and information security supported by the operation of CERTs' risk mitigation and response mechanisms. It is also expected that the private sector will develop its own cyber resilience capacities and shares best practices across sectors.

ENISA's new mandate

The new ENISA Regulation updating the Agency's mandate[21] enshrines ENISA's achievements in key areas of network and information security and it underscores the requirement to continue implementing measures that further the ability of the EU and of the Member States to tackle cyber threats to the internal market. The new Regulation provides a mandate for ENISA in terms of:

- Providing ENISA with a strong interface with the fight against cybercrime - focusing on prevention and detection - with Europol's European Cybercrime Centre (EC3)
- Supporting the Member States on building capacity for CIIP and cybersecurity strategy
- Supporting the development of EU cybersecurity policy and legislation
- Supporting research, development and standardisation, with EU standards for risk management and the security of electronic products, networks and services
- Supporting the prevention and detection of, and response, to cross-border cyber-threats
- Supporting the European Commission in implementing certain aspects of the EU Cybersecurity Strategy (e.g. NIS Platform). Aligning ENISA more closely to the EU Regulatory process, providing EU countries and Institutions with assistance and advice (e.g. on incident reporting, proposed NIS Directive).

ENISA seeks to become the catalyst that brings together existing groups to work on problems which are important in today's policy agenda; once these groups start working together ENISA can then focus on other areas of interest.

The new mandate gives ENISA a more proactive role in cyber security. This is illustrated in the area of standards, where ENISA will facilitate the establishment of technical standards on network and information security instead of passively tracking standards (as specified by the former mandate).

Other regulatory initiatives

Other regulatory proposals have provided fresh impetus for ENISA's involvement in new policy areas. ENISA has also been an active contributor to EU policy and support to Member States in

[21] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

implementing Article 13a of the telecoms Framework Directive.[22] ENISA also assists Member States in implementing Article 4 of the e-Privacy directive.[23]

In 2012, the European Commission made a proposal for a Regulation on electronic identification and trusted services for electronic transactions in the internal market,[24] and it addresses shortcomings of Directive 1999/93/EC on a Community framework for electronic signatures, aiming at secure and seamless electronic transactions.

[22] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

[23] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[24] COM(2012) 238/2Proposal for a Regulation of the European parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Responding to policy challenges

In response to its own policy goals emanating from the regulatory framework, ENISA aims at providing:

- Support for policy and governance: Supporting the EU bodies, ENISA contributes to specific policy goals with designated Commission Services and Agencies, helping them meet their goals.
- Cross-border collaboration: the response to Network and Information Security challenges depends on the ability of the respondents to act together in a coordinated manner. ENISA seeks to identify the areas where collaboration is likely to bring about tangible results and then it seeks to coordinate efforts and actuate the stakeholders involved to take measures mitigating perceived risks.
- Preparedness and knowledge: as a centre of expertise, ENISA develops its own content and capabilities in a range of areas of broad policy interest, supporting its stakeholders with analyses and recommendations on issues of concern.

Support for policy and governance

In terms of policy and governance ENISA has received a clear mandate to provide support to the European Commission's CERT for the European Institutions, as well as the European Cybercrime Centre (EC3) at Europol. ENISA has also been actively supporting the Member States in implementing Article 13a of the telecommunications Framework Directive[25] and it assists Member States in implementing Article 4 of the e-Privacy directive.[26] Additionally, ENISA will support Member States in implementing article 15a of the proposed EU eTrust Directive[27]. ENISA therefore has the opportunity to contribute to concrete collaborative efforts at the level of the Member States as well as with the EU bodies, supporting all with advice and assistance.

Supporting the CERT for the European Institutions (CERT-EU)

In 2012, a permanent Computer Emergency Response Team (CERT-EU) for the EU bodies was set up. CERT-EU brings together IT security experts from the European Commission, General Secretariat of the Council, European Parliament and Committee of the Regions/Economic and Social Committee. It cooperates with other CERTs in the Member States and beyond, as well as with specialised IT security services. CERT-EU is likely to extend its services, on the basis of the requirements of its constituency, and taking into account the available competencies, resources and partnerships. The role of ENISA is to provide support to CERT-EU, building on its successful work with administrative

[25] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

[26] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[27] COM(2012) 238/2Proposal for a Regulation of the European parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

and governmental CERTs. The Agency will pursue two different approaches - introducing and integrating CERT-EU into existing CERT communities, and building up and extending CERT-EU capabilities by means of providing appropriate training.

Support for Europol and the European Cybercrime Centre (EC3)

ENISA's new Regulation gives it the scope to closely cooperate with Europol in supporting the fight against cybercrime. Europol hosts the European Cybercrime Centre (EC3) that coordinates law-enforcement efforts in combating cybercrime. In 2013 ENISA collaborated with Europol in such areas as the 8th Annual CERT workshop, co-organised with the European Cybercrime Centre, as well as involving Europol and the EC3 in network and information security projects. While Europol and EC3 clearly serve the operational aspect of the fight against cybercrime, ENISA contributes by deepening the cooperation capabilities between CERTs and law enforcement agencies, for example by developing training for CERTs to support this cooperation further and by regularly bring people from both sectors together to discuss operational issues and obstacles, e.g. how to handle evidence when first entering a crime scene.

Requests for advice and assistance

In line with article 14 of the ENISA Regulation, the Agency stands ready to support the needs of the Member States, the European Commission and the European Parliament with expertise on network and information security. An area that ENISA sees gaining in importance and visibility is CERT in-house training for designated stakeholders in the Member States and in EU Institutions. In 2013, ENISA responded to the following requests:

- The National Regulatory Authority of Cyprus (OCECPR) sought the support of ENISA in a workshop organised with the participation of the Cypriot electronic communications providers. ENISA's role was to represent the European context and provide suitable advice.
- A request from Estonia was responded to by organising and delivering training on "Incident handling during an attack on Critical Information Infrastructure".
- Latvia's Information Technology Security Incident Response Institution CERT.LV made a request for ENISA to provide an on-site training course on "Social networks used as an attack vector for targeted attacks". Additionally, ENISA contributed to the CERT.LV annual conference "Information Security – Key for Success."
- The Agency for the Cooperation of Energy Regulators (ACER), has been setting up an IT system to collect and analyse data on wholesale market energy markets across the EU, and asked for the support of ENISA to ensure operational reliability and protection of the received data and prevent unauthorised access to that information.
- A request of the European Commission (DG HOME) to provide input in the context of the review of the EU legal framework for data retention has been dealt with. ENISA's contribution seeks to identify the benefits, main impacts and possible means of enforcement of new data security measures in the reform. ENISA is also assessing the "good practice" potential of current security measures for data retention in selected Member States.
- At the request of the European Commission, ENISA organised a seminar on the organisation and planning of cyber exercises. An outline of a "cyber-scenario" was developed and adapted to the needs of the European Commission using as guidance input from the Cyber Europe 2012 exercise which was facilitated by ENISA.

Cross-border collaboration

The primary goal of ENISA is to be a catalyst where collaboration is essential to bring about tangible results in the area of network and information security. The emerging regulatory framework underscores this role. Collaboration and exchange of information are essential elements in the fight against cybercrime. When the integrity of networks, infrastructures and control systems is at risk, threatening millions of citizens and business, acting alone pays no dividends. ENISA has a successful record of helping others to help themselves, by bringing together stakeholders involved in a policy area in network and information security. ENISA is the organisation that helps stakeholders translate policy into action.

Cyber Incident Reporting in the EU

Security incidents leading to large outages and data breaches still remain largely undetected as information about them is collected mostly for the in-house use of those affected. This shortcoming makes it difficult for regulatory authorities to improve on measures to take and serve public interest by disclosing breaches that concern individuals and businesses alike. The Framework Directive on electronic communications[28] stipulates measures that have been supported by ENISA. ENISA has set up a national regulators' expert group that has developed a set or reporting procedures for incidents. Additionally, in an annual incidents report, the Agency analysed 79 major incidents and given an overview of their causes. Lastly, ENISA provided recommendations on national roaming as a measure for mitigating mobile network outages, and power supply dependencies to reduce the impact of power outages on electronic communications.

In 2013 the Agency started a new expert group of supervisory authorities (being, data protection authorities and telecommunications regulators) for the implementation of Article 4 of the e-privacy directive.[29] The main goal is to provide a platform for exchanging experience between experts in different countries. Where possible, ENISA seeks to build on synergies between expert groups on Article 13a and Article 4, to develop a unified framework for security measures and incident reporting. ENISA also assists Member States in the implementation of article 15 of the directive on electronic identification and trusted services for electronic transactions in the internal market. The Agency brings together competent regulatory bodies in the Member States, and supports debates on the services concerned, the reporting scheme, and the parameters and thresholds.

Cyber Crisis Cooperation and Exercises

ENISA has a strong track record of contributions in cyber crisis cooperation and exercises in the EU. This is an area where ENISA has made major breakthroughs, such as its series of pan-European cyber

[28] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

[29] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

exercises, establishing strong relationships and gaining the commitment of European Union Member States. In 2013, ENISA issupporting the cybercrisis management exercise of the Eurocontrol air traffic control agency, with a large-scale cyber incidents scenario. ENISA builds successful exercises by establishing the cyber exercises area, and building a high-level of expertise by bringing together Member States, European Free Trade Association (EFTA) countries, and EU Institutions.

ENISA's series of international conferences on cyber crisis cooperation and exercises offers a key knowledge sharing platform to international cyber security experts and decision makers, highlighting how to deal with cyber crises and applying appropriate contingency plans and escalation procedures. The conferences aim to facilitate debate and information exchange and offer networking opportunities to both technical experts and executive stakeholders.

In 2013, ENISA organised its second International Conference on Cyber Crisis Cooperation and Exercises, with a focus on various topics in the area of cyber crisis cooperation. These include information gathering and common situational awareness, escalation processes and procedures, cybercrisis management in the general crisis management context, cross-border cyber exercises, and tools and platforms for information exchange and communication.

As cyber exercises and European network and information security cyber cooperation plans and procedures gradually come together, ENISA will continue to support an umbrella EU NIS cooperation plan, in line with the EU Cybersecurity Strategy. Starting from 2014, the cyber exercises will aim to cover all levels of escalation when cyber incidents lead to a cyber-crisis and will thus test technical level, operational level and political level cooperation procedures and responses.

Similarly, international efforts, with conferences organised by ENISA and the cooperation of third countries, are continuing, thus contributing to an enhanced level of preparedness to face cyber-crises on a global scale.

The European Cyber Security Month

In 2013, a fully-fledged European Cyber Security Month (ECSM) is taking place across Europe with the support of DG CNECT and ENISA, bringing together over 40 public and private actors and implementing more than 50 activities.[30] As an instrument of collaboration among stakeholders in network and information security, ENISA seeks to facilitate sharing good practices, and thereby increase the results for the work of network and information security communities. ECSM is an EU campaign that takes place in October to promote cybersecurity awareness and training among citizens. The campaign has the objective of changing the perceptions of cybersecurity threats at work and in the private sphere. It also aims to provide updated security information through education, good practice and competitions.

Securing Smart Grids

ENISA has launched a series of activities aiming to bring together stakeholders in the area of critical information infrastructure protection and engaging them in an open discussion on smart grid cybersecurity. The principal goal is to identify the main issues of concern regarding the security of

[30] Network Information Security events are taking place in 26 countries: Austria, Belgium, Bulgaria, The Czech Republic, Germany, Estonia, Greece, Spain, Finland, France, Hungary, Ireland, Iceland, Italy, Latvia, Lithuania, Luxembourg, Moldova, The Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Sweden and the United Kingdom.

smart grids in support of national, pan-European and international initiatives. ENISA supports the efforts of the European Commission and of the Member States on smart grids by facilitating Expert Group 2 on Regulatory Recommendations for Privacy, Data Protection and cyber-security in the Smart Grid Environment.[31] In an effort to advance collaboration in this field ENISA has been tasked by Expert Group 2 to organise consultations on these minimum security requirements with national cybersecurity authorities and the energy and ICT industries, and possibly also selected non-EU partners. Based upon this process, recommendations to Member States on minimum cybersecurity requirements for smart grids will be drafted.

EP3R and NIS Platform

The European Private Public Partnership for Resilience (EP3R) was established as a follow-up to the policy initiative on Critical Information Infrastructure Protection (CIIP) adopted by the European Commission on 30th March 2009.[32] The scope of EP3R was to propose strategic and tactical solutions, in the areas of: key assets, resources and functions; baseline requirements for security and resilience; and coordination, cooperation and response to large-scale disruptions. ENISA chaired task forces and work objectives groups, providing a flexible structure to allow the development of the works, supplying secretariat support and technical expertise. After two years of operation, a stocktaking exercise is under way to understand the impact of EP3R and propose improvements.

In 2013, EP3R is being followed by an initiative called the NIS Platform. The NIS platform is organised in working groups that aim to provide a further dimension to Public-Private Partnerships in Europe. ENISA plans to provide technical support to NIS Platform working groups, subject matter advice on issues discussed in the working groups and background research on open issues raised.

Supporting the CERT community

Capacity building for CERTs in the EU has been central to ENISA throughout 2013. CERTs are key for Critical Information Infrastructure Protection and are a primary security service provider for governments and citizens.

The 8th annual CERT workshop was held in Bucharest, Romania, and was co-located with the 39th TF-CSIRT meeting. The workshop focused on ENISA CERT exercises and fostered cross-sector collaboration, in particular between CERTs with national and governmental responsibility and their national law enforcement “counterparts”, emphasising “automated sharing of information”. In this workshop ENISA experts provided technical training to attendees, focusing on “Incident handling during an attack on Critical Information Infrastructure”, ”Mobile threats incident handling” and “Honeypots”.

[31] In 2009, the Smart Grids Task Force (SGTF) was set up by the European Commission (EC) to reach a consensus on policy and regulatory directions for the deployment of Smart Grids. SGTF operates in five discrete Expert Groups.

[32] The Communication on Critical Information Infrastructure protection (CIIP) of the European Commission focuses on the protection of Europe from cyber disruptions by enhancing security and resilience. The action plan brings together Member States and the private sector and it is based on five pillars: preparedness and prevention, detection and response, mitigation and recovery, international cooperation and criteria for European Critical Infrastructures in the field of ICT.

CERT / Law Enforcement collaboration

The fight against cybercrime is important to law enforcement agencies across Europe and worldwide. ENISA aims at bringing CERTs to closer collaboration with law enforcement bodies in order to make skills and expertise available to combat cybercrime. ENISA seeks to facilitate cross-sector community building, bringing together operational players, and actively supporting cross-sector training and education. The work aims to develop trust between these two sectors through regular meetings and training. Additionally, alternative strategies include discussions and exchange of good practices in operational areas (such as guidelines for first responders entering a crime scene), or tackling legal issues with cross-border sharing of operational information (log files, IP addresses, etc.). Ideally the outcomes of discussions result in further items to address in the future, developing new material for common training with CERTs and law enforcement personnel.

Cooperation in the standardisation process

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 needs to be close cooperation with international partners to prevent and to respond to cyber incidents. ENISA tracks the development of standards from a more global perspective in Network and Information Security. The Agency monitors network and information security standards in the EU and globally, including areas that are not specifically related to the priorities of the ENISA work programme. This approach allows the Agency to keep its stakeholders informed on new network and information security standardisation activities and to flag opportunities and/or risks as they develop.

In 2013, ENISA is continuing to contribute to the joint ETSI CEN-CENELEC Cyber Security Coordination Group (CSCG), an advisory and coordination body on political and strategic matters related to cybersecurity standardisation. The role of ENISA is to assess whether there is a gap between these standardisation activities and state-of-the-art developments in network and information security.

Preparedness and knowledge

As a centre of expertise, ENISA has continued to develop its unique body of knowledge in network and information security, aiming at informing policymakers, businesses and citizens alike. The areas that ENISA undertakes to develop are influenced of course by regulatory developments, threats and policy requests.

Cyber crisis cooperation in Europe

ENISA carried out a study on National Network and Information Security Contingency Plans by analysing the national-level best practices, procedures, roles and responsibilities, for management and cooperation during major cyber incidents, escalating to a cyber-crisis.

In the framework of the Cyber Europe series of exercises organised by ENISA, the EU Member States have prepared procedures for cooperation at the operational level, including alerting, information exchange and situational awareness. In 2013, a report of the working group of the EU Forum of Member States (EFMS) on European Cyber Crisis Cooperation Framework (ECCCF) identified the need for cooperation at all three levels: technical, operational/tactical and political. In response ENISA drafted a report that took into account the above-mentioned considerations.

The operational procedures developed within the context of the Cyber Europe exercises, as well as the existing national-level NIS Cooperation Plans in EU Member States, would play a central role in establishing a European Union-level NIS Cooperation Plan, in line with the proposed Directive on NIS.

Industrial Control Systems Security

Industrial Control Systems (ICS) are command and control networks and systems designed to support industrial processes in such industries as gas and electricity distribution, water treatment, oil refining and railways. Industrial control systems constitute a strategic asset, with a rising potential for catastrophic terrorist attacks affecting these critical infrastructures. These systems have often been the target of malicious actors in cyber-attacks. While industrial control systems are sufficiently robust the operation, management culture and appreciation of threats in these systems could be improved. ENISA has carried out an analysis to facilitate agile and integrated responses to incidents contributing to their analysis.

In industrial control security, independent evaluations and tests are missing, leading to the ineffective operation of industrial environments. ENISA aims at assessing the need among the Member States for a national ICS-SCADA testing framework, identifying the gaps in testing practices and producing guidance for both the development of new and harmonization of current ICS-SCADA test beds frameworks (if any) among Member States. Finally a good practice guide on a European ICS-SCADA test bed programme/framework will be developed. Additionally ENISA provides advice on assessing the challenges involved in developing ICS-SCADA patching good practices and it has provided relevant recommendations.

Cloud computing

ENISA lends its support to the Member States in terms of incident reporting in Cloud computing services (e.g. eHealth, transport etc.). In that respect ENISA is preparing a good practice guide on

how to report outages in cloud computing according to their impact and the criticality of the service affected.

ENISA supports the European Commission on the implementation of their EU cloud strategy. The report on Securing Governmental Cloud Computing infrastructures is a study on the cloud uptake across the EU. It includes initiatives at national and regional level and provides a set of recommendations on how to safely deploy cloud solution in the public sector. Also ENISA's security guidance for SMEs is an updated version of the 2009 risk assessment. It focuses on SMEs presenting the highest risks and opportunities. Finally ENISA participates in the certification industry group of the EU Commission that aims at establishing a list of certification schemes and support voluntary certification schemes for cloud computing providers. In May 2013, ENISA launched the "Cloud Security and Resilience Experts group" where experts from industry and the public sector participate.

Resilience of European network interconnections

In 2013, ENISA is furthering its goals in the area of resilience of network infrastructures and the mechanisms for emergency communications that have been in place in Member States by shifting focus to the technical and the organisational component. ENISA seeks to provide insight to the "structure of the Internet" at the physical and network layers in the Member States, which could be used by governments or policymakers to develop a strategy to ensure that critical services remain functional when there are interruptions in network performance or connectivity. An additional policy and organisational component aims to collect information on the legal framework concerning the relationship between telecommunications regulators and Internet Service Providers involved in the Member States in order to improve collaboration.

Resilience of European mobile networks

To counter outages involving mobile network operators in the EU, ENISA analyses national roaming frameworks which allow customers to use the network of other mobile operators. The main goal of this work is to investigate how and if national roaming could be used to address the impact of outages in terms of technical, legal, financial and administrative aspects. The scope includes mobile devices at large, including mobile communications between machines. The goal is to provide a set of approaches that telecommunications' Regulators could consider in mitigating mobile network outages using national roaming. The impact of this activity is significant in civil protection, crisis management and critical industries as improving resilience of mobile communications for critical functions and critical services that rely on mobile networks can generally be improved.

ICT Security of inter-bank transactions

The challenges faced by financial sector ICT professionals in ensuring integrity, availability and confidentiality of information in transit have been analysed by ENISA in terms of risk awareness, the state of prevention of security risks, ways to detect incidents, policies and organisational aspects. ENISA seeks to identify actual challenges faced by ICT professionals in the financial sector in terms of ensuring the integrity, availability and confidentiality of information in transit. A global stocktaking activity on the matter would help ENISA *inter alia* to better understand:

- The actual risk awareness among ICT professionals of the financial sector
- The state of prevention of security risks

- How incidents are detected, associated risks are mitigated and flaws are fixed on a continuous basis
- Whether global policies favour the response to incidents
-

Baseline capabilities - harmonised approach towards incident response

ENISA supports Member States in enhancing and strengthening cooperation among CERTs to achieve powerful incident response when needed. Continuously working together with the CERT community on improving a common "denominator", called "CERT baseline capabilities" that allows for better cross-border information sharing and cooperation. In 2013 ENISA is assessing the level of compliance of CERT Baseline Capabilities in the Member States and is providing a report on harmonisation in such areas as terminology, validation processes and requirements. ENISA will further examine a suitable certification (or similar) to assess the baseline capabilities of CERTs.

CERT training and good practice

In 2013 the ENISA CERT training programme is continuing by developing the curriculum further to include new scenarios on cybercrime for CERT and Law Enforcement Agencies' staff. The CERT training material features a handbook for the tutor and a toolset for students, together with virtual computer images to support hands-on training sessions on the students' computers. Additionally ENISA is re-releasing the TRANSITS program with training material for new CERT staff.

Good practice Guides for CERTS: Improving information sharing

Secure communication and information sharing on security threats can be shared among CERT teams to improve security and efficiency, as well as to speed up incident response. In 2013, ENISA is reviewing enablers and barriers for information sharing. Taking stock of the current communication exchange practices of CERT teams and input from standards, this initiative aims at improving information sharing practices. A good practice guide in the area of "Alerts, Warnings and Announcements," aims at addressing issues related to these areas, as well as increasing the security awareness of stakeholders.

A good practice guide on the practical implementation of the "Directive on attacks against information systems and repealing Council Framework Decision - 2010/0273(COD)"[33] aims at identifying the implications of the Directive on stakeholders such as (national/governmental) CERTs and law enforcement bodies. This guide focuses on how to implement the Directive in the Member States and makes relevant recommendations.

Network and Information Security driving licence

The EU Cybersecurity Strategy suggests the developing a roadmap for a Network and Information Security driving licence as a voluntary certification programme to promote enhanced skills and competence for IT professionals. In 2013, ENISA kicked off the consultation process with relevant stakeholders to guide the process.

[33] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

Moving ahead with ENISA

The Cybersecurity strategy of the EU has given new impetus to the response of the EU to cybersecurity challenges. The high political visibility of this initiative was demonstrated by the joint involvement of Commissioners Cécilia Malmström, Vice President Neelie Kroes and High Representative Cathy Ashton. Political attention and support for this strategy is fundamental in order to see a stable and safe progression in improving cybersecurity and curbing the impact of cybercrime.

ENISA has provided much sought after expertise to guide policymakers with dependable opinion and substantiated recommendations. Additionally, it has coordinated efforts of actors involved and stakeholders at large in order to be more efficient, focused and effective in taking important decisions in cybersecurity preparedness. The role of ENISA in implementing the EU policy and regulatory framework might sometimes go unnoticed, as initiatives undertaken are often discreet by nature and actions happen behind the scenes; ENISA however has proven its ability to act discreetly as a catalyst, and to actuate stakeholders with a view to bringing about change in network and information security. With the advent of the new mandate, ENISA looks forward to becoming further involved in promulgating information security standards, which in the EU is a way to narrow the gap between policy and operational performance.

ENISA supports the European Commission and Member States by providing them with information on trends and emerging threats, and by providing guidance on risk management and appropriate prevention and response measures. The Agency also facilitates dialogue on Network and Information Security across communities and with different international counterparts. This dialogue is a critical precursor to any long-term action plan for protecting information services that benefit EU citizens and it helps Member States to align their approaches to specific issues.

EU cyber cooperation is again at a crossroads as the regulatory framework has to be transposed and implemented across the EU. Additionally the emerging regulatory framework in electronic communications, privacy and trust is likely to lead to greater cooperation among stakeholders. ENISA, with its newly defined role, remains in support of policy, coordination and expert knowledge. ENISA is a key player supporting the alignment of public and private sector strategies to reach a level of common policies and good practices that will give the EU an edge in mitigating cybersecurity risks. ENISA with its unique mission has a clear role to play in helping the Commission and Member States in turning high level policy into action items, and engaging with stakeholders to help them actuate and eventually help themselves.

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"[34]. Being proactive in building cyber cooperation in cross-border communities will bring benefits both in terms of the effectiveness of common strategies and efficiency in the use of evolving assets.

[34] COM(2010) 673 final p. 16

Network and information security will always need to be built into future plans, as it is an issue that is here to stay, with ICT leading growth. In the interdependent world that we live in, acting together in a cohesive manner is essential. ENISA has undertaken the pivotal role to provide support and expertise whilst responding to challenging digital changes. If the Internet fails to remain safe the impact for modern societies will be too costly to bear. All efforts and strategies towards securing Europe's cyber cooperation must be coherent, consistent and united; and there is no better time to respond and move ahead than now.

References

Regulation (EU) No 526/2013 of the European Parliament and the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.

A Digital Agenda for Europe, COM(2010)245, May, 2010.

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

Regulation 580/2011 of the European Parliament and of the Council of 8th June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

ECJ 02.05.2006, C-217/04, United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union.

Treaty for the Functioning of the European Union.

Joint communication to the European parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Join (2013) 1 final.

Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final.

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

COM(2012) 238/2Proposal for a Regulation of the European parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

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 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu