

EU cyber cooperation the digital frontline

EU cyber cooperation: the digital frontline

Author: ENISA

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

- 4 Executive Summary
- 6 Explaining the terms
- 8 Introduction
- 10 The Evolving Threat Landscape
- 14 Mitigating the Threats – a reality check
- 16 Examples of ENISA’s contribution to cyber security
- 17 Cyber exercises
- 21 Supporting the CERT Community
- 22 “Be Aware, Be Secure”: the first European Cyber Security Month
- 23 Cyber crisis cooperation conference
- 23 Workplace IT: The “Bring Your Own Device” trend
- 24 Improving Security Breach Notification: Article 13a
- 25 Liaising with the EU Cybercrime Centre (EC3)
- 26 International cooperation
- 27 Information exchange
- 28 Cyber cooperation communities
- 29 ENISA’s role - looking ahead
- 30 Conclusion

Legal notice

Please note that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA), 2012

Executive Summary

We all share a common interest in guaranteeing a free, safe and sound life in cyberspace. ENISA firmly believes EU cyber cooperation is crucial to establishing a proficient and coherent approach to Network and Information Security (NIS). This includes coordination 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. What are the next steps to build stronger bridges and common ground in these ever-evolving cyber scenarios? What are the EU institutions', the private sector's and the citizens' next challenges in responding to destructive digital assaults?

Information and Communication Technologies (ICT) have provided countless benefits to citizens, businesses and governments, and have reinvented Europe's society and economy. The future of such technologies holds a double edged sword: greater benefits and inevitably, new threats. Very few of us are in a position to appreciate the magnitude of damaging activity that occurs online every day, yet all of us depend inextricably on cyber-space and the multi-dimensional facets it entails. The number and sophistication of cyber-attacks affecting public and private information systems has increased dramatically over the last year, and is expected to continue to grow at a fast pace.

The borders between virtual and real worlds are dissolving. New technologies, services and business models push existing concepts and regulation to their limits. The organizational structures and physical barriers that have stood for centuries, are being severely put to the test by cyber threats that are continually evolving. Even national borders may hinder us more than protect us against challenges which are global in nature and which require responses that are coordinated across sectors, organizations and national borders. The leading role that information technologies play in modern society have made cyber security essential to the worldwide economy.

We are currently witnessing unprecedented prospects that an open and free cyberspace brings to all our societies. We therefore need to take all precautions to make sure that *the Internet is not becoming the victim of its own success*.¹ In this context, it is interesting to note that according to the Special EUROBAROMETER 371 on Internal Security, eight out of ten (81%) Europeans consider cybercrime to be an important challenge to EU security, 43% saying that it is a very important challenge, and 38% describing it as important².

Since its launch in 2004, ENISA has been striving to build bridges between communities by promoting cooperation across the EU and further. It has successfully done so, in activities such as supporting the CERT community (including the newly formed EU CERT), organising the Cyber Europe and Cyber Atlantic exercises, assisting the Member States in implementing the requirements of security breach notification legislation and many more. The Agency aims to support those communities that are striving to improve the level of EU cyber security by improving the resilience of critical information infrastructures and services, in both public and private sectors.

1 http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/132712.pdf

2 http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf

3 Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)

ENISA's recent achievements in cooperation include:

- Managing Europe's biggest ever cyber security exercise, Cyber Europe 2012, involving all EU Member States and countries from the European Free Trade Area (EFTA)
- Taking a formal role in Europe's Cyber Incident Reporting framework, under Article 13a of the EU's Telecommunications Framework Regulation³
- Responding quickly and efficiently to Member States' requests for Assistance, through ENISA's Athens-based Mobile Assistance Team (MAT)
- Helping to establish new Computer Emergency Response Teams (CERTs) in Malta, Romania, Cyprus and Ireland, as well as on-going support to established teams

In addition, a new ENISA Regulation is progressing towards its final stages within the European Parliament and the Council of Ministers.

The coming into force of the Lisbon Treaty offers an unparalleled 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 effectiveness of approach and efficiency in use of resources.

At a time in which the importance of cyber security is recognised by all, it is important that efforts to protect and facilitate the development and prosperity of the European Information Society do not lose momentum due to insufficient preparatory measures for a range of security-related incidents that could result in large scale disruption. ENISA is assisting the Commission and the Member States in identifying and preparing for such incidents and is actively collaborating with a wide-range of stakeholder communities as part of this effort.

Finally, it is important that ENISA is fully supported and further developed to allow the Agency to continue to respond to these challenges and provide support and expertise for stakeholders across Europe.



Explaining the terms

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

Cybersecurity:

Cyber security 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 user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment⁴. 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.

Cybercrime:

Because cybercrime covers such a broad scope of criminal activities, it is difficult to produce a single definition. Whether using a computer as a tool or as a target, criminality is increasingly present in cyberspace. On the internet the time and place of the crime do not have the same significance as in the physical world. 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:

Cyber espionage is the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers⁵.

In 2012, European security researchers reported that a cyber espionage virus found on personal computers in several countries in the Middle East was designed to eavesdrop on financial transactions and perhaps disable industrial control systems. Researchers at Kaspersky Lab, a Russian IT security company in Moscow, identified the surveillance virus, dubbed Gauss, on PCs in Lebanon and other countries in the region and remark it appears to have been developed by the same team or 'factory' that built the Stuxnet and Flame computer viruses⁶.

4 <http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>

5 <http://en.wikipedia.org/wiki/Cyberwarfare>

6 <http://lexicon.ft.com/Term?term=cyber%20espionage>

7 DOD – Cyber Counterintelligence

8 <http://www.bloomberg.com/news/2012-10-12/cyberattacks-could-become-as-destructive-as-9-11-panetta.html>

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. Nowadays, the line between soldier, terrorist and criminal is often a very blurry one. With Internet technology it is possible for an individual, group or state to carry out remotely controlled, often covert, cyber-attacks on the critical infrastructures of a state. When used as a preventive mechanism, cyber counter-intelligence’s role is to identify, penetrate, or neutralize foreign operations that use cyber means as an offensive capability. This includes foreign intelligence service collection efforts, which use traditional methods to measure cyber capabilities and intentions⁷. U.S. Defence Secretary Leon Panetta went as far as saying: “A cyber-attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11. Such a destructive cyber terrorist attack could paralyze the nation.”⁸

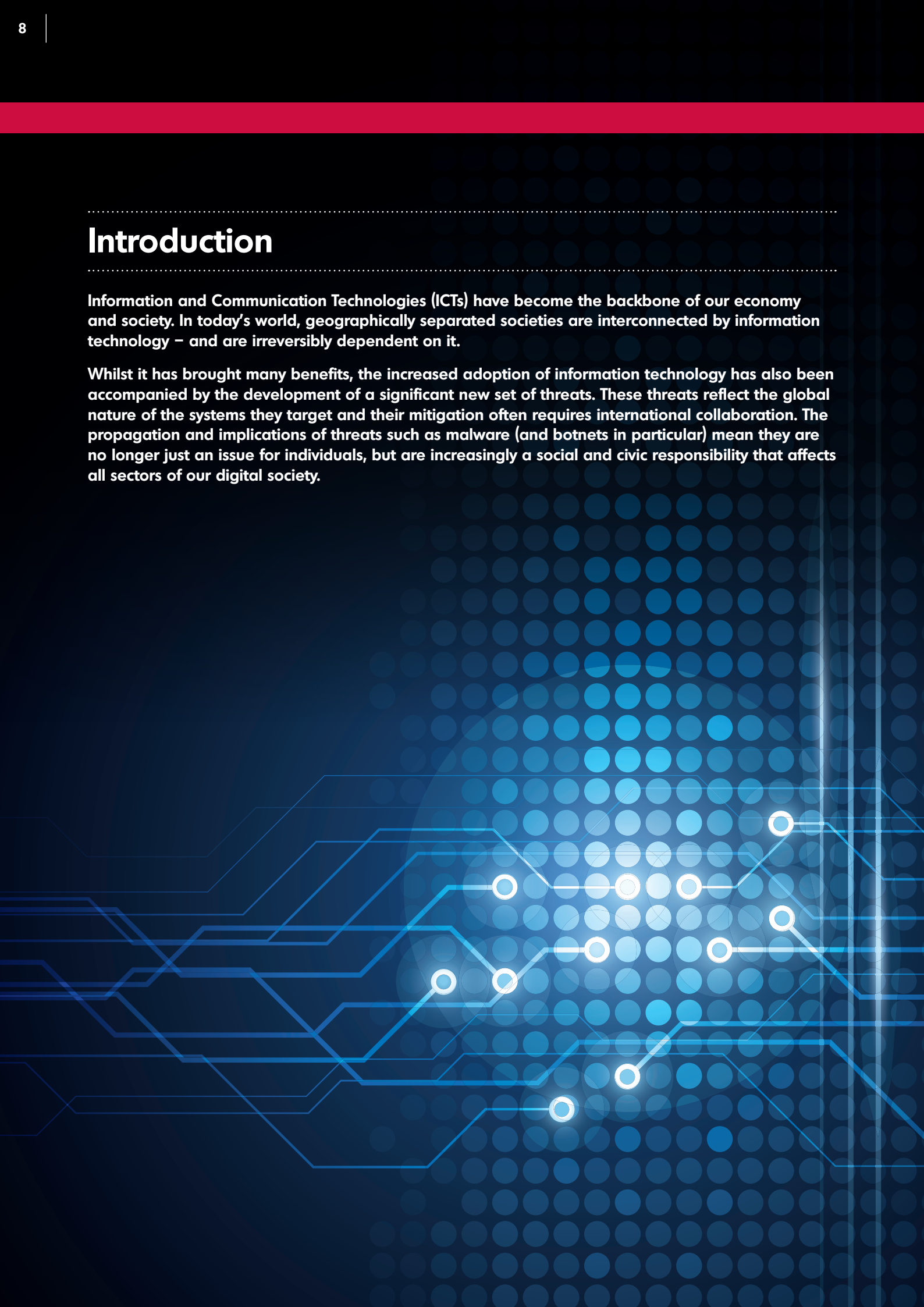
These terms are not mutually independent and there are many overlaps of scope when discussions take place, especially at a more detailed level, where similar issues and problems are discussed by many communities in both the public and private sectors. Unfortunately, information and experiences are often 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, to which our adversaries are not subject - and which they may actually benefit from if our responses are not coordinated across sectors and national borders.

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.

Whilst it has brought many benefits, the increased adoption of information technology has also been accompanied by the development of a significant new set of threats. These threats reflect the global nature of the systems they target and their mitigation often requires international collaboration. The propagation and implications of threats such as malware (and botnets in particular) mean they are no longer just an issue for individuals, but are increasingly a social and civic responsibility that affects all sectors of our digital society.



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 content⁹. 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. In this context, it is interesting to note that the *Special Eurobarometer 390 on Cyber Security*¹⁰ (published in July 2012) indicated that 29% of EU citizens do not feel confident in using the Internet for banking or purchases and 12% said they had already fallen victim to online fraud.

The EU's competitiveness and prosperity are closely connected to the safety and security of critical infrastructures; hence we need to cooperate closely in order to strive for the EU as a whole to be equipped with appropriate protection and defence mechanisms, including an overview of major cyber incidents. 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 yet, as approaches vary in different Member States and communities. Without a coordinated global strategy for combatting major incidents on the Internet, Member States could find themselves in a situation where local systems cannot function effectively because of issues that are outside their control.

The EU institutions and bodies play an important role in improving cyber security by providing support for collaboration and a policy 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 providing an objective 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
- Supporting other community actors in 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. This is already now under way with cyber incident reporting under Article 13a of the EU's Telecommunications directive¹¹, but there is scope for this to be done across more areas.

9 1 COM(2010) 245 final/2

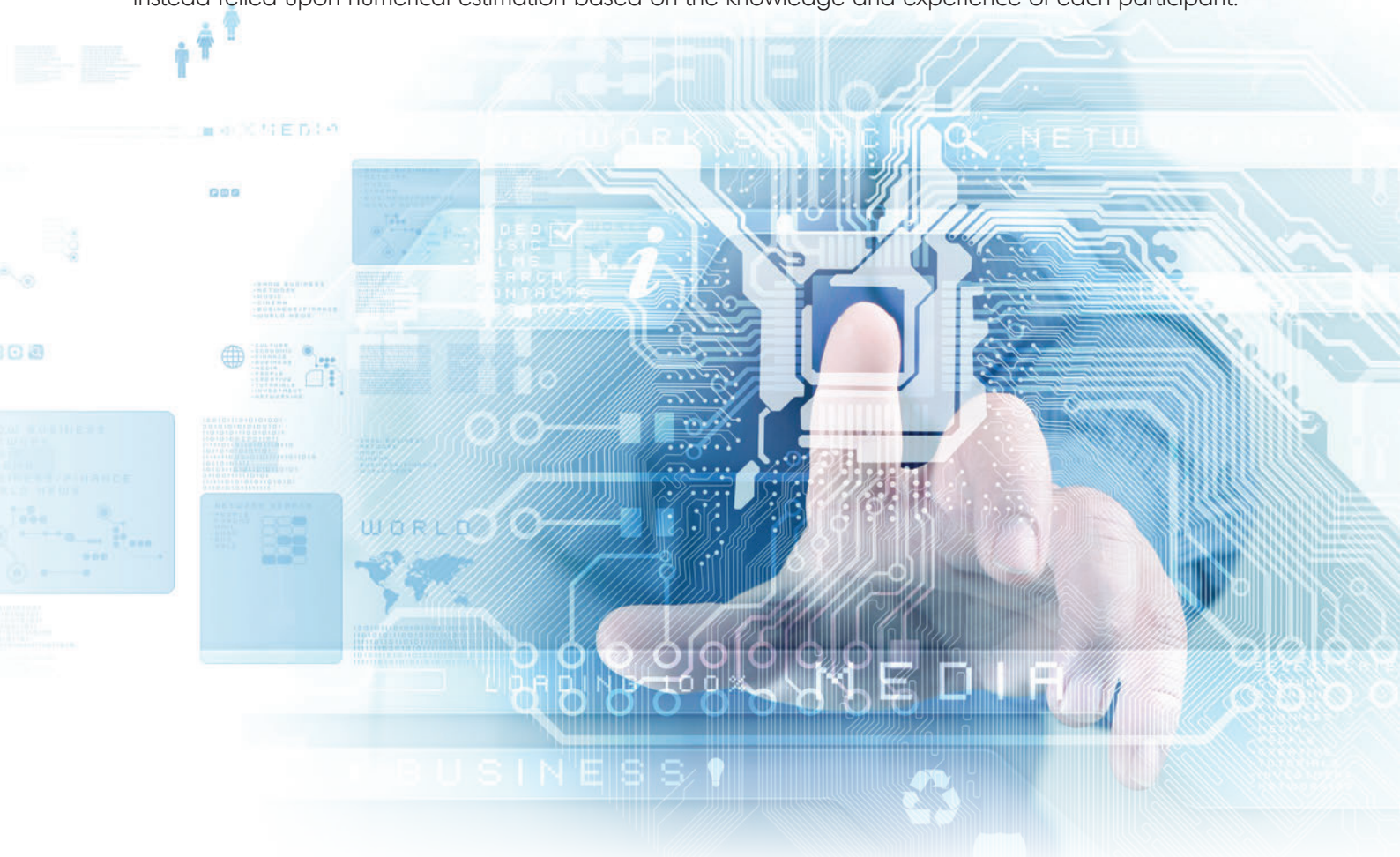
10 http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

11 <http://www.enisa.europa.eu/media/news-items/agency-initiative-to-implement-art.-13-of-telecom-package>

The Evolving Threat Landscape

While the vision of a Digital Society is compelling, robust Network and Information Security (NIS) will be needed to get there. For in the area of NIS, we face an entirely new set of challenges. New technologies and new business models are emerging at an ever faster pace, pushing existing concepts and regulations to their limits. The consumerization trend in IT, for example, renders the security perimeter blurred, whilst the convenience of being able to access both private and business data 'anywhere, anytime' will stretch our data protection concepts.

According to the Ponemon Institute's HP-commissioned **2012 Cost of Cyber Crime study**¹², the frequency of successful cyber-attacks has more than doubled over the last three years, but the annual cost to organizations has slowed dramatically in the last two years. The study is a series of individual reports covering five major markets: the US, the UK, Germany, Japan and Australia. The headline figure is the total cost of cybercrime for an analyzed sample of about 200 companies across the five countries, ranging from \$3.2 million in the UK to \$8.9 million in the US. The value of the reports, however, is not in their absolute figures, but in the comparative analysis both between the markets and over the last three years. The report itself states that, "Data collection methods did not include actual accounting information, but instead relied upon numerical estimation based on the knowledge and experience of each participant."¹³



12 <http://www.hp.com/hpinfo/newsroom/press/2012/121008a.html>

13 [http://www.infosecurity-magazine.com/view/28664/the-2012-cost-of-cyber-crime-report-says-successful-attacks-doubled-/](http://www.infosecurity-magazine.com/view/28664/the-2012-cost-of-cyber-crime-report-says-successful-attacks-doubled/)

Figure 1:
Attack distribution data for 2012¹⁴

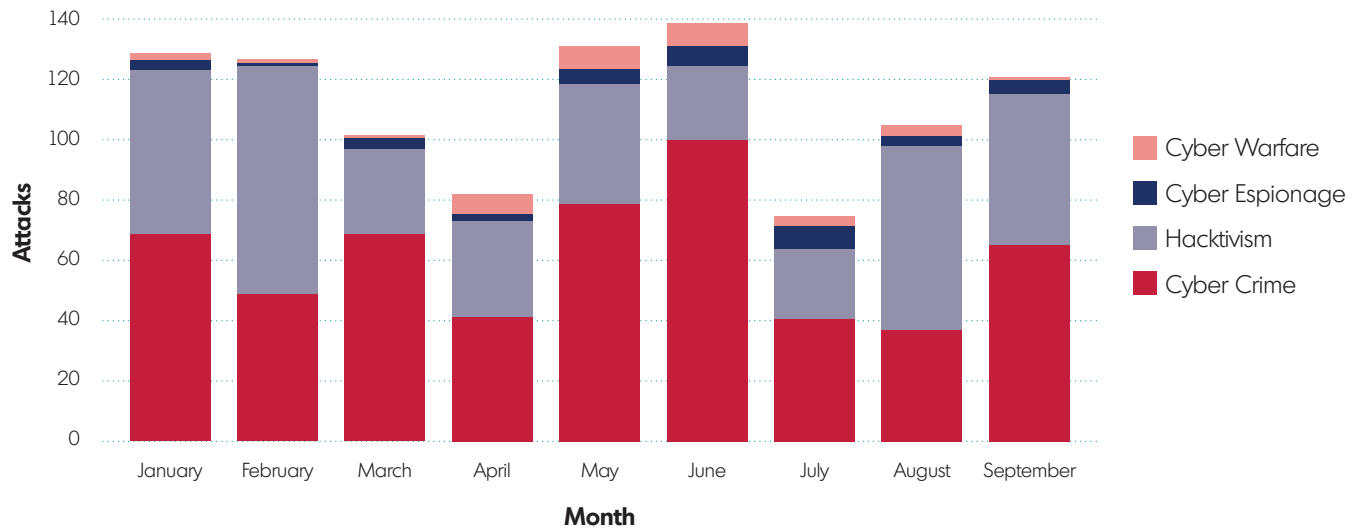


Figure 1 shows how different types of cyber-attacks have evolved throughout 2012. It is clear from this data that the majority of attacks fall into the category of cybercrime or hacktivism. Some of the more distinctive recent attacks are described below. Each of them highlights different aspects of the types of threats we are facing - and their consequences. They all illustrate the seriousness and global dimension of network and information security issues.

Operation High Roller

Cyber bank robbers attacked banks in Columbia, Germany, Italy, the Netherlands, the United Kingdom and the U.S. The research on this case, conducted jointly between McAfee and Guardian Analytics, found that the size of the attempted fraud was approximately 2 billion Euros. The Netherlands topped the list of number of successful attacks. The old adage that “criminals go where the money is” today means that “bank robbers go online”, as the Executive Director of ENISA, Professor Udo Helmbrecht stated¹⁵.

Flame malware

Flame, also known as Flamer, sKyWIper, and Skywiper, is modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system. The program is being used for targeted cyber espionage in Middle Eastern countries.

Its discovery was announced on 28th May 2012 by MAHER Center of Iranian National Computer Emergency Response Team (CERT), Kaspersky Lab and CrySyS Lab of the Budapest University of Technology and Economics. The last of these stated in its report that it “is certainly the most sophisticated malware we encountered during our practice; arguably, it is the most complex malware ever found”.¹⁶

A variant, Miniflamer is even more specialised and tightly targeted, and, as far as is known, has only been used against 10s or 100s of PCs.

14 <http://hackmageddon.com/2012-cyber-attacks-statistics-master-index/>

15 <http://www.enisa.europa.eu/media/press-releases/eu-cyber-security-agency-enisa-2012-high-roller-2012-online-bank-robberies-reveal-security-gaps>

16 [http://en.wikipedia.org/wiki/Flame_\(malware\)](http://en.wikipedia.org/wiki/Flame_(malware))

Shamoon

The virus is being used for cyber espionage in the energy sector. Its discovery was announced on 16 August 2012 by Symantec, Kaspersky Lab, and Seculert. Similarities have been highlighted by Kaspersky Lab and Seculert between Shamoon and the Flame malware.

The virus has been noted as unique for exhibiting differing behaviour from other malware cyber espionage attacks. Shamoon is capable of spreading to other computers on the network, through the exploitation of shared hard drives. Once a system is infected, the virus continues to compile a list of files from specific locations on the system, erasing and then sending information about these files back to the attacker. Finally, the virus will overwrite the master boot record of the system to prevent it from booting¹⁷. 30.000 computers were affected in Saudi Arabia's state oil company and a Qatari gas firm, as Shamoon wiped files replacing them with images of a burning American flag.

Cyber-attacks on US banks

Cyber-attacks on the biggest U.S. banks, including JP Morgan Chase & Co. and Wells Fargo & Co., have breached some of the nation's most advanced computer defences and exposed the vulnerability of its infrastructure, according to cyber security specialists tracking the assaults. The assaults were the focus of closed-door White House meetings in the following few days, and President Barack Obama's administration is circulating a draft executive order that would create a program to shield vital computer networks from cyber-attacks¹⁸.

Attacks on Swedish websites

In October 2012, several Swedish government websites were knocked offline under a DDoS (distributed denial of service) attack. Websites around the country went offline after 10am, including the Courts Administration, the Swedish Armed Forces and the Swedish Institute. The attacks came just days after police raided a Stockholm-based web hosting company, PRQ, and a video was posted on YouTube - allegedly made on behalf of the hacker group Anonymous - warning Swedish authorities of repercussions¹⁹.

17 <http://en.wikipedia.org/wiki/Shamoon>

18 <http://www.businessweek.com/news/2012-09-27/cyber-attacks-on-u-dot-s-dot-banks-expose-computer-vulnerability>

19 http://www.cbsnews.com/8301-205_162-57525278/anonymous-claims-hack-on-swedish-websites/

20 [http://en.wikipedia.org/wiki/Anonymous_\(group\)#Cyber-attacks_and_other_activities](http://en.wikipedia.org/wiki/Anonymous_(group)#Cyber-attacks_and_other_activities)

21 <http://www.notebookreview.com/default.asp?newsID=6310>

Hackers

'Hackers', such as Anonymous, have carried out cyber-attacks against a number of EU Member States' government websites. The group is also thought to be responsible for cyber-attacks on the Pentagon and the News Corp media group, and has also threatened to destroy Facebook. In late May 2012 alleged Anonymous members claimed responsibility for taking down a website about genetically modified crops. In early September 2012 they claimed responsibility for taking down GoDaddy's Domain Name Servers, affecting small businesses around the globe²⁰. The evolution of online protest in the name of "e-Democracy" is taking cyber threats to a brand new level: a prolific and potentially uncontrollable one.

Over the past year, hackers have been conducting large-scale exploits to infiltrate law enforcement agencies and major companies, and steal sensitive data "for the purposes of embarrassing or damaging" these organizations, according to Ed Skoudis, founder and chief security consultant at InGuardians²¹, a vendor-independent Information security consultancy .

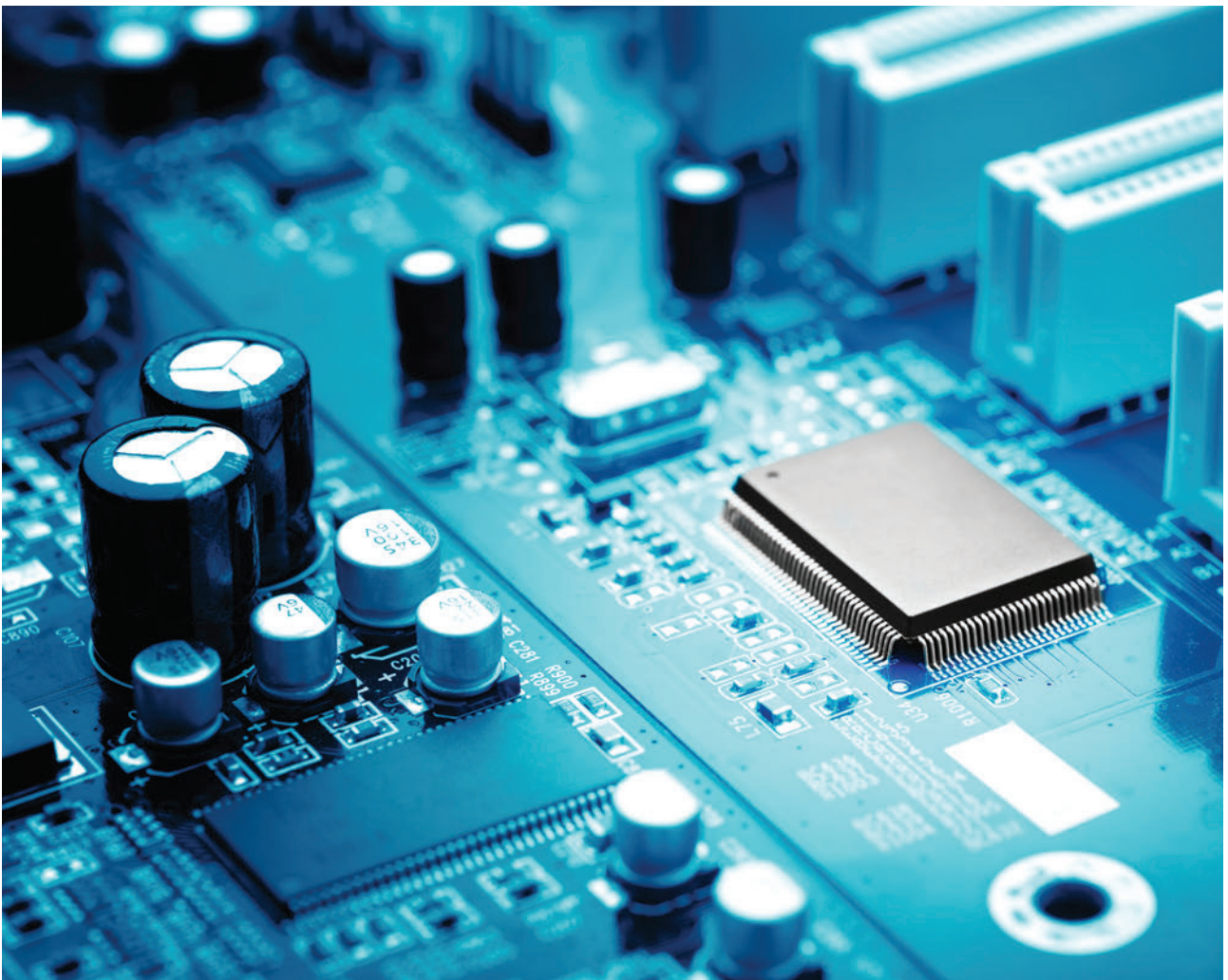
Of course, it is not only threats that are evolving. The countermeasures to tackle them have also changed. These developments include improvements to networking best practices; more focused policies, regulations and directives; increased insight into multi-sector implications of security issues and the recognition of the importance of having a global perspective on NIS. It is important to maintain and adapt these efforts to improve NIS, so as to keep pace with the continuous evolution and increasing pervasiveness of the technology itself.



Mitigating the Threats – a reality check

Despite the incidents mentioned earlier, it is essential to achieve a holistic approach to cyber security cooperation, including cybercrime, on a pan-European level. However, despite the scale of the challenges, the approach to mitigating threats remains overly fragmented. Different approaches to securing information and systems are developed independently in different European Union (EU) Member States and in different ICT communities. As a result, weaknesses in one Member State's defences can easily be used to compromise security in others. Increased cyber cooperation in the EU would ensure that the principle of the weakest link no longer applies in the future. To this end, ENISA is supporting the Commission and the Member States in elaborating an EU Cyber Security Strategy.

Although there is a significant amount of work to be done to achieve this vision of a harmonised approach to cyber security across the EU, it is clear that a lot of progress has already been made in collaborating across communities and across national boundaries.



The **Taurus Botnet Monitoring** project is a good example of cyber collaboration where both the Netherlands' High Tech Crime Unit and GOVCERT.NL cooperated to investigate and take down the Win32/Bredolab botnet. The project had three phases – (a) information gathering (on malware, servers hosting control and command), (b) investigation and (c) intervention (GOVCERT.NL helped in taking down servers). The cooperation enabled the taking down of certain parts of the botnet in 2010. Note however that some command-and-control (C&C) servers were kept alive in order to gather more data and do further analysis on it. As part of the mitigation measures, computers that had been infected with Bredolab received a popup detailing instructions on how owners could clean their systems.

This type of cooperation provides a fast and effective way to tackle threats whose exact characteristics are not known until the attack is under way. The flexibility of a cooperative approach enables counter-measures to be rapidly scaled up as attacks develop, and be prepared to tackle and prevent information and networks being jeopardised.

ENISA's role in NIS facilitating cooperation is ever more fundamental. The Agency is in a unique position within Europe to eliminate barriers to cooperation between various communities²².

Despite daily cyber-attacks launched **at the London 2012 Olympic Games**, the Olympics Technology Operations Centre was prepared and responded efficiently. When asked if London 2012 was hit by a particularly major cyber-attack, Chief Information Officer, Gerry Pennell simply replied: "Yes. And that's all I'm saying." Inside the Olympics Technology Operations Centre on the 21st floor of London's Canary Wharf, there was even a special security hotline, housed inside a glass phone booth, with a direct connection to "relevant authorities" in the event of a major attack, according to Pennell. However, while some threats were potentially serious, others were easier to defend against²³.

In 2011, ENISA established its Mobile Assistance Team (MAT) within its Technical Competence Department. The aim was to improve the effectiveness of its activities by developing the capability to mobilise teams of security experts in order to assist Member States, by providing technical assistance wherever and whenever it is required. Appropriate use of the Mobile Assistance Teams has already enabled ENISA to respond to Member States' needs in an agile manner and to increase the scalability of its activities by leveraging existing experience in the EU community. In particular, the Mobile Assistance approach has been instrumental in allowing the Agency to respond quickly and effectively to 'Article 10 Requests' (these are requests for assistance that are made directly to the Agency by the European Commission, the European Parliament or Member States). The number of Article 10 requests has grown rapidly since the formation of the MAT. At the time of writing, ENISA is working on 22 such requests thus increasing its impact by providing direct assistance on problems that are seen as important by some of its key stakeholder communities.

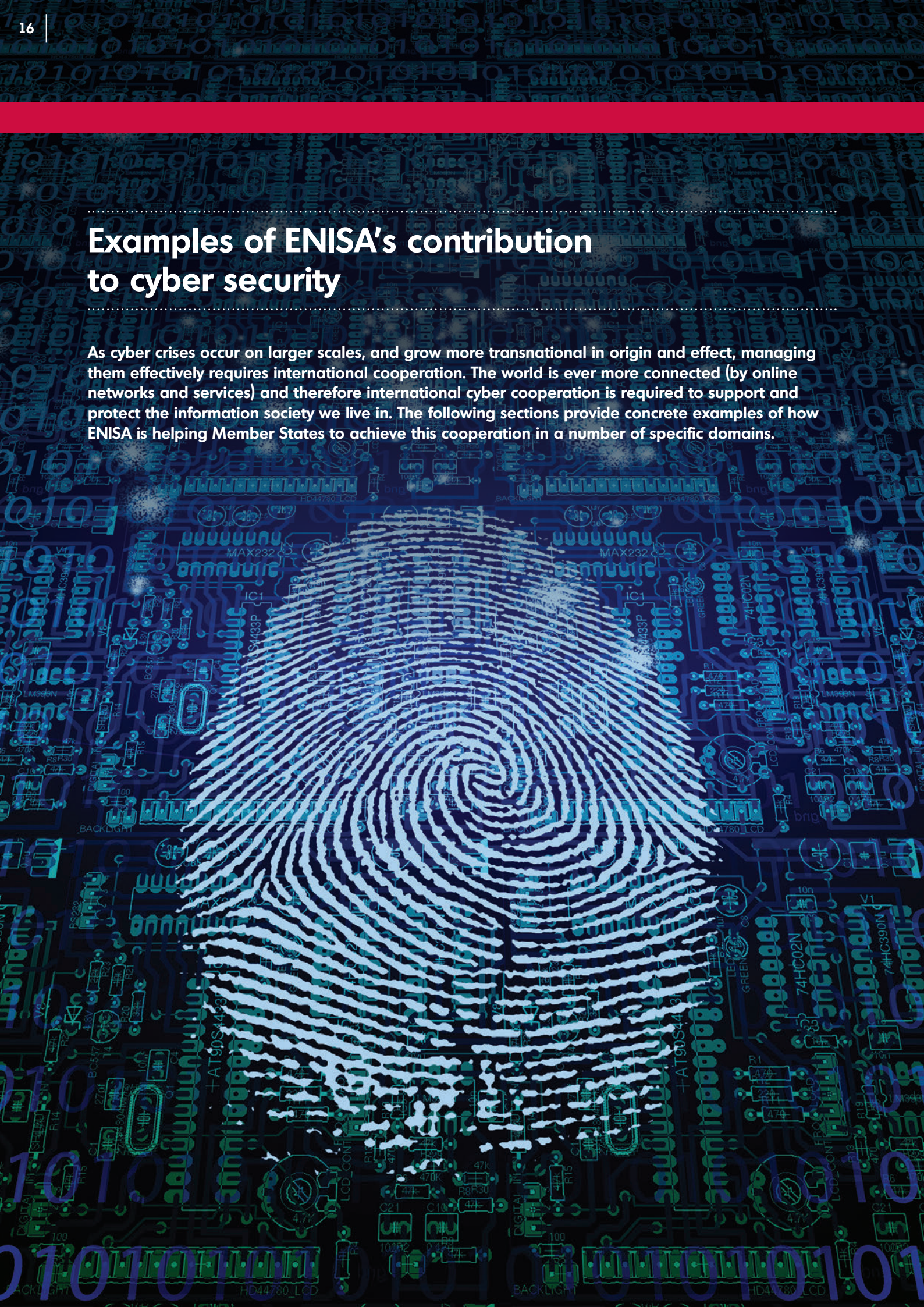
This is one of a number of organizational changes that are enabling ENISA to work more efficiently and focus its resources to best effect.

22 <http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cybercrime>

23 <http://www.computerweekly.com/news/2240168945/Cyber-attacks-launched-at-London-2012-Olympic-Games-every-day>

Examples of ENISA's contribution to cyber security

As cyber crises occur on larger scales, and grow more transnational in origin and effect, managing them effectively requires international cooperation. The world is ever more connected (by online networks and services) and therefore international cyber cooperation is required to support and protect the information society we live in. The following sections provide concrete examples of how ENISA is helping Member States to achieve this cooperation in a number of specific domains.



Cyber exercises

Cyber exercises are an important tool to enhance, improve and focus on large scale cyber crisis cooperation. Supporting EU-wide cyber security preparedness exercises is one of the main actions of the Digital Agenda for Europe. Strengthening Europe's cyber defence and combating potential online threats to essential infrastructure helps ensure that businesses and citizens feel safe and secure online. Moreover, making the best possible use of ICT could help speed up economic recovery and could lay the necessary foundations for a sustainable digital future.

ENISA has extensive experience in organising and facilitating cyber exercises for the EU Member States. This experience is used to organise pan-European and regional exercises; support the organisation of national exercises, and offer seminars to public authorities in the European Union and EFTA countries.

Cyber Atlantic 2011

The first joint cyber security stress-test exercise between the European Union and the United States

Following an EU-US commitment to foster greater efforts and cooperation on cyber security, the first joint cyber security exercise between the EU and US was held in November 2011, with the support of ENISA and the US Department of Homeland Security (DHS). Cyber Atlantic 2011 was a centralised table-top exercise, with over 60 participants from 16 EU member states and the US.

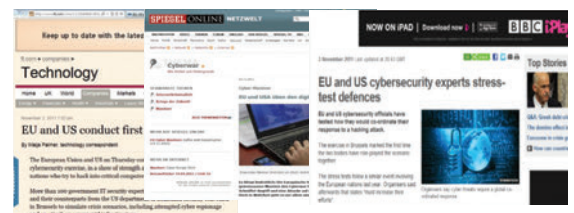
The day-long exercise simulated a series of cyber-crisis scenarios to explore how the EU and US would not only engage with one another, but also co-operate, in the event of a cyber-attack on critical international infrastructure. Two scenarios were used to explore an attack based on advanced persistent threats, where sensitive data was "ex-filtrated" from governmental systems, and the other involved a staged attack on supervisory control and data acquisition systems (SCADA) in power-generation infrastructures.



Objectives:

1. Explore and improve the way in which EU Member states would engage the US during cyber crisis management activities, notably using operating procedures for cooperation during cyber crises;
2. Explore and identify issues in order to improve the way in which the US would engage the EU Member states during their cyber crisis management activities, using the appropriate US procedures;
3. Exchange good practices on the respective approaches to international cooperation in the event of cyber crises, as a first step towards effective collaboration.

The exercise was planned by a joint EU-US group facilitated by the European Network and Information Security Agency (ENISA) and Department of Homeland Security (DHS). Cyber Atlantic 2011 was a major event that attracted the attention of the mainstream media²⁴.



24 <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-atlantic>

Cyber Europe 2012

Cyber Europe 2012, the 2nd pan-European exercise on Critical Information Infrastructure Protection (CIIP)²⁵, was a major milestone in the efforts to strengthen cyber crisis cooperation, preparedness and response across Europe. This exercise was a distributed table-top exercise, facilitated by ENISA and supported by the European Commission's in-house science service, the Joint Research Centre (JRC). In this exercise, more than 300 cyber security professionals across Europe from both the public and the private sector joined forces to counter a massive simulated cyber-attack. Compared to the inaugural 2010 exercise, Cyber Europe 2012 was considerably more ambitious in scope, scale and complexity.



Cyber Europe 2012 had three main objectives:

1. Test effectiveness and scalability of existing mechanisms, procedures and information flow for public authorities' cooperation in Europe;
2. Explore the cooperation between public and private stakeholders in Europe;
3. Identify gaps and challenges on how large scale cyber incidents could be handled more effectively in Europe.

Four countries were observing the exercise and 25 countries actively participated. Using the lessons learned from Cyber Europe 2010, the private sector (from finance, ISPs and eGovernment) took part for the first time. In the exercise, public and private participants across Europe took action at a national level. The scenario for Cyber Europe 2012 combined several technically realistic threats into one simultaneously escalating Distributed Denial of Service (DDoS) attack on online services in all participating countries. This kind of scenario would disrupt services for millions of citizens across Europe.

The complexity of the scenario allowed the creation of enough cyber incidents to challenge the several hundred public and private sector participants from throughout Europe, while at the same time triggering cooperation. By the end of the exercise, the participants had to handle more than 1000 injects (simulated cyber incidents)²⁶.

By building on and tying together activities in the EU, at both national and European level, the exercise helped to improve the resilience of Critical Information Infrastructures. As for the first pan-European cyber security exercise, the second exercise was considered to be a success by all participants.



25 <http://www.enisa.europa.eu/media/press-releases/europe-joins-forces-in-cyber-europe-2012>

26 <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-information/briefing-pack>

The Anatomy of National and International Cyber Security Exercises



In its October 2012 report, the European Network and Information Security Agency examined **85 national and international cyber-exercises between 2002 and 2012. The report²⁷ issued seven recommendations:**

1. Establish a more integrated global cyber exercise community;
2. Ensure exchange of good practices on cyber-exercises, including public–private cooperation;
3. Support development of exercise management tools for better exercise planning, execution and evaluation;
4. Conduct more complex cyber-exercises at inter-sectorial, international and European levels;
5. Exercises should be included in the lifecycle of national cyber crisis contingency plans;
6. Promote good practices for national exercises, and initiate a step-by-step methodology for cross-border cyber-exercises;
7. Develop feedback mechanisms.

²⁷ <http://www.enisa.europa.eu/media/press-releases/the-anatomy-of-national-and-international-cyber-security-exercises-new-report-by-the-eu-cyber-security-agency-enisa>

Regional cyber security exercises

In addition to this work, ENISA also organised two regional cyber security exercises in 2012. These were held to familiarise participants with cross-border cooperation procedures and mechanisms for dealing with large-scale cyber crises in Europe. Countries that took part included: Cyprus, Estonia, Greece, Malta and Iceland (first exercise); and Belgium, Denmark, Ireland, Italy, the Netherlands, Romania and Spain (second exercise).

ENISA's experience in developing and facilitating exercises allows the Agency to develop complex, highly realistic scenarios that provide an effective test of cooperation mechanisms. In one recent exercise, the players had handled more than 1000 cyber incidents²⁸.



28 <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-information/briefing-pack/ce2012-information-about-the-scenario>

Supporting the CERT Community

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 continues to collaborate with Europol, for example by organising joint workshops for CERT and Law Enforcement Agencies' representatives from Member States.

ENISA has published an interactive CERTs map and Inventory of CERTs activities in Europe, containing publicly listed teams and co-operation, support and standardisation activities. The Inventory's tabulated format shows Europe's CERTs by sector for each country, while the map provides filtering capabilities for all CERT teams in the wider EU geographical region. This now includes 195 CERT teams, 22 more than when the inventory was last updated in spring 2012.

An extra feature of the map is the inclusion of the General CERT Report and the National Governmental CERT Report, which provide information on the countries' CERT teams with the push of a button.

The Inventory and map are available online at <https://www.enisa.europa.eu/activities/cert/background/inv> and its subpages.

CERT-EU

Following preparatory work in 2011, in September 2012, the EU Institutions have set up a permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies. The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, and Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the Member States and beyond as well as with specialised IT security companies. ENISA was closely involved in the CERT-EU pre-configuration team, with the secondment of a senior staff member full time to Brussels to work in the project team.

CERT-EU will gradually extend its services, on the basis of the requirements of its constituency and taking into account the available competencies, resources and partnerships.

The Digital Agenda also calls on all Member States to establish their own CERTs, paving the way to an EU-wide network of national and governmental Computer Emergency Response Teams by 2012²⁹ (see IP/11/395).

29 http://cert.europa.eu/cert/plainedition/en/cert_about.html



7th CERT workshop

Organised by ENISA, the 7th CERT workshop was hosted at Europol Headquarters in October 2012. The purpose of this annual event is to improve cooperation between law enforcement and CERTs in cyber security- related crime. It brought together national and international representatives from both the CERTs and the law enforcement communities. These events are continuing on an annual basis, being hosted alternately at Europol and ENISA³⁰.

"Be Aware, Be Secure": the first European Cyber Security Month:

**BE AWARE,
BE SECURE.**

Mobilizing awareness amongst citizens of how to be secure online is an important aspect of cyber security. Drawing on international experiences, for the first time a pilot for a European Month of Cyber Security was held in October 2012. The Czech Republic, Luxembourg, Norway, Romania, Slovenia, Spain, Portugal, and the United Kingdom joined forces in the pilot, and organised various activities and events to raise awareness of cyber security.

Activities included TV and radio advertisements; social media campaigns and quizzes with prizes; news articles; conferences and student fairs. The campaign increased citizen's confidence in the security of the Internet, helping to reduce the number of cyber incidents and breaches. In the end, this is vital for the success of the digital economy in Europe.

Vice President and Commissioner for the Digital Agenda, Neelie Kroes commented:

"We all have a stake in keeping the Internet safe. Whether you are a parent, a business owner, or just someone who loves their smartphone – the same principles apply. Be aware, use common sense. I am pleased that so many are supporting European Cyber Security Month – a great way to present these issues to the general public in a fun and engaging way."³¹

30 <http://www.enisa.europa.eu/media/news-items/focus-on-the-fight-against-cybercrime-7th-annual-cert-part-ii-workshop>

31 <http://www.enisa.europa.eu/media/press-releases/the-first-european-cyber-security-month-starts-today-across-europe-be-aware-be-secure>

Cyber crisis cooperation conference:

In June 2012, ENISA organised the first international conference on cyber crisis cooperation. This conference focused on cyber exercises as part of an ongoing effort to enhance network and information security and cyber crisis cooperation across the European Union.

The objectives of the first international conference on cyber crisis cooperation were:

- to exchange good practices in the field of international cyber crisis cooperation, specifically focusing on cyber exercises
- to identify gaps and challenges in the field of international cyber crisis cooperation and in particular on cyber exercises³².



Workplace IT: The “Bring Your Own Device” trend

In today's high-pressure work environment, mobility and networked knowledge are two key factors shaping the future of professional life. These factors, combined with the consumerization of all kinds of IT components, make it imperative to consider the role of private IT in corporate IT strategies. The “Bring Your Own Device” option, where staff use their personal computers to perform tasks in the workplace or elsewhere, can bring a wide range of potential benefits. Among the opportunities presented by this consumerization of IT are:

- employer and staff flexibility on hours and work locations
- savings through lower infrastructure costs
- increased productivity and staff satisfaction through developing their own skills
- lower infrastructure costs from moving to flexible IT solutions, such as cloud computing

But with the potential benefits come risks, which must be foreseen, with proper policies and mitigation strategies. Among the top risks are:

- confidential information being lost, stolen or made public, whether through poor IT security on personal devices, or through the theft of mobile devices or computers
- potential issues over data ownership, unauthorized sharing, and legal governance over devices, programs and content
- increased opportunities for cyber-criminals to target corporate data

32 <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-exercises/cyber-exercise-conference>

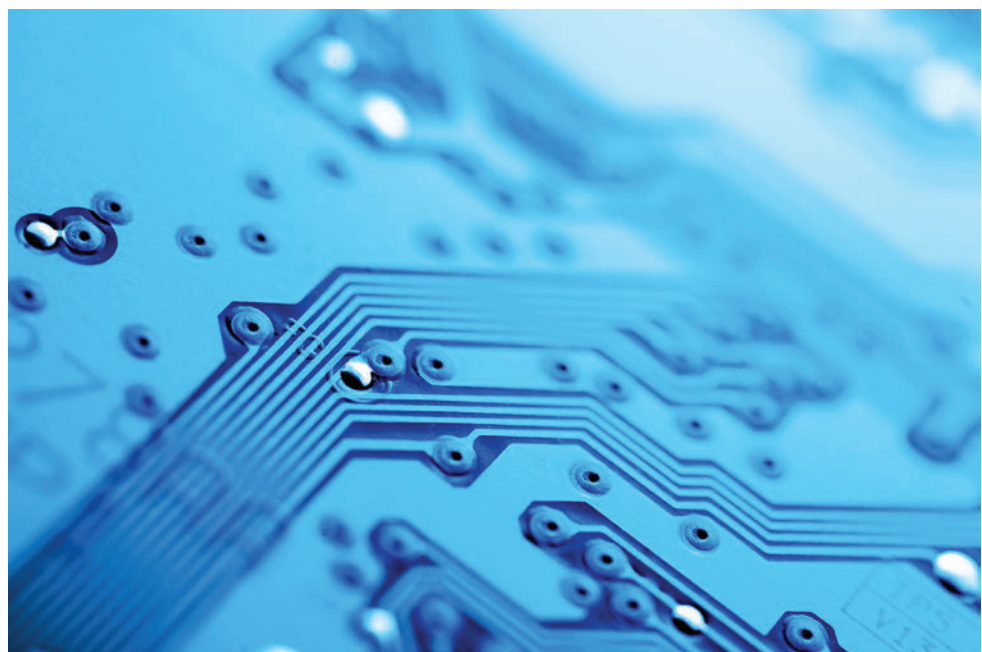
Improving Security Breach Notification: Article 13a

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 Electronic Communications Regulatory Framework Directive³³. 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, ENISA is also working on the broader concept. In particular, the Agency is 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.

For the first time in the EU, in spring 2012 national reports about security incidents were reported to ENISA and the European Commission, under Article 13a of the Framework Directive (2009/140/EC)³⁴ which is a new article in the EU legal framework for electronic communications. In the first ever analysis of this information, ENISA has analysed the 51 incident reports of severe outages of electronic communication networks or services.

ENISA will publish a similar overview and analysis, yearly, following subsequent rounds of annual summary reporting by the National Regulatory Authorities (NRAs) in the EU Member States. The next report will be published in spring 2013, and will summarize and analyse the incidents that occurred in 2012.



33 Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)

34 <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/article-13a-annual-report-2012?searchterm=Article+13>



Liaising with the EU Cybercrime Centre (EC3)

In response to the European Commission's communication "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre", the Council of the EU have endorsed the establishment of a new European Cybercrime Centre (EC3) at Europol in The Hague.

The Centre will become the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of cyber-attacks. It will support Member States and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners.

ENISA is supporting the cybercrime centre's establishment, as called for in the EU Internal Security Strategy, and recognises the importance of setting up a structured approach to information exchange between this centre and ENISA. The Agency is represented in the centre's Programme Board, and is helping the centre set up a dialogue with the CERT community and is providing the centre with access to its other stakeholder communities as needed.

In October 2012 Europol hosted the second meeting of the new European Cybercrime Centre (EC3) Programme Board. In addition to ENISA, the board has representation from CEPOL, the EU Cybercrime Task Force, CIRCAMP, Cyber EMPACT, Council Secretariat, EEAS and EC3 staff³⁵.

Cooperation between the Cybercrime Centre and ENISA is initially focusing on exchanging information 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. Whilst the law enforcement agencies deal with response, ENISA tackles prevention.

35 <https://www.europol.europa.eu/ec3>

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 needs to be close cooperation with international partners to prevent and to respond to cyber incidents.

At the EU-US summit 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 collaboration³⁶. ENISA contributes 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.

The European Neighbourhood Policy

The need for greater security, including cyber security, is recognised in the EU's Neighbourhood Policy (ENP³⁷), which is seeking to reinforce relations with neighbouring countries to the east and south to promote prosperity, stability and security at its borders. The ENP refers to the overall European Security Strategy³⁸, which acknowledges that;

"...attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon,"

and;

"More work is required in this area, to explore a comprehensive EU approach, raise awareness and enhance international co-operation."

At present, 16 partners are addressed by the ENP: Algeria, Armenia, Azerbaijan, Belarus, Egypt, Georgia, Israel, Jordan, Lebanon, Libya, the Republic of Moldova, Morocco, the occupied Palestinian territories, Syria, Tunisia and Ukraine. The ENP provides the EU with the means to deepen bilateral relations with these countries. The policy is based upon a mutual commitment to common values: democracy and human rights, rule of law, good governance, market economy principles and sustainable development³⁹.

36 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm

37 http://eeas.europa.eu/enp/index_en.htm

38 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf

39 http://eeas.europa.eu/enp/index_en.htm

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.



Cyber cooperation 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 key 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.

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 is an interface between different operational communities in general. The objective is to ensure that the overall approach to improving information security throughout Europe is both coherent and efficient, by identifying synergies and eliminating duplication of tasks.



ENISA's role – looking ahead

The era of online security is entering a brand new chapter with the Proposal for a European Strategy for Internet Security⁴⁰ under the remit of Commissioners Cécilia Malmström, Neelie Kroes and High Representative Cathy Ashton. The political capital invested in this strategy is fundamental to its success if we are to see a stable and safe progression into the digital future.

ENISA was created 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”⁴¹ as set out in the founding regulation of the Agency.

Since then, the challenges related to NIS have developed alongside technology and market developments.

This is why a significant part of the Agency's work is concerned with protecting our infrastructure and applications, and ensuring that we are prepared for future 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.

At the request of the Commission, ENISA has expanded its work in cyber exercises across Member States (Cyber Europe 2010 and 2012) and facilitated an exercise with the Department of Homeland security in the US (Cyber Atlantic 2011). The global scale of cyber security is challenged by the utter lack of online borders, and these exercises are vital to assess and enhance European and worldwide cyber-crisis preparedness..

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. In this capacity, the Agency plays an important role in bridging the gap between policy and operational requirements.

ENISA supports 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. The Agency also facilitates dialogue on NIS 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.

The Agency is working hard in the relevant fields of information security management in order to be in the unique position of brokering the way forward.

The decision has been taken to modernize and further develop ENISA as a professional platform and a proficient body which serves as the EU's center of expertise in NIS. The future sees a new mandate for the Agency, which reflects the need for work to progress in the constantly evolving NIS environment. This will give the Agency more flexibility to interact with and respond to the needs of stakeholders across Europe.

40 http://ec.europa.eu/governance/impact/planned_ia/docs/2012_info_003_european_internet_security_strategy_en.pdf

41 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML>

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 protect and strengthen the true benefits.

EU cyber cooperation is at a crucial stage of its development and alignment. By helping the public and private sectors to develop common strategies and support each other in each Member State, we can reach a level of common policies and best practices that will put the EU in a position to be emulated worldwide. The global cyber map is an ever changing one, and its scenarios are advancing at a relentlessly fast pace.

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.⁴²”

ENISA already plays an important role in supporting the EU institutions and the Member States in securing the ICT infrastructure, focusing on the global challenges ahead to align their approaches to targeted EU cyber matters. A proactive approach to building cyber cooperation in the cross-border communities will bring great benefits both in terms of the effectiveness of its common strategies and efficiency in the use of its evolving assets.

The future of NIS will always be ahead of us, and cyber security is an issue that is here to stay.

In this new inter-dependent world we must act as one, and develop a cohesive online ethos: the next chapters of cyber security depend on it. This is why ENISA’s pivotal role is to be strengthened, so it may continue to provide support and expertise whilst responding to these challenging digital changes, as foreseen in the proposal to modernise the Agency, which is currently under discussion by the EU’s Council of Ministers and the European Parliament.⁴³

It is imperative that the Internet is defended as a safe arena for commercial, governmental and cultural and leisure uses. As cyberspace becomes an increasingly integral part of our everyday world, more and more of our critical infrastructures will depend on it, and be at risk if cyberspace is not made secure. Therefore all the efforts and strategies towards securing Europe’s cyber cooperation must be coherent, consistent and united.

42 COM(2010) 673 final p. 16

43 (COM(2010)521)

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



Follow ENISA on

 [Facebook](#)  [Twitter](#)  [LinkedIn](#)  [YouTube](#) and  [RSS feeds](#)



P.O. Box 1309, 71001 Heraklion, Greece

www.enisa.europa.eu