European and International Cooperation on Incident Response

Udo Helmbrecht
Executive Director
ENISA

Telecom Ministerial Conference on CIIP
Balatonfüred, Hungary, 15th April 2011

Check against delivery.

Introduction

Ladies and Gentlemen,
Let me please begin by thanking our hosts today for giving me the opportunity to underline the importance of international cooperation for effective incident response and protection of our critical information infrastructures.

Information and communication technologies have become the backbone of our economy and society. On a global scale, societies are interconnected by information technology - and are irreversibly dependent on it. Unfortunately global threats have also become possible and very real.

ENISA is working to secure Europe's information society. A great part of this is to protect our critical information infrastructure and the applications that run on top of it[1] and in parallel we have to reinforce incident response. Only then can growth and prosperity continue to be possible in a competition-oriented, globalised world.

Security and safety are basic needs. The state guarantees us territorial security. There are safety standards in road traffic or in construction projects which protect our physical safety and our property. In the information society we are concerned with information and cyber security. We talk of IT threats and vulnerabilities, IT systems and infrastructure. On a grander scale, we discuss issues such as cybercrime, cyber espionage and cyber warfare.

The definitions of these terms need to be further refined and often depend on the author and the context. If we talk about war we go to the military and get military solutions; if the threats are criminal in nature then we go to the police for solutions; if it is espionage the intelligence community handles it. How we talk about the subject of IT security, and how the headlines on this look, affect which solutions we get. The people who abuse the Internet don't care about this. If malware attacks IT-systems it is sometimes difficult to understand who is behind the attacks. This illustrates an important point: we have an opportunity to bring communities together and to harmonise the different approaches that are being taken to deal with different aspects. Currently, we can establish the following classification:

Cybercrime: Criminality is on a new scale on the internet. In conventional crime the perpetrator has to be at the scene of the crime. In a bank robbery he has to enter the bank. On the internet the time and place of the crime are not dependent on each other.

[1] An insecure application running on secure infrastructure is still insecure. A secure application running on insecure infrastructure can still be secure as long as we can ensure availability and performance.

If I am *phishing*, in theory 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 state A to arrest a criminal in state B.

Therefore organised crime can scale up its illegal operations.

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

However, whereas in the past the spy had to run the risk of having his cover blown at the crime scene, today he can spy unseen from afar using for example Trojan horses[2].

Cyber warfare: This is a new field of asymmetrical warfare. In the past troops from opposing countries confronted each other. The Geneva Convention[3], for example, describes rules for the protection of people who do not take part in the fighting.

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

With internet technology it is possible to carry out attacks on infrastructures, so-called critical infrastructures[4], of a state as an individual or group with or without government tolerance. Therefore the line between soldier, terrorist and criminal becomes blurred.

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

The Treaty of Lisbon paves the way for increased dialogue between communities and, as long as we approach this dialogue in a cautious way in close collaboration with the Member States, we should be able to achieve an overall more level playing

[2] http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29
[3] http://en.wikipedia.org/wiki/Geneva_convention
[4] http://en.wikipedia.org/wiki/Critical_infrastructure

field and hence a greater level of cyber security for all communities. It is worth noting that those who seek to cause damage are not restricted by artificial barriers to communication – it is critically important that the communities that are responsible for keeping cyberspace safe benefit from the same freedom of dialogue and information flow.

ENISA's role is to facilitate dialogue between different communities for all aspects related to Network and Information Security and we can support the Commission and the Member States in promoting and maintaining this dialogue. In this way, we can contribute to a high level of network and information security and thus to securing Europe's information society "for the benefit of citizens, consumers, business and public sector organizations in the European Union, thus contributing to the smooth functioning of the internal market,"[5] as is our task according to the regulation establishing the Agency.

The development of information technology in the past 40 years has been rapid. So have the threats against it. The first malicious programs had already appeared in the early 1970s: "Creeper"[6] was one of the first viruses. In 1971 it "infected" the DEC[7] computer belonging to Arpanet (Advanced Research Projects Agency Network of the American Defence Ministry) and on the infected computers displayed the words "I am the Creeper: CATCH ME IF YOU CAN." In May 2000 the "I LOVE YOU" worm attracted headlines across the world. It was an e-mail with "I LOVE YOU" in the subject line and spread explosively. The worm was attached to this e-mail. Anyone who received this e-mail from someone they knew, and opened it trustingly with a click of the mouse, unknowingly and automatically activated the malicious program[8]. The worm caused damage amounting to billions of dollars worldwide. The motivation for creating the virus was possibly to impress a new girlfriend[9].

However, we are now faced with much more complex attacks with far more sinister motives. For example the *stuxnet*[10] malware which showed that even control systems, e.g. in manufacturing plants or power stations can be the target of attacks.

---

[5] Regulation (EC) No 446/2004 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[6] http://en.wikipedia.org/wiki/Creeper_virus Creeper is a comic character designed by Steve Ditko (Spiderman, among others). The words "I am the Creeper – catch me if you can" appeared on the screens of infected computers.

[7] DEC = Digital Equipment Corporation. It was taken over by Compaq in 1998 and since 2002 has belonged to Hewlett-Packard. http://en.wikipedia.org/wiki/Digital_Equipment_Corporation

[8] http://en.wikipedia.org/wiki/I_Love_YOu_virus On infected computers the worm wiped all files with certain file extensions and automatically forwarded them. Because of the way in which it spread exponentially, in the first few hours it overloaded many mail servers.

[9] http://www.theregister.co.uk/2005/05/11/love_bug_author/

[10] It is speculated that *stuxnet* was written with the aim of sabotaging the control system of a uranium enrichment plant in Iran. http://en.wikipedia.org/wiki/Stuxnet

It is noticeable in this case that the virus was specially written for the SCADA[11] systems used there. This requires special knowledge of the control systems. Due to the complexity of these systems a great deal of money has to be invested in hardware and software resources with a criminal motive to develop a virus of this kind and place it in a targeted setting.

Only last month RSA[12] issued a statement that there has been an attack against their infrastructure which they categorise as an Advanced Persistent Threat. This means that for some time they have been under a sophisticated attack which seems to have had the purpose of extracting specific information on their SecurID two-factor authentication products.

Even if we agree on definitions, the following examples show that the distinctions are hazy. In 2007, servers of the Estonian government were attacked, i.e. were paralysed by Distributed Denial-of-Service-Attack[13] (DDoS) which allegedly came from computers in Russia. The background to this was that the Estonian government had removed a memorial from the centre of the city which had led to violent protests from the Russian population living in Estonia. In 2008, Russia was presumed to have carried out DDoS attacks on the websites of the Georgian government. Many Georgian servers fell under foreign control and websites of the Georgian authorities were said to have been partly blocked. Estonia in 2007[14] and the Georgian conflict in 2008[15] are still not cyber warfare but they do show the potential for possible future conflicts.

Given the global nature of information and communications technology, and the growing and ever more sophisticated forms of cyber security threats, international coordination and appropriate networks focusing on foreign and security policy aspects are indispensable. This includes cooperation throughout Europe as well as internationally in both the public and private sector.

We have to conduct a global social debate and find a consensus about a global internet society. It is not just about what we in Europe would like. The internet does not end at our borders. It is about what is achievable worldwide! Protectionism and national power only guarantee limited influence. In the real world political power and personal dealings are territorially limited. Legal systems and therefore security for the citizens were and still are state-specific today. Empires were indeed able to extend their spheres of influence but journeys, including military troop movements and communications, take time. With the options offered by telecommunications, towards

[11] http://en.wikipedia.org/wiki/SCADA
[12] http://www.rsa.com/node.aspx?id=3872
[13] http://en.wikipedia.org/wiki/Denial-of-service_attack
[14] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[15] http://en.wikipedia.org/wiki/Georgia_2008_war

the end of last century and particularly through mobile communications, we can communicate at the same time – and attack quickly and from afar.

With the internet a new virtual world has come about in which in particular there are

1. no national borders
2. no uniform legal system
3. a new currency: personal data

The newly released cyber security strategies[16] from France, Germany and the Netherlands share several points which are of interest to this session. For example, that the types of attacks we are facing are often cross-border. And also that it is difficult to determine both the cause and the source of attacks and disruptions. That is, to track back and find the perpetrator. Other common themes cover how to better prepare for and respond to attacks and disruptions, namely that there is a need for increasing international cooperation as well as between the public and private sector. The strategies recognise that ICT is of ever increasing importance for our society and therefore we need to protect our critical information infrastructure (and the applications that run on top of it) and reinforce incident response. This is also reflected in the national security strategy of the UK, which will release a cyber-security strategy in the spring of this year[17].

ENISA – Securing Europe's Information Society

The European Network and Information Security Agency (ENISA) is an EU agency created to improve the functioning of the internal market by ensuring that network and information security is leveraged as a competitive advantage, rather than introducing barriers to further development. Though this session is about incident response, ENISA actually operates in the sphere of prevention. We do this as an advisory body to support the European Member States and the European institutions on network and information security. We also facilitate the sharing of experiences and good practices between the European institutions, the Member States and private business and industry actors.

We welcome the communications and initiatives from the Commission to improve incident response, CIIP and the overall level of information security in Europe. As the recent communication on Critical Information Infrastructure Protection shows, we have, on a pan-European level, already made several important first steps to improve our cyber security. ENISA is playing a key role in facilitating much of this activity, and will continue to do so. Hopefully in a strengthened role from the new mandate, as the communication recognises that "strengthening and modernising

[16] http://www.enisa.europa.eu/media/news-items/cyber-security-strategies-of-de-nl-presented
[17] http://www.cabinetoffice.gov.uk/sites/default/files/resources/Factsheet18-Cyber-Security.pdf

ENISA will help the EU, Member States and private stakeholders develop their capabilities and preparedness to prevent, detect and respond to cyber security challenges."[18]

As is also evident in the communication, at ENISA, we are currently concentrating much of our effort on critical infrastructure protection and the strengthening of the CERT[19] community in Europe. We are, however, also working with the public and private sectors to correctly secure new technologies and business models such as those arising from the adoption of cloud computing.

Cooperation and communication are key to ensuring a successful response to an eventual cyber attack or other large-scale disruption of ICT systems. This needs to be organised at a global level to be able to fight and mitigate security threats which cut across borders and legal jurisdictions effectively. Ideally, this should ensure that the local response to a global issue will be optimal.

In other words, most Member States are best positioned to defend their own infrastructures. However, in a global networked environment, there will only be an optimal response if issues that transcend national boundaries are managed and controlled correctly. Without a coordinated global approach to major incidents on the Internet, Member States could find themselves in a situation where local systems cannot function correctly due to issues that are outside their control.

Improving the capability for dealing with cyber attacks is part of the objectives of the EU Internal Security Strategy[20]. ENISA acknowledges the importance of the fight against cybercrime as well as the need for a strong collaboration between CERTs and law enforcement. ENISA's role is not operational, but rather it acts as a facilitator and information broker for CERTs/CSIRTs. As an EU expert body, it must stay in touch with all the CERT/CSIRT communities – in Europe and beyond. Since its inception, ENISA has sought to foster a good working relationship with relevant communities in both areas. We will continue to work together with the CERT community as well as Law and Enforcement agencies to assist CERTs in their efforts against cybercrime and to work for better protection and resilience of ICT in Europe.

The need for international cooperation

Addressing threats and strengthening security in the digital society is a shared responsibility – of individuals as much as of private and public bodies, both at home and globally. A good example of an initiative to build bridges between the public and private sector is the EP3R (European Public-Private Partnership for Resilience). Since

[18] COM(2011) 163 final
[19] Computer Emergency Response Team
[20] Action 3 of objective 3 is entitled 'Improving capability for dealing with cyber attacks'

2009 ENISA has facilitated and supported the activities of the working groups in the EP3R on security and resilience objectives, baseline requirements, as well as good policy practices and measures.

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

At the EU-US summit[21] in November, held in Lisbon, it was agreed to set up a working group on cyber security and cybercrime to evaluate and coordinate opportunities for enhanced collaboration. One of the areas which this working group should focus on is cyber incident management to enhance collaboration between national and governmental computer security incident response teams in Europe and the US. Cyber security exercises, which could include regional exercises and a possible synchronized trans-continental exercise in 2012/2013, might also be a useful way of evaluating incident management processes.

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 respond to the most important risks.

On the one hand we are increasingly aware of how sensitive and how vulnerable to attack our IT infrastructures are and on the other hand we lack adequate information by which to be able to recognise and react to dangers in due time.

Similarly, poor information exchange mechanisms are likely to result in a duplication of effort and a slower learning curve for implementing 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 recent cyber security exercise, involving all 27 Member States and facilitated by ENISA, was the

[21] MEMO/10/597 http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/597

exchange of experience at the national level on preparedness exercises. Later, I will return to what we can learn from the exercise Cyber Europe 2010.

CERTs in Europe

In its Communication "The EU Internal Strategy in Action: Five steps towards a more secure Europe"[22] of September 2010 the European Commission stresses ENISA's role in improving Member States' capabilities for dealing with cyber-attacks. An emphasis is put on the establishment "... within existing structures (of a) cybercrime centre, .." which should "... establish cooperation with ENISA and ... a network of national / governmental CERTs."

Since 2005 ENISA has run a programme dedicated to reinforcing national and governmental CERTs. The goals of this programme are:

- The proliferation of CERTs in Europe in general.
- To support the EU Member States in establishing and developing their national and governmental CERTs according to an agreed baseline set of capabilities.
- To generally support and reinforce CERT operation and cooperation by making available good practice in cooperation with national and governmental CERTs.

We also seek to

- reinforce cooperation by analysing barriers for cross-border cooperation and proposing measures to tackle them.
- support and facilitate the relationship and cooperation between CERTs and other crucial stakeholders like law enforcemen.t
- develop and deploy further the activities around information sharing and alerting of citizens in the Member States, such as the European Information Sharing and Alert System (EISAS)[23].

The ultimate goal of this activity is to help CERTs to improve the effectiveness and the efficiency of their response mechanisms, particularly where cross-border incidents are concerned. More recently, ENISA is aiming to assist Member States in leveraging the CERT community in order to make the fight against cybercrime more effective.

[22] http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf
[23] http://www.enisa.europa.eu/act/cert/other-work/eisas_folder

CERT for EU institutions

The Digital Agenda for Europe[24] is a flagship initiative under the EU 2020 Strategy[25]. Key Action 6 of the Agenda is to: "Present in 2010 measures aimed at a reinforced and high level Network and Information Security Policy, including […] measures allowing faster reactions in the event of cyber-attacks, including a CERT for the EU institutions."

In August 2010, European Commission Vice-Presidents Neelie Kroes and Maroš Šefčovič established a "Rat der IT Weisen" which I was a part of[26]. We were asked to provide the Commission and the EU institutions with advice regarding the establishment of a CERT for EU institutions.

As for any other public administrations around the world, the level of cyber threat for the European institutions is very high and multiple incidents have already occurred.

Certain organisations, both inside and outside the EU, would undoubtedly detect such an attack (as this is the case for current attacks against the EU institutions). The sooner they would have the tools to warn EU institutions about the attack, the quicker EU institutions could react and the lower the damage would be. But in such a case, a first obstacle to a quick reaction would the absence of a single and known point of contact within the EU institutions for all that concerns their network and information security.

Only last month we were faced with headlines in the world's largest media, telling us about a serious attack on EU bodies.[27] Another recent and well publicised attack is the theft of close to 30 million euro worth of emissions allowances from the national registries in the EU Emission Trading Scheme. [28] We have gathered publicly available information about the attacks and spoken to a major victim of the attacks. We have analysed the causes of the attacks and the vulnerabilities in the systems, including systemic vulnerabilities. This showed for example, that contact details of traders are published and phishing sites are still online over a year after an initial series of phishing attacks and there are no identity checks on account holders, so allowing effectively anonymous accounts. This was a cross-border attack with serious financial and operable impact. We believe there remains a serious threat unless co-operative action is taken to implement best practice across the member state registries.

[24] COM(2010) 245 of 19.05.2010
[25] COM (2010) 2020 of 3.3.2010
[26] Ad personam (not as ENISA's ED)
[27] For example, http://www.bbc.co.uk/news/world-europe-12840941 & http://edition.cnn.com/2011/WORLD/europe/03/24/eu.cyberattack/
[28] http://en.wikipedia.org/wiki/European_Union_Emission_Trading_Scheme

Today most big organisations – public or private – have a CERT. The EU institutions would benefit from having a CERT that is both focused on their own needs and capable of liaising with the existing CERT communities. The role of supporting a specialised community and ensuring a constructive and effective dialogue with other members of the CERT community is central to the role of an EU institutional CERT.

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

Therefore the Rat der IT Weisen strongly recommend the establishment of a CERT for the EU institutions and propose that it is called "iCERT@eu".

Our final report identifies two crucial aspects for success of such a body:

- Providing a single point of contact for the 'outside world', and therefore for example taking away from third parties the burden of deciding to which institution specific information needs to be sent. iCERT@eu should have a clear and recognised coordination function among the EU institutions.
- Developing credibility, reputation and trust among the CERT community. It should be highly integrated into existing CERT communities, and find an active and responsive role among all other CERTs, in Europe and beyond.

ENISA, in its position as independent, experienced and – above all other things – trusted body in Europe is uniquely positioned to play the key role in the coordination of the incident response capabilities of the European Institutions. Experts from ENISA are established members of FIRST[29] and TF-CSIRT[30], and maintain vital relationships to all other CERT communities around the globe (like AP-CERT[31] and others). Furthermore, ENISAs experts have extensive experience in assisting CERTs in the provision and coordination of NIS incident response.

Hence we should build on already existing capabilities and enhance these, but also make sure that they work well together.

CYBER EUROPE 2010 Exercise

In November 2010, the first Pan-European Exercise for Critical IT Infrastructure Protection – Cyber Europe 2010 – was conducted. It was organised by EU Member States, facilitated by ENISA and supported by the Joint Research Centre.

[29] http://www.first.org/
[30] http://www.enisa.europa.eu/act/cert/background/coop/status-quo/evaluation/tf-csirt
[31] http://www.enisa.europa.eu/act/cert/background/inv/initiatives-outside-europe/ap-cert

More than 150 experts from 70 public bodies around Europe participated in this table top exercise. 22 Member States participated as players and eight Member States as observers.[32] In all, approximately 50 people were present in ENISA's branch office in Athens where the Exercise Control Centre was located They were exposed to more than 320 so called 'injects' related to the availability of Internet and corresponding critical online services. Across Europe in the participating Member States, around 80 people were acting upon the instructions of their national moderators in Athens. Typical profiles of players were Computer Emergency Response Teams (CERT), Ministries, National Regulatory Authorities, Intelligence Services, Cyber-Crime Units, etc.

The objective of the exercise was to trigger communication and collaboration between countries in Europe to try to respond to large-scale attacks.

The exercise was a first, key step for strengthening Europe's cyber defences and vital for the common goal to combat potential online threats to essential infrastructure, so ensuring that businesses and citizens feel safe and secure online. Supporting EU-wide cyber security preparedness exercises is one of the priorities of EU policies, in particular of the Digital Agenda for Europe.

The exercise tested three things:

- In the event of an incident which has its origin in another EU Member State – who do you call?
- How well do you understand the mandate and the decision making power of the person you are in contact with (you do not want to talk to someone for 30 minutes in a crisis situation only to discover that they cannot help)?
- Which communications channels should be used for which type of information?

Although these points appear to be obvious, the exercise showed that we have to improve in each of these areas if we are to be able to adequately face a major cyber incident.

Due to the time constraints, the private sector was not involved in the exercise. However, after the exercise, it was almost unanimously agreed that, in order to achieve more realistic exercises, the private sector must be involved. In this way, exercises will have a broader scope and be more realistic, thereby testing measures beyond cross country communication.

The exercise has shown that the procedures on how to handle cyber incidents do not yet exist on a pan-European level. Such procedures need to be identified and tested

[32] Including 3 EFTA countries, namely Norway, Switzerland and Iceland.

in future exercises. Also the dialogue on the necessity of Single Point of Contact or Multiple Points of Contact at the EU level should continue.

The Evaluation Report of Cyber Europe 2010 is available on ENISA's website on Monday.[33]

CONCLUSION

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.

International cooperation on incident response is by no means an easy task, and may require agreement on international rules of conduct, standards and norms. However, it is necessary if the international community is to be able to protect cyberspace.

We are in many ways moving in the right direction, and to continue on this path I strongly recommend the establishment of a CERT for the European Institutions.

ENISA's role is to support the Commission and Member States in facilitating dialogue on Network and Information Security across communities and with different international counterparts. We believe that this dialogue is a critical precursor to any long-term action plan for protecting information services that benefit EU citizens.

Thank you.

[33] http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report/at_download/file