



## ***Report on 7th ENISA CERT Workshop***

*Part II: Addressing NIS aspects of cybercrime*

*[Deliverable – 2012-11-15]*



### ***Acknowledgements***

We would like to thank Europol for co-organising this event, especially to Jaap van Oss, Tom Robson and Alexander Schol for their support in organising this event.

Our special thanks go to the moderators of the workshop sessions, namely Luc Beirens Federal Computer Crime Unit (Belgium), Dr. Serge Droz (SWITCH) and Vincent Danjean (INTERPOL), the presenters Steve Purser (ENISA), Monika Josi (Microsoft EMEA) and Olivier Burgersdijk (Europol) and to all participants.

Further acknowledgement should be given to the ENISA colleagues Jo De Muynck and Andrea Dufkova.

## About ENISA

The European Network and Information Security Agency (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](http://www.enisa.europa.eu).

## Contact details

To contact ENISA for this report please use the following details:

- Email: [opsec@enisa.europa.eu](mailto:opsec@enisa.europa.eu)
- Internet: <http://www.enisa.europa.eu>

### Legal notice

Notice must be taken 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

## Contents

Introduction .....	6
1 Methodology.....	7
2 Agenda .....	8
2.1.1 1st half day (16.10.2012): .....	8
2.1.2 2nd full day (17.10.2012): .....	9
3 1st Keynote: Moving Towards a European Cyber Security Strategy Steve Purser, ENISA .	10
4 2nd Keynote: The European Cybercrime Centre Olivier Burgersdijk, Europol.....	11
5 3rd Keynote: Cybersecurity & cybercrime Monika Josi, Microsoft EMEA.....	12
6 4th Keynote: Botnet Mitigation Luc Beirens, FCCU (Belgium) .....	14
7 Session 1: Botnet mitigation .....	16
7.1 Is botnet mitigation a business case for CERTs? .....	16
7.2 Ongoing and planned projects .....	16
7.3 Prioritization .....	16
7.4 Partners in this fight .....	17
7.5 Gaps.....	17
8 Session 2: Capacity building.....	19
Meetings .....	19
8.1 Liaison officers.....	19
8.2 Case studies.....	19
8.3 Data Protection .....	19
8.4 Exercises .....	19
8.5 Prosecutors.....	19
8.6 Member States' capabilities.....	19
8.7 Best Practices for management .....	20
8.8 Summary.....	20
9 Session 3: Cooperation/practical aspects of the fight against cybercrime .....	21
9.1 Inventory of information sources and how they are managed .....	21
9.2 Improving triage and alerting processes.....	23
9.3 Need for a global directory .....	23

9.4	Exchange Format .....	23
9.5	Lack of human resources or budgets .....	23
9.6	CERT statuses .....	24
9.7	Incompatible priorities .....	24
9.8	Way forward, next generation incident response workflow .....	25
9.9	Internet Service Providers' role.....	25
9.10	Intelligence and evidence collection .....	26
9.11	Takedown and sinkholing .....	26
9.12	Curative actions .....	26
9.13	Arrests.....	27
10	Evaluation.....	28
10.1	Presentations .....	28
10.2	Time .....	28
10.3	Sharing knowledge .....	28
10.4	Expert knowledge .....	28
10.5	Networking .....	28
10.6	Venue.....	28
10.7	Future.....	28
10.8	Topics.....	29
11	Conclusions .....	30
11.1	Highlights of the workshop sessions and conclusions.....	30
11.2	Remaining gaps and open gaps .....	30
12	Studies/reports mentioned during this workshop .....	31

## Introduction

ENISA and Europol organised jointly the 7th annual CERT Workshop, Part II, as a follow up event to the very successful 6th Annual CERT workshop<sup>1</sup> held last year in Prague, Czech Republic. This year the workshop was held at the Europol premises in The Hague on 16-17 October 2012. The focus remained on cooperation between national/governmental CERTs (n/g CERTs) in Europe and their national Law Enforcement counterparts (LEAs).

Out of a total number of 44 participants, 15 represented the national/governmental CERT, 12 the national Law Enforcement Agency (usually the high tech crime units). The other participants were experts from Industry as well as from international organisations. Belgium, Czech Republic, France, Germany, Greece, Hungary, Ireland, Luxembourg, Netherlands, Slovenia, Spain, United Kingdom were the EU Member States that participated as well as Norway and Switzerland.

The emphasis was on how to increase an exchange of information on cybercrime threats and the cooperation and collaboration on a practical working level between n/g CERT and LEA communities, both on a national and cross-border level. There is an urgent need for these two communities to collaborate because of their complementary responsibilities. A mutual cooperation can mean a win-win situation for both communities, because both CERTs and LEAs can learn from and support each other in the fight against cybercrime. Currently, in many cases this collaboration is very limited and sometimes even non-existent. The workshop aimed to identify synergies and gaps and practically address these obstacles for cooperation. It was also intended to discuss next steps which need to be taken in order to improve this collaboration in short term.

The format of this workshop was very similar to the approach chosen last year and was in essence composed of four keynote presentations followed by three interactive working sessions. Sessions were on the following topics:

- Botnet mitigation
- Capacity building
- Workflows and incident response

This report should be seen as a summary of the content presented and discussions which took place during one and a half day lasting workshop. It should be noted that this report represents the views of moderators, presenters and participants that emerged from the debate. It is not exhaustive and only points out the main thoughts and ideas.

This is the public version of the report. A similar non public version was sent out to all participants including a participants list and the presentations.

---

<sup>1</sup> <http://www.enisa.europa.eu/activities/cert/events/6th-workshop-cybercrime>

## 1 Methodology

The goal of sessions was to enable both communities to debate together and address questions such as how the collaboration can be achieved and improved. Each session was moderated by a specialist in the cyber security field. The moderators were suggested by ENISA and Europol and volunteered to lead the groups. The moderators had different methods to approach their sessions and in all three cases there was an intensive debate and discussion taking place. It should be noted that participants were split in three groups and each session was ran three times. This model enabled more room for discussion as the groups were small in size.

## 2 Agenda

### 2.1.1 1st half day (16.10.2012):

13:00-13:50	Registration
13:50-14:00	1st day opening (ENISA and Europol)
14:00-14:30	1st keynote ENISA, Steve Purser Head of Technical Competence Department
14:30-15:00	2nd keynote Europol, Olivier Burgersdijk Assistant Director and Designated Head of the European Cybercrime Centre (EC3)
15:00-15:30	Coffee break
15:30-16:15	3rd keynote Microsoft, Monika Josi Chief Security Advisor EMEA
16:15-17:00	4th keynote FCCU, Luc Beirens Head Federal Computer Crime Unit (Belgium)
17:00-17:30	Tour of Europol facilities incl. the new EC3
19:00-21:00	Dinner



### 2.1.2 2nd full day (17.10.2012):

09:00-09:30	2nd day opening (Europol and ENISA) and introduction to the working sessions by each moderator
09:30-11:00	Working sessions (1st round) Session 1: Botnet mitigation Presentation/Moderation: Luc Beirens, FCCU Session 2: Capacity building Presentation/Moderation: Serge Droz, SWITCH Session 3: Workflows and incident response Presentation/Moderation: Vincent Danjean, Interpol
11:00-11:30	Coffee break
11:30-13:00	Working sessions (2nd round) Session 1: Botnet mitigation Session 2: Capacity building Session 3: Workflows and incident response
13:00-14:00	Lunch break
14:00-15:30	Working sessions (3rd round) Session 1: Botnet mitigation Session 2: Capacity building Session 3: Workflows and incident response
15:30-16:00	Coffee break
16:00-16:45	Working sessions' conclusion – presenting the outcomes: 16:00 – 16:15 Session 1: Botnet mitigation 16:15 – 16:30 Session 2: Capacity building 16:30 – 16:45 Session 3: Workflows and incident response
16:45-17:15	Q&A
17:15-17:30	Closing notes (ENISA and Europol)

### 3 1st Keynote: Moving Towards a European Cyber Security Strategy Steve Purser, ENISA

The first keynote was given by Dr. Steve Purser, Head of Technical Competence Department, ENISA on the topic of 'Moving Towards a European Cyber Security Strategy'.

The presentation started with a brief introduction of ENISA's history, scope and tasks. As a Centre of Expertise the Agency supports the Commission and the EU Member States in the area of information security. ENISA facilitates the exchange of information between EU institutions, the public sector and the private sector.

After the introduction, the speaker elaborated on the topic of cyber security. From a technological perspective, there is little that separates classical information security from cyber security. Cyber security is about securing data and systems in the global environment. It is just the perspective and scope that change.

Adopting this point of view, cyber security is by definition a global concern. Due to the nature of this problem, advances in cyber security are most likely to be achieved through political (cross-border) cooperation.

Dr. Steve Purser gave an overview of European Member States with a National Cyber Security Strategy (NCSS) in place and noted that there is quite some difference in these strategies. He also briefly mentioned the Cyber Security Strategies of Canada, Japan and USA. There is no uniform way to approach such a strategy and it is clear that many countries have a different focus and scope in such strategies.

Towards the end of 2012 the EU Cyber Security Strategy<sup>2</sup> is expected. The main elements of this strategy are likely to be:

- Fostering close cooperation and early warning between Member States' competent authorities and the private sector;
- Ensuring adequate capacities and structures for prevention, detection, mitigation and response at national and EU level;
- Stimulating efforts to improve security of products, networks and services;
- Ensuring a strong EU response to cybercrime;
- Supporting R&D investments and strengthening the competitiveness of the EU's security industry;
- Reinforcing cooperation with international partners.

---

<sup>2</sup> COM(2011) 777 final VOL. 1/2 [http://ec.europa.eu/atwork/programmes/docs/cwp2012\\_en.pdf](http://ec.europa.eu/atwork/programmes/docs/cwp2012_en.pdf)

## 4 2nd Keynote: The European Cybercrime Centre Olivier Burgersdijk, Europol

The next presenter was Olivier Burgersdijk, Head of Strategy and Outreach for the European Cybercrime Centre (EC3). He gave an insight in the new EC3, its role and responsibilities and its place within Europol structure.

The EC3 is a part of Europol and its governance. EC3 is governed by a Programme Board consisting of external partners including international organisations such as ENISA and Interpol. The implementation phase has started in 2012 and is expected to be finished in 2014.

EC3 has multiple roles. It should function as a Fusion Centre, namely an information hub on cybercrime. The EC3 should:

- provide support on cyber operations and forensics;
- assist with capacity building (Law Enforcement, Prosecutors, Judges);
- reach out to the public and private partners;
- have a global view in order to define a strategic response;
- provide a collective 'voice' for European cybercrime investigators.

To achieve these roles, the EC3 has built relations with different partners. The key partners of EC3 are:

- Institutional partners (Including Eurojust, ENISA, EU CERTs, CEPOL, EUCTF, Interpol) ;
- Law enforcement (Member States, Cooperation partners);
- Judicial authorities;
- Private Sector;
- Universities;
- Non-governmental organisations.

EC3 defined specific priority crime areas where the centre will focus on. Among others this includes intrusion incidents, cyber-attacks, malware, internet based trade in counterfeit products, payment card fraud and child sexual exploitation.

## 5 3rd Keynote: Cybersecurity & cybercrime

### Monika Josi, Microsoft EMEA

The 3rd keynote was presented by Monika Josi, Chief Security Advisor EMEA, Microsoft, on the topic of cyber security and cybercrime.

She opened her talk by mentioning some cybercrime ‘realities’ mentioning some specific recent cases such as recent attacks on governments and private sector companies as well as ZBOT<sup>3</sup>.

She referred to specific organisational cyber security challenges, namely:

- Organizational fragmentation
- Lack of communication
- Unclear roles and responsibilities
- Lack of expertise

Cyber security is mostly seen as a national security topic. Reality and recent cases, however, show that the implications of cybercrime and hence cyber security reach all aspects of society. Currently, a lot of governments are looking into establishing a cyber-security strategy as a way to address this issue.

There is no one definition of cyber security or cybercrime. Nevertheless, the descriptions and definitions provided by the Council of Europe of cybercrime and cyber security<sup>4</sup> are used frequently. When using this definition, offenses involving Information Communication and Technology (ICT) are related to cybercrime and non-intentional incidents could be considered as purely cyber security related. However, there are also two big areas of overlap, namely offenses by means of ICT and intentional incidents. Very often it is a case that different stakeholders are involved in cyber security, than in cybercrime and cooperation between those stakeholders is in many cases not optimal.

From the perspective of Microsoft (and more specifically their Chief Security Advisors and Digital Crimes Unit) cyber security and cybercrime are seen as closely interlinked. This has not always been the case and only very recently have they realised from both sides that they could not be successful without listening and learning from each other. Today, there is hardly a day without communication between Security Advisors and their colleagues from the Digital Crimes Unit. This communication could be on national botnet projects, information sharing and capacity building initiatives.

A good way to approach this is to adopt a cyber-security/cybercrime agenda. The speaker referred to some influencing factors for such a comprehensive agenda, namely:

- A country’s threat landscape including threat actors and available threat intelligence data

---

<sup>3</sup> <http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fZbot>

<sup>4</sup> <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>

- A country's IT environment
- General technological trends such as Cloud, Consumerization of IT, social media
- The local market, e.g. the opportunity to turn cyber security into a competitive advantage to enable economic growth

Taking this broader view will help to address all aspects of the 'cyber-cycle' taking both cyber security and cybercrime aspects into consideration

- Protect information systems (typically the domain of cyber security)
- Detect anomalies (combined cyber security/cybercrime approach)
- Respond to incidents (combined cyber security/cybercrime approach)
- Recover from incidents (typically the domain of cyber security)

Important aspects are to see these as a 'cyber-cycle' rather than a bullet list and to make sure that there is a close collaboration between cyber security actors, cybercrime fighters, academia and the private sector. The involvement of all the aforementioned parties is important to be able to come to an accurate threat assessment, which will allow a pro-active response to the current threat landscape. Ideally, this collaboration is also fostered by the establishment of a common threat information sharing platform so this assessment and the corresponding response can be made based on a coherent information base.

## 6 4th Keynote: Botnet Mitigation

### Luc Beirens, FCCU (Belgium)

The next presenter was Luc Beirens, Head of the Federal Computer Crime Unit (FCCU) of the Belgian Federal Judicial Police and Chairman of the EU Cybercrime Task Force<sup>5</sup>. His speech was about a botnet mitigation issue. The aim of the presentation was an introduction to his moderated session the next day.

First the presenter showed some general trends applicable to today. He mentioned an evolution towards the e-society, where persons are replaced by e-applications, where all systems are interconnected, where there is a rise in the amount of mobile devices and where social networks are used increasingly. Throughout these trends, Internet Protocol (IP) is the common platform offered by many Internet Service Providers (ISPs) integrating telephone, data, Virtual Private Networks (VPS), etc.

Furthermore Mr Beirens stated that identity fraud is an easy thing to carry out as currently there is a poor security in legacy applications and protocols, and because the end-user is not yet educated to act properly. Cybercriminals mainly want to become rich and powerful in a rapid and easy way. Some of them want to destabilize society. But what is cybercrime exactly? It is a collective noun for many criminal activities. However, a big part of it can be linked to botnets, networks of systems being compromised by malware. Botnets are used for spamming, click generation, dialer installation, spyware/malware/ransomware installation, espionage, etc. They are also frequently used for Distributed Denial of Service attacks in order to disturb the functioning of an internet device. The fight against botnets is hence an important part of the fight against cybercrime.

New evolutions that could be seen in the field of cybercrime are:

- Political motivated attacks, namely hacktivism;
- Apple is no longer out of range and also starts to be targeted;
- Mobile device and smartphones are botnets of the future, as they're always online;
- P2P botnets, which are more difficult to fight, as there are no Command & Control servers (C&C) that could be taken down.

But do we have accurate statistics for cybercrime? No, we don't. Victims are sometimes unaware of the incident or the fact that their systems have been compromised. They also try to solve it themselves and rarely file a complaint. This lack statistics is according to the presenter one of the reasons why hackers go on with developing botnets.

So what are currently the barriers for an effective combat of cybercrime? The presenter mentioned the following issues:

- Lack of awareness and negligence of the victims/end users
- Lack of an overall/global view

---

<sup>5</sup> <https://www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523>

- Everyone is working on his own
- Lack of specialized investigators
- Jurisdiction is limited by national borders
- Mobility of criminal services

To overcome these barriers, everyone has to play a role in cyber security and they have to do it as partners and in an integrated way. The presenter gave insight into the Belgian situation and elaborated further on the topic to introduce his session the next day. The goal of his session is to see where good results in cooperation can be achieved.

## 7 Session 1: Botnet mitigation

The moderator of this session was Mr Luc Beirens from Federal Computer Crime Unit (FCCU) of the Belgian Federal Judicial Police. The session format was structured in an interactive discussion. Several questions were presented to the participants and various topics were addressed.

### 7.1 *Is botnet mitigation a business case for CERTs?*

In all sessions it was unanimously stated that botnet mitigation clearly is a business case for the CERT community. However, it became obvious that in various countries the roles of and workflow/approach between LEA and CERTs diverge (e.g. inform victim about infection and advise to report to the police vs. taking down C&C).

### 7.2 *Ongoing and planned projects*

To the surprise of the moderator hardly any ongoing or planned projects regarding botnet mitigation were known to the participants. This underlines the fact that there is a need for a broader awareness about what all stakeholders in the fight against botnets are actually doing. Communication between the CERT community and LEA can be improved and that projects should be made more known. Some of the projects mentioned were botfrei.de<sup>6</sup>, OPTA<sup>7</sup>, etc.

### 7.3 *Prioritization*

But somewhere in this fight we also have to prioritize. Generally it was acknowledged that work needs to focus on victims, internet infrastructure, end-user, botnet servers and hackers. During discussions the views on this question differ between CERTs and LEA. While LEA clearly argued for a prioritization - amongst others due to limited resources – some CERTs considered all C&C found on national territory worth action, whereas others argued that this was a question of criticality.

An interesting opinion was that the responsibility of the ISP regarding bots should be enhanced – if needed through a change of legislation.

Also, it became clear that additional progress needs to be made regarding the cooperation between CERTs and LEAs. One remark was to consider cooperation based upon contracts which clearly state roles and tasks for each partner (e.g. cooperation agreements). It has to be noted that this potential approach was not at all shared by all participants.

---

<sup>6</sup> <https://www.botfrei.de/>

<sup>7</sup> <http://www.opta.nl/>



## 7.4 Partners in this fight

Groups identified the following partners in the fight against cybercrime. This list should however not be seen as a ranking and complete. The following stakeholders were recognized:

- CERTs
- LEAs
- Internet Service Providers, telecom services, telecom regulators
- Antivirus industry
- Political decision makers
- Judiciary
- Intelligence services
- Software producers
- Hosting industry
- National Cyber Security Centers
- Financial institutions
- Operators of Critical Infrastructure
- Academia
- ICANN and other registrars
- Non-profit organisations e.g. Shadowserver
- End-users

## 7.5 Gaps

There also seemed to be a knowledge gap about roles, responsibilities and tasks of each stakeholder and this needs to be overcome in order to build up trust. Mechanisms on how to inform the others should be identified and implemented.

It became clear that actions and measures could be taken; however, legal dispositions on who can take down a botnet (legally and practically) remain an obstacle. In various countries the status of CERTs diverges and different CERTs (governmental, private, academia, etc.) are given different powers.

Another unanimously acknowledged problem identified was a lack of communication between CERTs and LEA. As a conclusion, it was established that clear roles and responsibilities, a clear vision of who needs which information in which format, could enhance trust which forms a basis for a fruitful cooperation.

Some additional problems and questions from a rather practical point of view were also identified and debated on:

- Can a botnet be used to send a patch?
- Since operators often work with virtual providers, they do not know who their customers really are (problem whom to inform).

- “Take downs” and giving image samples of infected PCs to the Anti-Virus industry may cause civil damage resulting in civil suits.
- An analysis of an infected victim PC would require asking consent of the victim.
- How do I know (as LEA or CERT) that my counterpart (LEA or CERT) is not focusing on the same target? There is a clear need for common communication procedures. This is an important for example for CERTs to know that they should not disturb an ongoing investigation and evidence gathering.
- PPP is essential but requires clear goals and roles for every partner.
- Often lack of voluntary cooperation between ISP and hoster to take down C&C indicates a need to start judicial or regulatory procedure.
- In some cases LEA is informed; however, the information provided does not fulfill requirements regarding the legality of the chain of custody and is not actionable by police.

## 8 Session 2: Capacity building

The moderator of the second session was Dr. Serge Droz from SWITCH<sup>8</sup> (Switzerland). The goal was to collect ideas how an improved collaboration between LEAs and CERTs could be achieved.

During the discussion, a number of suggestions and recommendations were formulated.

### Meetings

Regular meetings should be held. In the beginning at least, the focus probably should not be on concrete incidents, but on common issues. One CERT reported to offer “Workshops as a service” to facilitate contacts to LEAs. In this context it seems important to manage expectations.

#### 8.1 Liaison officers

LEA liaison officer in CERTs could help CERTs focus on the right issues and avoid process/policy errors that might degrade the value of the information provided. Having a CERT member joining a LEA was considered less effective.

#### 8.2 Case studies

The availability of a number of successful case studies would help shaping and guiding the start-up of a collaboration. Inexperienced teams could thus learn from existing success stories.

#### 8.3 Data Protection

CERTs and LEAs handle data of varying degrees of sensitivities. Try sharing in the obviously simple cases and work your way up to the more sensitive cases, thereby establishing best practices. Sensitive data is already exchanged with financial institutions. Maybe we could learn from there?

#### 8.4 Exercises

The CERT – LEA collaboration should be trained in a next exercise. Obviously this implies an already existing collaboration to begin with.

#### 8.5 Prosecutors

In many cases prosecutors do not understand the role of CERTs. There is a need to educate and train them to point out the value of CERTs as another actor on the stage.

#### 8.6 Member States' capabilities

A matrix, containing the possible capabilities in each Member State could be useful.

---

<sup>8</sup> <http://www.switch.ch/>

### ***8.7 Best Practices for management***

It was felt, that a best practice document for the management (“higher levels”) would be useful. No need was seen for such a document for the operational staff.

### ***8.8 Summary***

The issue is longstanding and not easily tackled. While all attendees agreed that collaboration must improve and that there are clear benefits from such collaboration, there is a little consent on how this should be achieved.

Most participants agreed that regular meetings are essential to improving collaboration. The meetings should not initially focus on specific incidents, but rather on common issues and problems. At a later stage these meetings could be used to discuss specific cases. It seems that a trust model, which is considered to be a key ingredient in successful CERT collaboration, is required for success.

Another suggestion that was made was deploying a Liaison Police Officer to a CERT (and possibly also vice versa). While this could potentially be a very effective approach it already requires an existing and good relationship between the two organisations. It could be seen as a possible next step after having built up trust between them. In some countries such liaison officers are already in place at CERT. These countries acknowledged that there is an improved collaboration and understanding of the other organisation’s work a lot since that.

Somewhat surprisingly, data protection issues were not considered an issue by some representatives from LEA and prosecutors. However, there are huge differences between Member States on how data can be used in a prosecution.

## 9 Session 3: Cooperation/practical aspects of the fight against cybercrime

The moderator for this session was Vincent Danjean from INTERPOL. He triggered a discussion on ‘cooperation and the practical aspects of the fight against cybercrime’.

Focusing on the incident management workflow, the session concentrated its work on identifying what processes, tools, and synergies are efficient and which need improving.

There was no pre-defined set of processes, tools or possible synergies to be discussed. On the contrary, the participants were encouraged and guided to achieve a comprehensive list of all matters to be discussed collectively. All listed items were then regrouped in families and prioritized by the participants.

This was achieved using a formal process of recursive brainstorming.

### 9.1 *Inventory of information sources and how they are managed*

The incident workflow starts with information flows, either for threat evaluation or for actual incident reporting and handling. According to the working group answers, the monitoring of the web and the general public combined, are the source for half of the information collected.

The professional world (CERTs, LEAs, and security companies) account for the other half of information sources, each, in almost identical proportions.

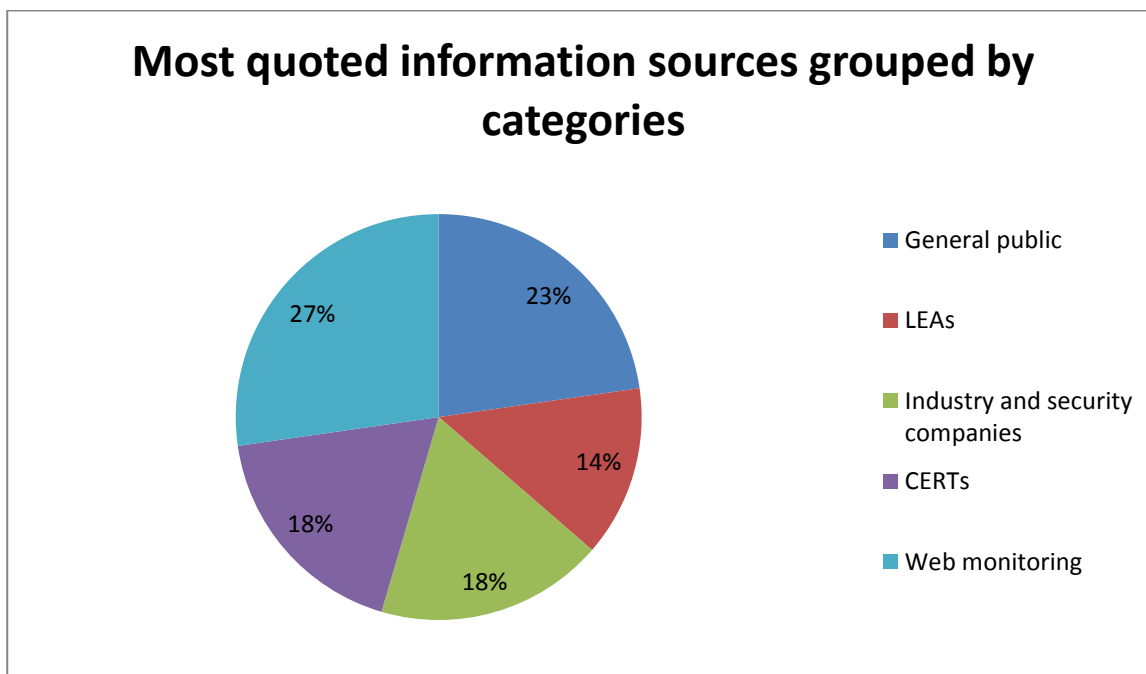


Figure 1 - Information sources by categories

Comparing the relevance of the information collected from each source provided a view on which sources are efficient, can be trusted or just create noise.

The Information shared from CERTs is for instance less prone to reveal false positives and consequently, the level of trust and efficiency is high. Generally we could conclude that the volume of information received from a source is inversely proportional to the level of trust the group has from this same source.

Automation is found to be a key in the management of information to avoid undue and inappropriate use of the limited resources. Public sources of information are found to be less structured and the management of it is still widely manual. ‘Professional’ information sources are increasingly structured. Information exchange formats exist but they are not yet sufficiently recognized. It was no surprise that only very few of the workshop participants actively use information exchange formatting and automation.

Web monitoring for information sources is an interesting case as well. Automated web monitoring tools are emerging and are rapidly adopted by the incident response community (marketing tools are derived from their initial purpose: brand monitoring, Google alerts, etc.). However, the offer not only lacks maturity when it comes to incident response matters but the volumes collected can be overwhelming. We can conclude that collection is increasingly automated but the processing (analysis, correlation, etc.) is far behind in terms of availability of automation.

The incident response community currently only handles information when it relates to an already identified issue. This was found mostly due to 4 factors: limited resources, overwhelming volumes, lack of automation, lack of source qualification.

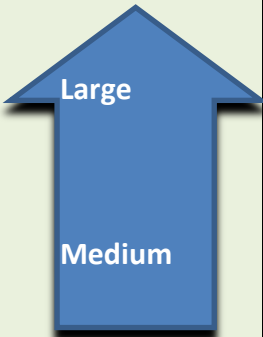
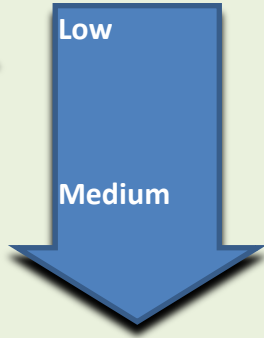
Source	Volume of information	Relevance and trust	Automation	Needs
General public (emails, contact forms, phone calls...)			Hardly available	Tools
Web monitoring			Collecting: basic	
Industry and security companies			Processing: widely manual	Regulation
CERTs			Exchange formats exist but are not widely used	
LEAs			case-by-case	

Figure 2 - Sources, showing volumes, relevance and trust, level of automation and improvements needed

## 9.2 *Improving triage and alerting processes*

The participants also concentrated on reasons why triage and alerting sometimes fails or is delayed.

## 9.3 *Need for a global directory*

Whilst the group recognized the efficiency of face-to-face meetings to build a network of trusted interlocutors, the group also acknowledges a strong need for a global directory. As people change, face-to-face networking shows its limits. The trust established at a personal level now has to be elevated to unit or department level trusts. A pyramidal overview needs to be established to break the silos.

The recommendation expressed by the group as a strong consensus was for the establishment of a structured directory; repository of specialized units and their expertise or domains of activity.

This global directory shall be designed and maintained by an international body (Europol or INTERPOL are proposed) and follow a structure established under the management of this body, based on the inputs from the community.

## 9.4 *Exchange Format*

When alerting and time is paramount, translation and misunderstanding will cause undue delays.

The information exchanged amongst the different actionable communities need to be shared in a common format AND based on the same understanding of confidentiality and handling rules.

This common framework therefore needs to address:

- the language barriers
- the criteria and accreditation required for the collecting and preserving of what is to be considered valid evidences (or else the information is to be considered as “actionable intelligence”)
- the set of possible items to be exchanged and their definitions
- the common rules for confidentiality and secure handling. TLP (Traffic Light Protocol) is becoming a fairly accepted and understood set of levels within CERTS, Industry and some Government bodies. But this needs to be balanced with other schemes derived (more or less accurately) from National or military grade confidentiality regimes.

## 9.5 *Lack of human resources or budgets*

The incident workflow is often failing due to lack of expertise or lack of human resource designed under the current priorities.

The group identified several reasons or potential avenues for improvement.

Because all participants reported failures of processing due to lack of resources, automation came to mind as a potential improvement.

Automation could indeed free precious human resources and offers the advantage to concentrate on the more rewarding and expert intensive tasks of the incident response workflow. Automation should therefore come concurrent with the delivery of training to optimize reallocation of the human resources freed.

Another avenue that clearly stood out of the group reflections is to provide higher authorities with the decision making proofs that incident workflow is key and currently vastly under prioritized. This can be addressed via awareness and reporting.

An additional advantage of reporting to and raising awareness to the highest authorities is that the lack of legal framework often quoted as another reason for failure, can also be acted upon by them.

### 9.6 *CERT statuses*

The statuses of National CERTs widely differ from one country to another. In the light of countries where digital forensics can be delegated to private entities by Law Enforcement, the group found it was urgent to address the legal status and bindings for CERTs (National or not).

Some consideration should be given to a legal framework: when working for Law Enforcement or with a view to civil or penal prosecution, the question is asked: would CERTs be legally empowered to collect evidences, should CERTs be the de-facto experts called to testify in court?

### 9.7 *Incompatible priorities*

Another identified reason for failure or undue delay in processing triage or alerting, is conflicting priorities amongst the actors.

Some examples:

- While a CERT's main priority would be to takedown a domain name in order to temporarily disrupt an attack, LEA's priority would probably be to delay the takedown in order to avoid collateral damage to other ongoing investigations or to gain sufficient time to collect substantial evidences.
- While industries main concerns could be related to financial aspects, the general public could be primarily concerned with its safety.

National laws and regulations are usually very clear in what is expected of LEAs or what a priority is when it comes to the protection of critical infrastructures. However for the other actors, the regulators have a role to play in order to establish what the obligations are for each party, regardless of their own prime interests.

The lack of harmonization of these priorities through the different legal or regulatory systems at international levels compounds this.



### 9.8 Way forward, next generation incident response workflow

The group created a large matrix of actors versus actions required in incident handling. Each individual in the group was given five 'priority points' to be posted on actors, actions or interactions that they believed called for the most urgent improvements or attention.

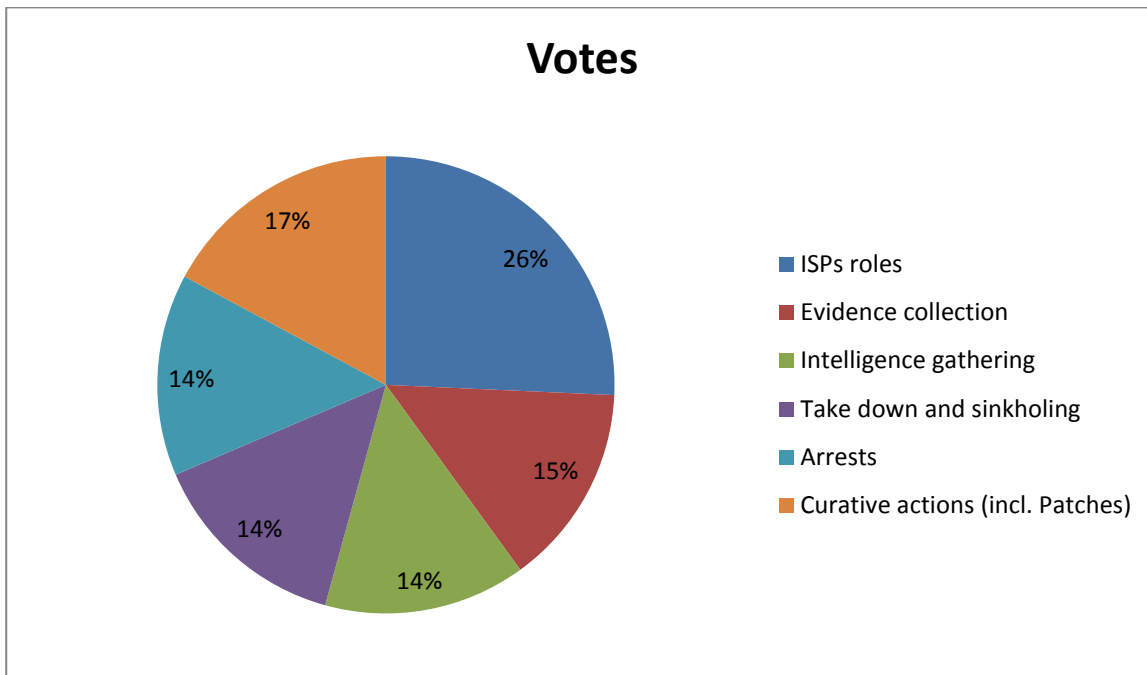


Figure 3 - Votes for top actors, actions or interactions. As is clearly seen in the above graph, Internet Service Providers come first. This is not a big surprise as they have a major role to play in almost all the steps in incident management.

The other priorities selected as the top ones have received approximately the same number of votes.

### 9.9 Internet Service Providers' role

With the strong take on Cloud computing, one should think of ISPs not only as carrying data but also as hosting, content or value-added service providers. Security around these services is such that investigations will be even more of a challenge if the ISP does not cooperate.

The role of the ISPs is amplified by the fact that some actions are required from them in the very first steps of the mitigation phase and are therefore urgent. Additionally, lack of cooperation from the ISPs in the evidence collection process will strongly impact the investigations.

LEA investigations demonstrate that malicious people choose their service providers (VPNs, servers, proxy services...) based on the ISP's policies towards logging and cooperation with Law Enforcement.

Several reasons were quoted by the group:

- Lack of resources (ISP staff and price of storage space for logging)
- Privacy laws used as a shield to evade logging obligations (IP address as personally identifiable information...)
- Fear of negative publicity

However, we have examples, including in Europe, where ISPs were not given choices as to whether they want to cooperate: civil law suit, Microsoft vs. servers of the Bredolab botnet or criminal law suits where LEA seized several servers and strongly disrupted the services of an ISP who refused to act upon a court order to help extract the relevant logs.

### 9.10 *Intelligence and evidence collection*

Intelligence and evidence handling were treated as one since up to now; they were mostly performed by the same experts. The concerns encountered by the group could be addressed in a common Standard Operating Procedure. This SOP would have to describe:

- The obligations towards monitoring, sharing and knowledge building
- The formats for exchange
- The legal frameworks
- The data quality insurance criterion

The judicial system was found by the group to be lacking expertise. CERTs have this expertise and could either train or are empowered to act on behalf of the judicial system (see “CERT statuses”, above).

### 9.11 *Takedown and sinkholing*

Takedowns and sinkholing are techniques used to heavily disrupt a botnet, fraud, phishing scam etc.. Whilst terminating resources in the chain of the fraud may deter or discourage criminals, in effect it merely just displaces the issues elsewhere. Victims are left unaware of the issues and collateral damages are to be expected (other licit services may suffer from the termination).

The international legal framework needs to address how incident management communities can legally contact potential victims (see below “curative actions”). This legal framework shall also document how botnets’ Command and Controls distributed over servers in several jurisdictions can be taken down. Big private institutions may have resources to coordinate civil law actions in each jurisdiction, but how does this compare to the capacities of the penal (criminal law) system or the CERT communities?

### 9.12 *Curative actions*

By curative actions the group discusses the means we have to fix a known issue. For this, botnets are a classical example. The botnet servers may be killed and criminals convicted but victims’ machines remain infected with malware long after this.

Product vulnerabilities are disclosed every day and exploits are soon freely available.

What are the responsibilities of the company creating the products, of the company using these products and of the end users using these products sometimes unwittingly?

The incident management community can help alerting the victims but are often not legally authorized to do so. As mentioned previously, the legal system shall define whose responsibility this is and the legal framework applicable to it.

When it comes to internet, the end user has a contract with its Internet Service Provider. This could be the only way to legally contact the end user and help enforce curative actions on their machines. These simple rules exist when we want to use the motorway, why not for the internet?

### **9.13 Arrests**

When discussing arrests, international aspects are soon on the agenda.

Legally, to define what a crime is and to define how international cooperation is carried out may assist prosecution.

Logistically, both the restraining on how criminals can move before they are localized by LEA and a greater mobility of the investigators and response teams will be of assistance.

The group repeated the need for an International instrument to tackle cyber issues.

## 10 Evaluation

After the workshop we have received a 27 written evaluation forms as well as some oral feedback. The results are described below.

### 10.1 Presentations

On the question 'Were the presentations of interest?' we received an average score of **4.3 out of 5** where 1 means 'not at all' and 5 means 'absolutely so'.

### 10.2 Time

The second question asked 'Was there sufficient time to discuss topics with others?'. The average score was **4.0 out of 5** where 1 means 'not at all' and 5 means 'absolutely so'. This means that generally speaking most participants were satisfied with this one and a half day approach. However, it must be noted that we received orally the feedback that some participants preferred to have a meeting lasting a little longer.

### 10.3 Sharing knowledge

Next to that we asked the participants 'Was it possible to share knowledge with others?'. The average score was **4.2 out of 5** where 1 means 'not at all' and 5 means 'absolutely so'. As this was one of the main objectives of this workshop we are pleased with this high score.

### 10.4 Expert knowledge

We also asked the participants if they learned from the experts and presenters at this workshop. We formulated it 'Did you benefit from the presenters' expert knowledge?'. Here we received a **4.1 out of 5** where 1 means 'not at all' and 5 means 'absolutely so'.

### 10.5 Networking

For both questions 'Was there sufficient opportunity to network?' and 'Did you identify new partners for your activities' we received **4.2 of 5** where 1 means 'not at all' and 5 means 'absolutely so'. Networking and finding new partners to connect with is key to the success of this workshop.

### 10.6 Venue

The average opinion of the venue and the catering was **4.7 out of 5** where 1 means 'didn't like' and 5 means 'liked very much'. We were extremely content that this year this workshop could be hosted at the Europol premises.

### 10.7 Future

Participants scored on average **4.6 out of 5** where 1 means 'didn't like' and 5 means 'liked very much' on the question 'I would like to participate in other workshops the following years'.

## 10.8 Topics

We also queried the participants on which topics they would like to see covered. These are the main topics that came out of this:

- Best Practices
- Elaboration on proposals for cyber legislation/legal framework of information sharing
- Roadmap to a shared future
- Public-Private cooperation (i.e. ISPs)
- Mobile/BYOD and other recent threats
- Automated data exchange between CERTs and LEA
- Use of sensors
- Presentation of the various botnet initiatives and the status of the botnet project ACDC<sup>9</sup>

Others comments we received:

- Add prosecutors to this workshop and explain them what CERTs do and vice versa.
- Limit the representation of the private sector to encourage information sharing.

---

<sup>9</sup> <http://www.law.kuleuven.be/icri/projects.php?projectid=256&where=>

## 11 Conclusions

The workshop mainly aimed to identify synergies and gaps and how to practically address these obstacles for cooperation. As the feedback and evaluations suggest, it is desirable to repeat this event. This workshop should be seen as one step in the process of creating a smoother CERT-LEA cooperation.

As the workshop sessions revealed, there are already a lot of good practices going on, but more can still be done.

Participants called for a stronger ENISA-Europol cooperation in addressing these problems.

The workshop was a clear success based on the feedback from the participants both during the workshop and through the evaluation forms afterwards.

### 11.1 Highlights of the workshop sessions and conclusions

- When sharing information and cooperating and collaborating on a cross-border level, several legal aspects should be taken into account.
- Trust is key to proper cooperation between CERTs and LEA. Good ways of doing this is by integrating someone from one team into the other team. This can be done through internships, but also a variety of other ways, for example by establishing a cybercrime coordination body. This is referred to as 'embedded LEA'.
- Collaboration should be bilateral. Information should flow in both directions in order to stimulate the CERT community to keep on cooperating. General feedback was that CERTs tend to stop sharing information when communication is only one way. LEAs should try to acknowledge the CERTs.
- When handling computer incidents, cooperation with other actors, e.g. ISPs, is particularly relevant.
- In general, if a request for information comes from CERTs from other country, the local CERTs can accommodate it and pass the information; on the contrary, if the request comes from the LEA from another country, this request in order to be accommodated must pass via the local LEA.

### 11.2 Remaining gaps and open gaps

- There are still a lot of differences between the Member States when it comes to information sharing and more specifically the Data Protection issues. This is possibly a good topic for a next workshop.
- Also the cooperation with ISPs seems to be an open issue.
- Automated data exchange between CERTs and LEA is also an open gap. This is also related to the Data Protection issues.

## 12 Studies/reports mentioned during this workshop

We list here some studies and reports mentioned during this event:

- ENISA, Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime - A first collection of practices  
<http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cybercrime>
- ENISA, Botnets: 10 Tough Questions  
<http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/botnets/botnets-10-tough-questions>
- ENISA, A flair for sharing - encouraging information exchange between CERTs  
<http://www.enisa.europa.eu/activities/cert/support/legal-information-sharing/legal-information-sharing-1>
- De Natris Consult, National Cyber Crime and Online Threat Analyses Centres: A study into national and international cooperation  
<https://woutdenatris.files.wordpress.com/2012/09/online-threats-report-17-09-2012.pdf>



P.O. Box 1309, 71001 Heraklion, Greece  
[www.enisa.europa.eu](http://www.enisa.europa.eu)