European Network
and Information
Security Agency

The Fight against Cybercrime

Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime

-

A first collection of practices
[Deliverable – 2012-2-28]

Acknowledgements

We would like to thank the members of the informal Expert Group established by ENISA to provide support for the review of this study; namely Hillar Aarelaid (CERT-EE), Carlos Fragoso (CESICAT CERT), Wim Hafkamp (EU FI-ISAC), Kauto Huopio (CERT-FI), Toshihiko Kamon (Interpol), Andrea Kropacova (CSIRT.CZ), Michael Samson (EU FI-ISAC), Jaap van Oss (Europol) and Anto Veldre (CERT-EE).

Further acknowledgement should be given to the ENISA colleagues who contributed with their input to this study, in particular: Agris Belasovs, Andrea Dufkova and Silvia Portesi.

Supervisor of the study and contributor: Jo De Muynck (ENISA).

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.

Contact details

For contacting ENISA or for general enquiries on ENISA's CERT activities, please use the following details:

- Email: cert-relations@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to this report, please use the following details:

- Email: jo.demuynck@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.

Contents

1 Executive Summary

To act against cybercrime, collaboration between many actors and communities is required. In this collaboration the Computer Emergency Response Teams (CERTs) and Law Enforcement Agencies (LEAs), are paramount and indispensable players. At present CERT and LEA communities work mainly on their own in the fight against cybercrime. This report is a first attempt by ENISA to stimulate the discussion on this topic and to enhance the collaboration between these two communities to deal with this phenomenon more efficiently and effectively.

The essential aim of this report is to improve the capability of CERTs, with a focus on the national/governmental CERTs (n/g CERTs), to address the network and information security (NIS) aspects of cybercrime. It focuses particularly on supporting n/g CERTs and their hosting organisations in the European Union (EU) Member States in their collaboration with the LEAs. It also intends to be a first collection of practices collected from mature CERTs in Europe, including among other things workflows and collaboration with other key players, in particular different law enforcement authorities, in the fight against cybercrime.

The chosen approach for this project was to enable and facilitate an initial meeting between the CERT and LEA communities on the European level and within its limited scope to trigger and intensify the debate between them in order to compose this document. This report is based on information gathered from three sources – an informal expert group, the ENISA 6th CERT Workshop and a tailored questionnaire.

This initial report tries to shed light on specific areas of the issue, especially focusing on commonalities and differences between the CERT community and the LEA community, their goals and methods. The main objective is to get a clearer and more detailed picture of the gaps and obstacles in their day-to-day practical cooperation and to propose possible ways to overcome them. It focuses on three domains of this collaboration, namely the operational-technical, legal and the cooperation aspects of the fight against cybercrime.

This first draft derives several conclusions and recommendations which are limited to the scope of this document, including:

<u>Conclusions</u>

- The importance of trust for cooperation between CERTs and LEAs. Integrating both teams is a good practice. Several types and levels of integration can be distinguished.
- Both formal and informal communication and cooperation between CERTs and LEAs should exist, as both have their own advantages.
- Collaboration has to be bilateral. Information should flow in two directions in order to stimulate the CERT community to cooperate.

- It is undoubtedly important for LEA teams to know that they can count on the expertise of a CERT team for assistance in handling certain cases; however, the mandatory handling of criminal cases could damage the agility of the CERT community, which is one of the most valuable assets of the CERT teams.

Recommendations

- Currently there is a lack of opportunities for CERTs and LEAs to meet. There should be a focus on national-level meetings. Synergies between meetings and events should be explored in order to decrease travel and time costs as much as possible.
- For the mitigation of cybercrime, it is recommended that national legislation is made clearer and that exceptions are made, for example for CERT teams.
- Europol and ENISA should cooperate to fill the gaps in education when it comes to training for officials such as judges and prosecutors on cybercrime matters, as there are already some initiatives in place. It is extremely important that these people are well informed on this topic as they have a decisive role in the investigation and prosecution of cybercrime.

In general, as CERTs and LEAs tend to be very different in nature and have different roles and priorities, it can be difficult to initiate cooperation. It is very important, though, to begin this collaboration, even if this partnership is only limited at the beginning.

2 Introduction

In 2010 the European Commission launched its Communication the ‘Digital Agenda for Europe’.[1] This policy agenda aims to achieve a new digital single market by the year 2020. One of the goals of this agenda is to provide Internet access to all Europeans. By 2013, all Europeans should have access to basic broadband and by 2020, all Europeans should have access to much higher Internet speeds of above 30 Mbps and secondly, 50% or more European households should have subscribed to Internet access above 100 Mbps.

Along with this foreseen and planned higher connectivity of European citizens, they have also become increasingly dependent on IT over the years. The World Wide Web, social networks, online shopping, mobile Internet, etc., are only some examples where technology is influencing our lives to an increasing extent and starts playing a vital role in both economic and social development.

The digital economy is laying the foundation for a more prosperous Europe; however, it also brings with it some challenges that should not be overlooked. As more and more Europeans get connected and the digital market becomes bigger and bigger, the incentives for criminals to try to make a profit out of this in illegal ways have risen dramatically in recent years. Crime in cyberspace is increasing and has become a real problem. Financial gains are the main motivation for cybercrime.

Cybercrime is real and it does form a realistic threat. One well known example, although not financially motivated, where a whole country was targeted was the attack against Estonia, which was hit by a large wave of cyber attacks back in 2007. Citizens, industry and governments are increasingly falling victim to all forms of cybercrime, including phishing, botnets, etc. It is essential that these challenges be addressed.

As a direct result, one of the focus areas of this digital agenda is ‘trust and security’. Europeans simply will not embrace technology they do not trust. Europeans should feel secure in order for them to engage in online activities, which get progressively more sophisticated every day. As we rely more and more on network and information systems to provide us with crucial services in our economic and social lives, it is not difficult to see the potential danger of cybercrime. In this respect, it is important to address and counter the rise of cybercrime and to prepare a concerted and coordinated response to cybercrime in general and to cyber attacks more specifically.

Collaboration between many actors and communities, including Computer Emergency Response Teams (CERTs) and Law Enforcement Agencies (LEAs), is paramount to a successful fight against the

[1] *COM (2010) 245 of 19 May 2010 (‘Digital Agenda for Europe’) available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:HTML [accessed on 2 December 2011].*

cybercrime. As CERT and LEA communities currently work mainly on their own, ENISA is looking more closely into this collaboration and trying to identify possible synergies and gaps. This report – which is one of the deliverables foreseen in the ENISA Work Programme (WP) 2011[2] – is the first attempt by ENISA to stimulate discussion on this issue and to enhance collaboration between these two communities.

2.1 Rationale

In November 2001, the Council of Europe Convention on Cybercrime[3] was opened for signature; now, more than 10 years later, it has still not been ratified by all the European countries.[4]

At the level of the EU Member States, gaps still exist in terms of preparedness to respond to cybercrime and cyber attacks. Until now, only some of the EU Member States have adopted national cyber security strategies (e.g. Estonia, Czech Republic, Finland, France, Germany, Lithuania, the Netherlands, and the UK) or carried out national cyber incident exercises or training (France, Germany and Sweden). National capabilities in information security, such as CERTs, are crucial for Europe to be able to handle a serious incident. What is clearly missing at present is a coordinated response to large-scale cyber attacks.

Cybercrime is currently one of the fastest-growing areas of crime.[5] Numbers do not show the complete picture though, as only a small number of cyber-related crimes are reported to law enforcement agencies.

The aim of this report is to improve the capability of the n/g CERTs to address network and information security (NIS) aspects of cybercrime. It focuses in particular on supporting n/g CERTs and their hosting organisations in the EU Member States in their cooperation with the LEAs.

This report intends to be a first collection of practices collected from mature CERTs, including among other things workflows and cooperation with other key players, in particular those concerned with law enforcement, in the fight against cybercrime.

[2] *ENISA Work Programme 2011 available at http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011 [accessed on 2 December 2011].*

[3] *Convention on Cybercrime (23/11/2011) 'Convention on Cybercrime, Budapest, 23.XI.2001', Council of Europe, Available from: http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm [accessed on 2 December 2011].*

[4] *The list of signatures, ratifications, and entry into force is available at: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG [accessed on 2 December 2011].*

[5] *https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf*

2.1.1 Background information and motivation

In chapter 2.3 of the abovementioned Communication 'A Digital Agenda for Europe', the European Commission states: 'Cooperation between CERTs and law enforcement agencies is essential'.

In that respect one of the ENISA's activities in 2011 focused on creating a first collection of practices in the form of a report for CERTs on addressing NIS aspects of cybercrime, more specifically in their cooperation with LEAs. Details are laid out in Work Package (WPK) 1.5 of ENISA WP 2011.[6]

Moreover, in its Communication 'The EU Internal Security Strategy in Action: Five steps towards a more secure Europe',[7] the European Commission stresses ENISA's role in improving Member States' capabilities for dealing with cyber attacks and highlights, amongst other priorities, the importance of CERT and LEA cooperation.

Pursuant to the ENISA Work Programme 2011 (WP 2011), this document tries to initiate and stimulate the discussion on potential synergies and gaps between the CERT community and the LEA community in order to enhance this collaboration in practice.

In 2012 ENISA continues to address this important topic. As stated in the ENISA WP 2012,[8] ENISA has carefully followed developments in information and communication technology (ICT) and changes in the global network threat landscape. Whilst the work programme itself focuses strongly on key policy objectives, ENISA has remained open for dialogue with other communities involved in improving information security, on both a pan-European and international basis.

2.1.2 Target audience and scope

The intended target audience for this collection of practices are managers and technical staff of national/governmental CERTs and LEAs, decision-makers in the Member States responsible for the integration of national/governmental CERTs into the national cyber security strategy and European and international institutions dealing with the fight against cybercrime. In addition to this, the initial document can be useful in helping any mature or newly established CERT or abuse team to better understand the collaboration between the CERT and LEA communities.

[6] *The ENISA Work Programme 2011 is available at http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011 [accessed on 2 December 2011]. See in particular Work Package (WPK 1.5) on pp. 24ff.*

[7] *http://ec.europa.eu/home-affairs/policies/iss/internal_security_strategy_en.htm*

[8] *The ENISA Work Programme 2012 is available at http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/copy_of_20111220WP2012V40.pdf [accessed on 25 January 2012].*

3 Approach

The general approach for creating this first collection of practice was to involve the CERT community and the LEA community as much as possible. Therefore ENISA chose three main sources for the relevant information.

3.1 Methodology

This report is based on three major inputs. A first part of the information ENISA gathered came from the ENISA informal expert group activities (NIS-CC-EG-2011) (see section below 'Informal expert group') in the field of CERTs which was set up to address NIS aspects of cybercrime to enhance the CERTs and LEA cooperation in fighting cybercrime. This expert group was established and run by ENISA in 2011 to support ENISA's activities in this area. Apart from providing input, this group also reviewed and commented on the final document. The second input came from the working sessions and the conclusions of the CERT workshop organised by ENISA together with Europol in October 2011. In addition, a short tailored questionnaire (see Annex I) was sent out to the European CERT and LEA communities, as well as the members of TF-CSIRT to collect information for the report.

3.1.1 Informal expert group

To support the draft and the review process, and in particular to ensure the practical usefulness of this report, in 2011 ENISA established an informal group of experts from the CERT and LEA communities, who discussed issues related to 'NIS aspects of cybercrime' and provided input to this report and a review of the final version. Other communities such as the financial community European FI-ISAC[9] were also brought into the discussion, because of their affinity with the topic of cybercrime.

This group was informal and was kept small in order to enhance the effective exchange of information and opinions. The format of communication was teleconferences and emails with one face-to-face meeting in Tallinn, Estonia, in December 2011.

The expert group was a valuable source of knowledge and experience for drafting this report.

3.1.2 ENISA's annual CERT Workshop

It is important to increase the exchange of information on cybercrime threats and the cooperation and collaboration on a practical working level between the CERT teams and law enforcement entities, on a

[9] *The FI-ISAC Europe (Financial Institutions – Information Sharing and Analysis Centre) was established in 2008 with the aim of building a network between financial institutions, law enforcement agencies and national CERTs. The idea was to share information on incidents, threats, vulnerabilities and good practices. ENISA supported the establishment of the FI-ISAC Europe.*

national and a cross-border level. The two respective communities are bound to collaborate because of their complementary responsibilities. Cooperation can mean a win-win situation for both communities as CERTs and LEAs can learn from and support each other. Hence, a workshop was organised by ENISA and Europol with the aim of aim of identifying synergies and gaps and discussing how these gaps can be overcome.

The annual ENISA Workshop 'CERTs in Europe'[10] took place on 3 and 4 October 2011 in Prague, Czech Republic. ENISA co-organised this 6th ENISA CERT Workshop together with Europol and with the support of the national computer emergency response team in the Czech Republic (CSIRT.CZ).

While ENISA focused the 2010 CERT Workshop on the role of national/governmental CERTs in national and cross-border exercises, the topic of the 2011 CERT Workshop was 'fighting cybercrime in practice', and more particularly the operational, technical and cooperation aspects of the collaboration between national/governmental CERTs and the law enforcement agencies (LEAs) in the different European Member States on both a national and cross-border level.

The workshop had the following main goals and objectives:

- To enhance cooperation between several European organisations active in the fight against cybercrime (ENISA, Europol, Eurojust, European Commission, etc.).
- To bring together for the first time representatives from both the national/governmental CERTs community and the LEA community in Europe to enhance dialogue on the topic of cybercrime.
- To collect information about the current state of collaboration between both communities and to take stock of examples and experiences of cooperation in the fight against cybercrime.
- To look for gaps and synergies in the collaboration between those communities. The different possibilities of overcoming these possible obstacles were addressed, more specifically with respect to the technical, legal and cooperation aspects of their collaboration in the fight against cybercrime.
- To facilitate a discussion on the role of ENISA, Europol, and other European and international organisations in this field.

Representatives, from both the CERT and LEA communities from different EU Member States and EFTA countries, as well as European and international organisations such as the European Commission, ENISA, Europol, Eurojust, Interpol, CERT-EU, NATO NCIRC/TC and CCDCOE, contributed to the discussions during interactive sessions.

[10] http://www.enisa.europa.eu/act/cert/events/6th-workshop-cybercrime/

The interactive sessions were moderated by external experts. The moderators led the debate and the participants discussed three topics relating to the fight against cybercrime with regard to the n/g CERT and LEA cooperation.

The topics were:

- Operational/technical aspects of the fight against cybercrime
- Cooperation/practical aspects of the fight against cybercrime
- Operational/legal aspects of the fight against cybercrime

Prior to the workshop several relevant questions (see Annex II) were distributed amongst the participants in order to facilitate preparation for the discussion and debate. These questions were targeted questions prepared by the moderators, based on their experience, and adapted and reviewed by ENISA in order to ensure coherence between the different sessions.

3.1.3 NIS aspects of cybercrime questionnaire

A short questionnaire was sent out to the European CERT and LEA communities, as well as the members of TF-CSIRT, in the second half of October, after the workshop. Questions were relevant to the operational, cooperation and legal aspects of the fight against cybercrime and tried to fill the gaps in the feedback received during the workshop. The questionnaire included 25 targeted questions and stayed open for three weeks. Unfortunately, the response was limited to this survey.

4 Different NIS aspects of the fight against cybercrime

Cybercrime is a very broad topic. Because of the scope and the available resources for this project ENISA decided to address only three aspects of the phenomenon in this initial draft. A first set of aspects are the operational and technical aspects of the fight against cybercrime, with a clear focus on a coordinated response and on cooperation between CERTs and LEAs. Next to that we take a closer look at the legal aspects of this fight. We conclude with some practical organisational aspects on the cooperation between CERTs and LEAs.

4.1 Operational and technical aspects of the fight against cybercrime

This section tries to give an overview of some operational, technical and practical aspects of the fight against cybercrime and more specifically of the collaboration between CERT and LEA teams.

4.1.1 Integration and trust

Trust is a strong factor for every form of collaboration for both CERT and LEA communities. It is important to know and trust members of the other team/organisation. Different approaches for establishing such a trust relationship are possible.

A first model to build trust between organisations is creating internship positions from one team to the other. This mostly relates to someone from the LEA team working in the premises of the CERT team. This way someone with a law enforcement background is present in the CERT team and can share the experience from his or her perspective and answer questions from the CERT team accordingly. It is also a major help when discussing incident triage, case transfer flow and which cases should be handed to the police. This could clearly enhance the collaboration between the teams and increase the level of trust between them. Some CERT teams are already doing this and report that it is very worthwhile. They learn a lot from each other during day-to-day operations. An example that could be mentioned here is CESICAT in Catalonia where a law enforcement officer is taking part in the daily operations of the CERT team.

There is a strong interest in doing this the other way around, and having someone from the CERT team present in the law enforcement team. The technical skills and background of CERT staff could be highly valuable to LEAs.

Another approach is to create new organisations or bodies, combining people from LEA and CERT teams, but also from the military, intelligence and other relevant key players. In some countries the CERT team itself is joined by people ‘seconded’ or ‘detached’ from LEA. This is the case in Romania, for instance.

Trust is also a very important aspect when cooperating across borders in general, and hence also on cybercrime cases. It was noted that CERT teams sometimes contact a foreign LEA team directly when they 'know' the team or a team member. There are some sensitivities in this area, however. For example, a certain case may not be a crime in local legislation but may be a crime in the foreign country. This would stimulate direct cross-border contact between the local CERT and the foreign LEA.

Direct cross-border cooperation is noted to be faster than going through the local LEA, but there are some legal aspects to this as well, which may mean that going through the local LEA is the only possible way. Cross-border communication can still take place in this instance, but only in the preparation phase of the case. Information gathered in this phase should be seen as intelligence, and cannot be used in a court case, for example. The legal aspects are touched on in the next section of this report.

To build international trust, regular meetings are important. Trust is built between individuals meeting each other and is based on both their character and their technical skills.

One factor that makes building trust more difficult is the very different way in which LEAs and CERTs are generally regulated. A trust-building effort might not be enough to tear down these barriers. In some Member States a free LEA–CERT information exchange might need specific changes in the national legislation as well as this trust factor.

4.1.2 Security controls

Most countries require security controls and role-based certifications to work together. Security clearances can, for instance, be necessary as well as physical and logical audits.

4.1.3 Workflows

In general, it is not common to have formal protocols and workflows in place to facilitate cooperation between the different teams, although some countries are currently heading in that direction. The activities that are considered most important by most of the participants are evidence acquisition (and preservation) and containment and disruption of the crime. There is no integration between the workflows of the different teams during the investigation and the forensic phase.

Some CERTs do not have workflows or any kind of protocol about how to handle transfer cases.

4.1.4 Information sharing and communication

Concerning the knowledge sharing and communication tools, most of the teams do not have any case tracking system or any knowledge management tools currently deployed to enhance collaboration between the LEA and CERT team, as the amount of information currently exchanged is still relatively small.

Communication in general between the teams is done mainly through classic media, such as phone and email. Encryption is considered by most teams to be crucial for trustworthy email communication. Physical meetings are still an important way of communicating; meeting the counterparty in person provides an easy way of communicating and builds trust.

A common classification and encryption level of information is valuable and necessary for communication between the teams. In some countries this classification is enforced by law; other teams agree on a common policy.

4.1.5 Statistics

Not all the teams consider integrating the statistics from both CERTs and LEAs as a useful thing to do, as most of the time statistics from CERTs and LEAs have different scopes. An incident for a CERT team might be defined in a totally different way by the LEA team, for example. Hence, at the moment there is not really a correlation of these data.

As a result of this, there are really very few statistics on cybercrime on a global, or even a pan-European, level. It is a difficult exercise indeed to ‘combine’ statistics from CERTs and LEAs; however, doing this could give an important insight into current cybercrime trends and can be considered as an important decision-making tool.

However, most CERT teams do provide early-warning information which LEA teams consider to be highly valuable for their macroscopic view of cybercrime.

4.1.6 Digital forensics and investigation methods

Digital investigation and forensics are provided as a service on an on-demand basis. A higher level of collaboration is considered by the participants to be the way forward to improve both the quality and the speed of results achieved in the fight against cybercrime. Some countries have deployed a cyber-forensics centre, mostly for LEAs.

Currently, digital forensics is mostly used for conventional crime investigations, such as white-collar crime, organised drug crimes, etc. Therefore many of the forensic services are not really experts on network technologies.

Fighting botnets is considered to be a successful case of collaboration between CERTs and LEA. There is, however, still room for improvement in this cooperation. This collaboration should be continued and further improved.

4.1.7 Requests for assistance

It is important for LEAs to know that they can count on the expertise of a CERT for technical assistance in handling certain cases; however, the mandatory handling of criminal cases could damage the agility of the CERT community, which is one of the most valuable assets of the CERT teams. Hence, it is probably not a good idea to make it mandatory to react on a request for assistance. The handling of cases by CERTs on the basis of their best effort can be considered better than making this mandatory. It can be considered to be better to make the handling of cases for CERTs based on their best effort.

Currently, this is a question of national legislation. In general, if law enforcement appoints a CERT member as a specialist, then it is mandatory to provide the LEA with assistance and expertise.

4.1.8 Reporting of cybercrime to LEA

There are valid arguments for and against mandatory reporting when a CERT team comes across a cybercrime case. At least it should concern aggravated cases only. Generally speaking, though, all crime should be reported to the police. Hence, it is strongly recommended that all cybercrime activities be reported to LEAs. Sometimes it is difficult, though, for a CERT to be sure if an incident leads or could lead to a cybercrime case. In this case, it is recommended that they consult the LEA. A good way to handle this problem is to integrate teams, as discussed above. In addition, it should be noted that in many cases of crime only the victim of crime can file the complaint. Depending on the nature of the crime and the law, the victim could be the user or, for example, the operator.

4.2 Legal aspects of the fight against cybercrime

It is clear that the fight against cybercrime, and more particularly the cooperation between CERTs and LEAs, raises some important legal issues. The following sections briefly address some of the legal challenges that CERTs and LEAs might face when cooperating to respond to cybercrime.

The list of legal issues is not meant to be exhaustive, neither are the descriptions complete. The aim of the following paragraphs is to encourage discussion on these issues and on the possible solutions to them.

4.2.1 Fetching data

At the CERT Workshop organised by ENISA and Europol in October 2011, an interesting discussion took place on how data are fetched from a keyloggers' dropzone, which is a data publicly writable directory on a server that serves as an exchange point for keylogger data.

It emerged that this approach varies considerably from country to country:

- in some countries CERTs do not fetch data themselves, but they can do it when they are asked to by the police and if they are acting on behalf of the police;
- in others, the police cannot ask a CERT to fetch data;
- in others, police can accept data from CERTs but cannot ask a CERT to collect the data;
- in others, CERTs can fetch the data but not if they are password-protected;

- in others, CERTs can fetch data, but if the data are password-protected, they fetch data only if the ISP is informed and has no objection;
- in others, governmental CERTs can fetch password-protected data when a critical infrastructure is in danger;
- in others, the intent is crucial, in the sense that if it can be proved that the malware was used for a criminal activity, then it is possible to fetch the data even if they are password-protected;
- in others, CERTs can fetch data locally, but if the data are in another country and the local CERT has contacts with a person in the CERT in the other country, data is fetched through the local CERT.

The issue of jurisdiction is particularly important when discussing how data are fetched. While a CERT fetching data in another country in principle is not seen as a problem, law enforcement operating in another jurisdiction poses problems. Moreover, in general, if the request for information comes from CERTs from another country, the local CERTs can accommodate it and pass the information; on the contrary, if the request comes from a law enforcement agency in another country, this request, in order to be accommodated, must pass via law enforcement channels.

At the CERT Workshop, it was noted that the communication channel 'CERT–CERT' is more efficient than the channel 'CERT–Law enforcement–CERT' and that the information flow CERT–CERT is more agile: the process via law enforcement channels generally takes longer.

4.2.2 Malware

Malware is short for 'malicious software'. It contains pieces of software specially designed to disrupt or contaminate a system or any other kind of abusive behaviour. Software is considered to be malware when there is bad intent by the creator. It is a collective noun for all kinds of malicious programs such as computer viruses, Trojan horses, worms, etc. When organisations come across these programs or contaminated systems, they need to investigate them. One possible way of doing this is running the malware in order to analyse and test it, but this is not straightforward from a legal point of view. Removing the malware on infected machines is another issue. Reverse engineering is another way of analysing malware.

Analysing malware

Sometimes during a cybercrime investigation, it might be useful for a CERT team or a LEA to run a malware. However – as emerged from the discussion at the CERT Workshop in October 2011 – it is not always self-evident whether this is legal, especially in cases where it is not known exactly what the malware does. Although in some countries this might be considered illegal, there might be exceptions specific to security research. In some countries, for example, 'hacking' is admissible if done by authorised bodies and for intelligence purposes (e.g. for the security of the state). Running malware as a means to analyse the effects of the malware generally cannot be done by the law enforcement agency. In some countries, for example, police cannot run malware because this is seen as provocative, unless for example it is run in a private protected and controlled environment. CERTs in most of the Member States can run malware if they have a private network or when they meet special conditions, such as running it in a protected and controlled environment.

Removing malware

The problem of removing malware is that it implies making changes, although sometimes they are relatively small, in the infected machine. It could cause the machine to crash and, secondly, it could possibly also remove important evidence.

It is much easier for industry than for CERTs or LEAs, for instance, to proceed to disinfect a machine from malware, as they can have a civil agreement with their consumers and therefore can do so based on this.

It should be noted, however, that the responsibility for removing the malware lies in the first place with the consumer and in the second place with the owner of the network. CERT and LEAs can advise its removal but in most cases it is impossible for either organisation to effectively do this. Cooperation between CERTs, LEAs and the network owner is another possibility and should be expanded in the future, as it has proved to be effective in the past.

4.2.3 Network-level mitigation

The CERT Workshop discussed the issue of whether operators must block, for example in cases where there is a drop zone threatening individual people but not critical infrastructures. In some countries there are legal provisions according to which operators can be asked by law enforcement to shut down specific end-users for a limited number of hours in order to solve incidents as fast as they can. In other countries, if ISPs are asked to shut down, they have to do so, but there is no deadline for them to do it. It depends very much on the local legislation and on the contractual agreements between the consumer and the ISPs.

In some countries CERTs can give recommendations to ISPs and if they do not follow these recommendations, law enforcement is addressed. Sometimes, when an ISP is informed by CERTs it is required to act because it has been notified of a threat.

Other countries have some sort of gentleman’s agreement between the CERT and the ISPs. These agreements work well; for example notice and takedown. Only in very rare cases is such an agreement not sufficient.

In some countries ISPs voluntarily filter malicious sources.

The question of whether taking down a service is CERTs’ responsibility was addressed: in some countries, if the police ask for it, CERTs can do it; in other countries if the police ask, it is mandatory for the CERT to do it (there is a general provision in the legislation saying that all instructions by the police must be followed).

A good example where CERTs and LEAs worked together was the Taurus Botnet Monitoring Project[11] in the Netherlands. There are many similar good practices and examples.

4.2.4 Notifying victims

In general, CERTs do not go via their LEA counterpart to notify the victims that they are/were contaminated. CERTs usually inform the victims of cybercrime on reporting the crime to the police; in many jurisdictions only the victim of crime can file a complaint, and the CERTs cannot do this in place of the victim.

Often notification is done via the ISPs. In some cases, notification might be done via the banks. In some countries, in certain cases, the security officers of the departments are contacted, instead of directly contacting the victims. Sometimes, even if there is willingness to reach the end-user, this is not possible for practical reasons, as CERTs sometimes do not know the victims, so the service providers need to be contacted anyway.

Sometimes it is not easy to establish which institution is competent (the institution that has the legal authority) to notify the victims. This can be challenging. In general, what is important is that the notification comes from an authority that is trusted (to enhance the trust, e.g. TV channels could be used). Although it is costly and time consuming, writing a formal letter seems in some cases to be the proper way to communicate to the public.

In general, cooperation between CERTs, LEAs and the network owner is recommended to tackle this issue.

When passing on information to victims in another country, especially outside Europe, it becomes even more difficult. In some countries the ISP will not pass information on IP addresses unless requested on the basis of a court order.

The importance of using secure channels when communicating information (in order not to expose the information to an additional risk) should be highlighted.

[11] *The Taurus Botnet Monitoring project is a good example of collaboration where both the High Tech Crime Unit and GOVCERT.NL cooperated to investigate and take down the Win32/Bredolab botnet. The project had three phases: information gathering (on malware, servers hosting control and command), investigation and intervention (GOVCERT.NL helped in taking down servers). The cooperation has led to the takedown of certain parts of the botnet in October 2010. Computers infected with Bredolab got a popup detailing instructions on how to clean their system. Some c&c servers were kept alive though to gather more data and do further analysis on it.*

4.2.5 Exchange of data

When there is collaboration or cooperation between CERTs and LEAs, this always results in some sort of exchange of data.

Different types of data can be distinguished. First of all there is 'traffic data', which is usually understood as information that can be extracted from TCP/IP protocol family headers. They do not identify a service or application at the server or at the client side. Another type of data is information retrieved for example from application logs which may differ from what is called 'incident data' below. The legal issues differ according to the type of data transmitted.

Exchange of traffic data

In some Member States there are no particular problems with passing traffic data (e.g. an IP address) between a CERT and a LEA team, while in other countries CERTs are not able to provide law enforcement with traffic data unless the law enforcement agency has a court order to request this. It depends on the jurisdiction.

IP addresses are considered to be personal data in some countries, and this represents a challenge when they need to be promptly exchanged to respond to (cyber)crime. There is indeed a delicate balance between the need to protect privacy and the need to identify criminals.

As foreseen in its WP 2011, ENISA has carried out a study into legal and regulatory aspects of information sharing and cross-border collaboration of CERTs in Europe.[12] This ENISA study provides more information about the complexity of legal factors surrounding the cooperation of CERTs and identifies some ways to further improve the work of CERTs.

Incident data as evidence

There might be cases in certain countries where there is an incident but not necessarily a crime and that therefore CERTs have to check, based on the data they have, whether there is evidence of a criminal action. In some countries it is possible for CERTs to pass information to the law enforcement agencies to take a decision on whether or not there is evidence of a crime.

In other countries, when the information is provided by the CERT to the law enforcement agency on a voluntarily basis, the police can use it as evidence; but if the police ask for this information, then it cannot be used as evidence and/or intelligence.

Another issue is whether an interview of a CERT officer as an NIS expert could possibly be used as a way to provide evidence; how the CERT officer could be protected as an informant should also be considered in addressing this issue.

[12] *This study is available at* http://www.enisa.europa.eu/act/cert/support/legal-information-sharing

Finally, it is important to note that the way evidence is collected has an influence on its admissibility into court. Good cooperation between LEAs and CERTs, certainly in the field of training, could avoid problems with admissibility by training experts who collect data about the methods that can be used and the legal aspects of evidence collection.

General information exchange

Concerning information flow from law enforcement to CERTs, e.g. on malicious activities, it should be noted that in some countries LEAs are not allowed to share such information with CERTs and that in general CERTs hand information to other CERTs much more quickly, through informal means of communication, than prosecutors from one country to another.

When CERTs provide LEAs with information or other forms of assistance they want to receive some sort of feedback afterwards from the law enforcement or from the prosecutors. Sometimes law enforcement faces a similar situation when they do not receive sufficient feedback from industry or banks, for example. Without feedback it becomes very difficult for teams to actually find out whether what they did was worth it and had the desired effect. All organisations need success stories, e.g. for their sponsors. Sometimes, however, it might take months before a case actually reaches the judicial phase and is decided by the court; therefore, giving feedback to the sources before then might be difficult.

4.2.6 Data retention

In some countries (e.g. the Czech Republic, Germany and Romania) the data retention directive was implemented, but the law transposing the directive was declared unconstitutional.[13]

The absence of an obligation to retain data does not always mean that the ISPs are required to destroy data. Sometimes ISPs, even in the absence of an obligation to retain data, keep the data for statistical and business purpose (technical reasons): such data can be used by the police. However, the data need to be destroyed after some time.

In certain countries there is a general provision that all people, if they are able to do so, must cooperate with law enforcement agencies.

There is resistance in some countries to transposing the data protection directive (operators are capable of retaining data but they are not willing to do so).

[13] *For more information, see, for instance, the European Commission's Evaluation report on the Data Retention Directive (Directive 2006/24/EC), (COM(2011) 225 final,) in particular the section on 'Decisions of Constitutional Courts concerning transposing laws'. Link: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:EN:PDF*

4.2.7 Specialisation of judiciary in dealing with cybercrime cases

There is an issue of the limited specialisation or non-specialisation of some judges and prosecutors in dealing with cybercrime cases. It can be very difficult to explain to the judges what, for instance, malware is, etc. The observation can be made that sometimes just using different wording to explain the same situation helps.

It is recommended that judges, prosecutors, etc., be given specialised education and training on cybercrime matters. ENISA and Europol should fill the gaps where such education is not available, as some initiatives are already in place.

In the past the law curriculum did not cover IT law, but nowadays more and more IT law courses are available; this should be highlighted as a positive trend.

4.3 Cooperation and practical aspects of the fight against cybercrime

This section focuses on cooperation and the practical aspects of the fight against cybercrime. It addresses the current level of cooperation between CERT and LEA communities across Europe and ways of improving this collaboration. It also focuses on the current levels of satisfaction in both CERTs and LEAs about the degree of cooperation between both communities and how this could be improved.

There is a clear difference between the collaboration of CERTs and LEAs on a national, European and on an international level. Some countries presently have good collaboration on a national level, but rarely on a cross-border level. But it may be the case that cross-border collaboration between CERTs and LEAs is not at all necessary. LEAs have their own networks and so do CERTs. LEAs could reach a CERT in another country, for example, via their local national/governmental CERT. It may seem as a bottleneck but in practice this scheme seems to work.

Most of the well-established teams already cooperate in some form with their counterpart in CERTs or LEAs. Generally this cooperation takes the form of informal information exchange, but a more formal way of cooperating also exists when, for example, technical investigations need to be performed and when CERTs testify in courts. CERTs also provide training on more technical topics to LEAs. LEAs could also train CERTs on legal matters, but in practice this does not seem to take place very often.

It is clear that cooperation and collaboration should be encouraged, as it provides added value for both communities. The focus for this collaboration between CERTs and LEAs should be on the national level. On the one hand, CERTs have an interest when incidents lead to actual criminal cases as this results in fewer incidents and makes their network safer. For LEAs the collaboration with CERTs gives them access to a network of CERTs, which is a large community with far fewer information exchange barriers. For both communities this leads to a safer Internet, so that collaboration is a win-win situation. On top of this, LEAs frequently suffer from a lack of resources. The number of staff and resources of LEA teams dealing with cybercrime are not increasing at the same pace as cybercrime. If CERTs could help them in an appropriate way, this could be an efficient use of resources.

4.3.1 Services

What services can CERT and LEA teams provide to each other and which services can be expected? Most of the countries do not think it is necessary to define a concrete service catalogue, as flexibility is highly valued. Teams should be able to adapt to on-demand needs and be flexible.

Incident response for containment and disruption in particular are highly valuable, as well as the contact network of the CERT community. This section covers some of the services CERT and LEA teams could provide to each other.

It is important, however, that both teams know what can be expected from the other team, although probably this should not really be made as explicit as a service catalogue.

CERT supporting LEA

So, how can CERTs support their LEA counterpart and do this in an efficient way? What are the needs of LEAs in their fight against cybercrime?

An important aspect that was constantly repeated is the need for training. LEAs are asking for training on more technical topics. The staff members of CERTs mostly have high-level technical skills and could share their knowledge with LEAs on a regular basis. This would help them acquire a common language so that both communities understand each other. This would facilitate information exchange about emerging threats. CERTs could share their knowledge about current trends, threats and early warning for cybercrime activities, for example with intelligence gathering and statistics.

CERTs could also help LEAs in solving particular cases with their technical competence. This could also include evidence examination and data mining.

As already mentioned, LEAs could, via the national/governmental CERT, use the network of the CERT community to carry out cross-border information exchange which would otherwise be impossible, or would be delayed by administrative and legal issues.

CERTs could also share their resources; not only human, but also software and hardware; for example digital forensics software and hardware.

National CERTs in general have a good overview and have contacts with different organisations, both in the private and public sector. As they have a good network they could function as an information broker during LEA investigations.

Reference here could be made to RFC 2350[14] as an overview of services that could be expected from CERTs. However, it should be noted that there are some specific services that CERTs would only do for LEA teams, such as digital forensics, etc.

LEA supporting CERT

LEAs have a different background and competences from CERTS. They can advise and assist the CERT teams with legal support as CERT teams in general do not have much expertise in this field.

They could give training on legal issues, but also on forensic procedures and how to handle possible future evidence. In this respect they could support CERT teams in obtaining evidence relevant for incident handling and forensic investigation.

4.3.2 Exercises

Some participants had performed periodic operational coordination exercises/tests between LEA and CERT teams, but most of the time this is not done in practice as it is done through the real work cases.

4.3.3 Formal vs. informal cooperation

When it comes to the form of cooperation participants use most often, both formal (e.g. defined PoC, cooperation agreements in place) and informal (e.g. trusted network, personal knowledge of your peers) forms of communication are used with their respective counterparts. Both have their pros and cons. Formal requests are obligatory for evidence gathering. It was strongly expressed by the stakeholders that one form of communication should not be chosen in preference to the other; instead, both forms should be used. Trust and trusted networking is the foundation of good collaboration and information sharing.

In the future, a more mature form of cooperation is needed, arising from both formal and informal networking models. Mainly it is the formal type of cooperation that needs to be improved; hence, management support should be gained to allow resources to be devoted to this collaboration.

Informal collaboration is most common between CERTs and LEAs and is very efficient from the operational point of view, although formal collaborations are necessary to help both teams to use information/investigation evidence safely.

Another aspect of this is that informal collaboration most of the time is based on personal relationships between employees of the different organisations. This brings with it a continuity challenge when employees change jobs or leave the organisation.

[14] http://www.ietf.org/rfc/rfc2350.txt

4.3.4 Meetings

Meeting people from CERTs and LEAs is very important, but the number of conferences and seminars may be excessive considering the average CERT team size. This is not cost effective and it is time consuming. It would be better to have fewer meetings, but to make the most of these meetings and go deeper into the topic (e.g. working group model). The aim should be to coordinate meetings as much as possible to reduce travel and time costs.

Nowadays, meetings and conferences are mostly focused on informative presentations. A good alternative to that is working sessions and hands-on training during these conferences.

4.3.5 Feedback

A bilateral information exchange between CERTs and LEAs is needed. Collaboration and information exchange should ideally take place in both directions. CERTs would welcome some feedback from LEAs when providing LEAs with information, cases or assistance. When no feedback is given to the CERTs this is very demotivating and does not encourage future collaboration.

However, at present most CERT teams get feedback at the end of the specific investigation, which could well be after a couple of years. It was stated that the CERT community should understand the obstacles from the LEAs' point of view and that LEAs are simply not in a position to give full feedback earlier.

LEAs could, on the other hand, try to give some limited feedback during the investigation, certainly at the beginning of the investigation, so that the CERT team knows how to react to questions from the media, for instance.

4.3.6 Europol and Interpol

Current practice is that CERTs do not communicate directly with Europol and Interpol. CERTs should not form yet another hub between the different police organisations, as they already have Interpol and Europol. CERTs must in the first place communicate with their local police organisations.

There is no such thing as an 'international LEA' that carries out investigations on a cross-border level. Judicial processes like the investigation of a criminal case have to be initiated by the LEA that has the jurisdiction.

4.3.7 24/7 model for cybercrime info request handling

Cybercrime is a 24/7 international problem and not a '9 to 5' (business hours only) national problem. Considering how cybercrime is evolving and how incident response requires multiple organisations in different time zones to collaborate, 24/7 could be seen as a strong requirement to cover the needs of cooperation between CERTs and LEA. It is a must-have if organisations decide to exchange operational cybercrime data. If only tactical information is being exchanged then there is not really a need for 24/7 support.

On the other hand, some organisations believe that crimes requiring this type of effort tend to be long-term operations, which hence also require long-term investigations.

4.3.8 Single point of contact

A lot of the stakeholders think national/governmental CERTs should act as a point of contact towards national/local LEA and the international CERT community. In this scheme, foreign LEAs should access the national/governmental CERT via the national/local LEA or respective n/g CERT. The latter is probably the better option to avoid legal issues.

Others distinguish between incidents and criminal cases. The national CERT is in this respect the only point of contact in a country for NIS incidents. When criminal cases are involved, the national/local LEA should be the contact point.

In effect, CERT–CERT contacts do work, based on the CERT community contacts. People do know who to contact. The same goes for LEA–LEA contacts, as they have the LEA contacts in Europe via Europol and go via INTERPOL on an international level.

On a national level, in most countries, there is also not a problem. In emergency cases, both sides know who to contact on the other team.

Cross-border LEA–CERT or CERT–LEA communication is a different matter. In general, trust is essential, which means that the first person you contact is the person you know and trust. A single point of contact is necessary for cases where such a trust relationship has not yet been established.

5 Organisations participating and contributing to this first draft

The organisations listed here are those that were involved in the process of drafting this report. It is in no way meant as an exhaustive list of organisations involved in the fight against cybercrime. It is intended rather as a very short description for reference purposes. In future versions of this document this list could be made more exhaustive and complete.

5.1 ENISA

The European Network and Information Security Agency (ENISA)[15] 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. ENISA's activities in the area of fighting the cybercrime in 2011 focused on creating a first collection of practices in addressing NIS aspects of cybercrime, more specifically in the cooperation of n/g CERTs with LEAs. These efforts will continue in 2012.

5.2 Europol

Europol's Cybercrime Centre ensures a high level of expertise throughout the EU Member States and beyond, through the coordination of investigations, development of cybercrime training and the delivery of operational support and analysis in the cybercrime area.

Specifically, the cooperation with the CERT community and the Internet industry is seen as an important topic, because of the need for a coordinated response in large cross-border cybercrime cases or, even more specifically, large electronic attacks.

5.3 Interpol

Interpol[16] is the world's largest international police organisation, with currently 190 member countries. Interpol's General Secretariat facilitates coordination on cybercrime investigations but does not itself conduct any operational investigations. Interpol's cybercrime programme focuses on training and operations and is keeping up with emerging threats.

[15] http://www.enisa.europa.eu/

[16] http://www.interpol.int/

5.4 Eurojust

Eurojust[17] is a judicial cooperation body created to help to provide safety within an area of freedom, security and justice.

Eurojust was set up[18] in February 2002 to improve the fight against serious crime by facilitating the optimal coordination of investigations and prosecutions covering the territory of more than one Member State with full respect for fundamental rights and freedoms.

5.5 European Commission

The European Commission[19] (EC) is one of the main institutions of the European Union. It represents and upholds the interests of the EU as a whole. It drafts proposals for new European laws and manages the day-to-day business of implementing EU policies and spending EU funds. The EC is active in the fight against cybercrime on various levels. The EU Internal Security Strategy ('Towards a European Security Model') sets out the challenges, principles and guidelines for dealing with security issues within the EU and addresses cybercrime.

5.6 CERT-EU

The EU Institutions set up a Computer Emergency Response pre-configuration Team (CERT-EU)[20] on 1 June 2011. This team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee) and ENISA (which represents all EU agencies).

5.7 NATO NCIRC/TC

NATO Computer Incident Response Capability – Technical Centre (NCIRC TC)[21] is the Tier 2 of the NATO Computer Incident Response Capability (NCIRC). The NATO Information Assurance Technical Centre (NIATC) provides operational CSIRT support to the NATO CIS community.

[17] http://www.eurojust.europa.eu/

[18] Council Decision 2002/187/JHA

[19] http://europa.eu/about-eu/institutions-bodies/european-commission/index_en.htm

[20] http://cert.europa.eu/

[21] http://www.ncirc.nato.int/

5.8 NATO CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)[22] was established on 14 May 2008, in order to enhance NATO's cyber defence capability. It is located in Tallinn, Estonia. The Centre is an international effort that currently includes Estonia, Latvia, Lithuania, Germany, Hungary, Italy, Poland, Slovakia, Spain and the USA as Sponsoring Nations.

5.9 TF-CSIRT

TF-CSIRT[23] is a task force, supported by TERENA[24] and with funds from the GN3[25] project, that promotes collaboration between CSIRTs at the European level, and liaises with similar groups in other regions.

5.10 EU FI-ISAC

The FI-ISAC in Europe (Financial Institutions – Information Sharing and Analysis Centre) was established in 2008 with the aim of building a network between financial institutions, law enforcement agencies and national CERTs. The idea was to share information on incidents, threats, vulnerabilities and good practices.

[22] http://www.ccdcoe.org/

[23] http://www.terena.org/activities/tf-csirt/

[24] http://www.terena.org/

[25] http://www.geant.net/pages/home.aspx

6 How do we improve cooperation in practice in the short term?

Many of the stakeholders would like to see closer collaboration between ENISA and Europol in order to improve collaboration between CERTs and LEA in fighting cybercrime.

ENISA is the organisation that helps to build a trusted network between CERTs and LEA and also coordinates the establishment or sharing of good practice between teams.

The following domains have been raised by stakeholders as possible fields where ENISA could help in the fight against cybercrime:

- unified standard procedures
- contact database
- regular workshops and training
- material for exercises and training
- best practices on workflows
- awareness raising activities from both the CERT and LEA community
- clarify the roles of both communities in the fight against cybercrime
- provide information exchange methods and tools for both communities

Overall it could be said that in countries where there is little collaboration between CERTs and LEAs, ENISA could play a role as a broker between both communities to enhance their collaboration, and to compile material which will support this process. In countries where such cooperation is already taking place, ENISA's role may be the promotion of joint training (both on a national and cross-border level), providing exercise material and keeping a contact database up to date. Best practices should also be promoted by ENISA and ENISA should support the European Commission in its aim for a harmonised legal framework for the EU on cybercrime matters.

7 Conclusions / Recommendations

7.1 Conclusions

- Trust is key to proper cooperation between CERTs and LEAs. A good way of establishing trust is by integrating both teams. This can be done through internships, but also in a variety of other ways, such as establishing a cybercrime coordination body.

- Any legal hindrances preventing CERT-LEA collaboration should be recognised. Overcoming these legal obstacles should be made a priority.

- Both CERTs and LEAs can profit from the services provided by the other team. However, in general, most teams do not like to formalise this into a service catalogue, and prefer to work on an on-demand basis.

When cooperating, special care should be taken about protocols, security clearances, physical security, etc.

- Concerning statistics, most teams do not really see an added value in putting together the statistics from both teams. Both communities have a different scope, so statistics are difficult to merge.

- Most teams think that both formal and informal information exchange and collaboration should co-exist.

- Collaboration should be bilateral. Information should flow in both directions in order to encourage the CERT community to keep on cooperating.

- When sharing information and cooperating cross-border, legal aspects should be taken into account.

- The approach to fetching data, running a malware, keylogging and passing data between CERTs and LEAs, varies from country to country and it also depends on the legal framework of the country.

- Generally CERTs do not go through law enforcement agencies to notify victims of cybercrime and CERTs inform the victims on reporting the crime to the police; in many jurisdictions only the victim can file a complaint.

- When handling computer incidents, cooperation with other actors, e.g. ISPs, is particularly relevant. In general, if a request for information comes from a CERT in another country, the local CERT can accommodate it and pass on the information; on the contrary, if the request comes from a law enforcement agency in another country, this request in order to be accommodated must pass via law enforcement channels.

7.2 Recommendations

7.2.1 CERTs and LEA cooperation

It is recommended that CERTs should not form yet another hub between the different police organisations, as they already have Interpol and Europol in place. CERTs must in the first instance communicate with their local police organisations.

7.2.2 CERT and LEA meetings

Currently there is a lack of opportunities for CERTs and LEAs to meet. There should be a focus on national-level meetings. For the time being, ENISA/Europol workshops/meetings, such as the ENISA Workshop ‘CERTs in Europe’ which took place on 3 and 4 October 2011 in Prague, Czech Republic, should be sufficient to cover the international aspects of this collaboration.

Cooperation between conference and meeting organisers should be encouraged and meetings should be coordinated as much as possible, to reduce travel and time costs to the minimum.

7.2.3 24/7 model for cybercrime

We recognise the importance of a 24/7 model; however, the cases where 24/7 availability is really needed are in practice very rare. Most teams face this situation at most about twice a year. From an economic point of view, this might hence not be the best option as it is very expensive to operate and maintain. It is instead recommended that emergency cases be dealt with on an ad hoc basis.

7.2.4 Mitigation

For mitigation of cybercrime, it is recommended that national law is made clearer and that exceptions are made for CERT teams if necessary. ‘Gentlemen’s agreements’ between CERTs and ISPs have also proved to be valuable. Hosting providers should try to introduce an ‘acceptable use policy’. This is already current practice but should be more widespread.

7.2.5 Education

It is recommended that judges, prosecutors, etc., be given specialised education and training on cybercrime matters. ENISA and Europol should fill the gaps where such education is not available, as some initiatives are already in place.

It is extremely important that these people are well educated on this topic as they have a decisive role in the investigation and prosecution of cybercrime. The initiatives that already exist could be good partners for ENISA and Europol in the future.

7.2.6 Formal vs. informal cooperation

A more mature form of cooperation is clearly needed, arising from both formal and informal networking models, as both models have their advantages.

7.2.7 Trust

In the end, collaboration and informal cooperation between teams is based on trust between members of teams, and more particularly on trust between individual employees of the CERT and LEA teams. It is important that those people know each other and that they meet face to face. Both teams should make an effort to overcome the distance.

7.2.8 Requests for assistance

It is undoubtedly important for LEAs to know that they can count on the expertise of a CERT team for assistance in handling certain cases; however, the mandatory handling of criminal cases could damage the agility of the CERT community, which is one of the most valuable assets of CERT teams. It is not recommended to make the response to a request for assistance mandatory by law.

7.2.9 Data protection

It is recommended that data protection authorities be asked for permission to handle IP addresses and bank account numbers, for instance. It might be the case that there is no need to change the law and that this is already possible.

7.2.10 Statistics

Although it is considered to be a difficult exercise to 'combine' statistics from CERTs and LEAs, correlating their statistics could give an important insight into current cybercrime trends and could be considered as an important decision-making tool.

7.2.11 Reporting of cybercrime to LEAs

Generally speaking, all crime should be reported to LEAs. Hence, it is strongly recommended that all cybercrime be reported to the appropriate LEA.

7.2.12 Starting cooperation

As CERTs and LEAs tend to be very different organisations with different roles and priorities, it can be difficult to initiate cooperation. It is very important, though, to make start on this collaboration, even if it is only minor at first.

8 Annex I: Questionnaire on NIS aspects of cybercrime

1. If you are CERT and cooperate with LEA (or vice versa), please describe the form, content, added value of the cooperation (e.g. information exchange by email, meetings, trainings, etc.)

2. Are you taking part in any national/international, regional, cross/border initiatives fighting cybercrime? Which ones? Do you cooperate directly with Europol or Interpol on any (national or cross-border) cases?

3. Should CERTs support LEA in the fight against cybercrime? If yes, how? If no, why not?

4. Which operational obstacles exist for CERTs to support LEA in the fight against cybercrime and how could they potentially be overcome?

5. Which are the main legal provisions applying when CERTs support LEA in the fight against cybercrime?

6. According to your opinion which (national/cross-border) legal/regulatory solutions would improve this process?

7. How important is a 24/7 model for cybercrime info request handling (Cybercrime Center/Real-time cooperation between CERTs and LEA, …)? If important, what would be the most efficient cooperation model in this regard?

8. Should the national/governmental CERT act as a single point of contact in a country for any LEA requests on NIS aspects of cybercrime? If yes, what are the advantages of such an approach? What should be the responsibility of the n/g CERT (or any other CERT in the country) in the fight against cybercrime (coordinating role, executive role, …)?

9. In your opinion, which way of collaboration, formal or informal, is used the most in collaboration between CERTs and LEA? In practice, which one would be the most efficient?

10. What do you think should be the role of ENISA in improving the collaboration between CERTs and LEA in the field of cybercrime? How can ENISA contribute to improve the fight against cybercrime?

a. workflows

b. unified standard procedures

c. contacts database

d. awareness raising of activities from both communities

e. clarifying roles of both communities

f. regular trainings

g. material for exercises

h. other…

9 Annex II: Questions in preparation of the workshop

9.1 Operational/legal questions

1. Suppose there is a keyloggers' dropzone (publicly writable directory on a server residing in the Internet that serves as an exchange point for keylogger data) in your organisation's jurisdiction. Could your organisation fetch the data from this dropzone over the net? a) if the data is not password protected? b) if the access control requires credentials that are hardcoded into a malware we have? If the data seems to reside in a netblock (group of IP addresses) allocated to another country. Would this change the situation or not? How would we feel if a LEA/CERT from another country would fetch data from our network space?
2. Suppose there is a command-and-control server (C&C) in your organisation's jurisdiction and your organisation has a very good malware analysis report. Could your organisation impersonate as a bot in order to gather intelligence on the C&C and on the botnet herders? If we can, to whom could we pass on the information acquired? Other CERTs/LEA? Identified victims? ENISA or other organisation's role?
3. Your organisation gets keylogger data from a foreign collaborator. The file contains traffic/log data, real names, credit card data, credentials to known services. Who would you notify? Individual victims? Service providers? Could we pass the data to LEA/CERT? ENISA or other organisation's role? Are there specific restrictions such as conditions on passing on personal data or traffic data (say ip + time stamp)?
4. Your organisation gets knowledge of an aggravated crime against a company dealing with critical infrastructure. Whom can we notify? Direct victims? Indirect victims? Other CERTs/LEA? ENISA or other organisation's role?
5. There exist any legal/regulatory obstacles hindering the cooperation between CERTs and LEAs, how could ENISA support CERTs and LEAs to overcome them?
6. Are there any other specific legal problems we see at the moment in the CERT + LEA collaboration inside our own jurisdiction or cross-border?
7. Can we give either mandatory commands or recommendations to network connectivity providers in order to filter traffic related to a 'cyber-attack'?
8. Can we postpone a takedown if we knew that the LEA had an ongoing operation? Can we exchange this kind of operational information or not with our local LEA?
9. We have loads of traffic data of a large man-in-a-browser online banking case. Could we take data requests from foreign LEA directly, or would we rather take the requests only from our local LEA who would first verify the foreign counterpart?

9.2 Operational/technical

1. Have you agreed on an operational workflow to ask for support, respond to requests or manage case transfers? Do you know what the LEA/CERT team could do for you (i.e. service catalog)? Is it 24x7? Does your CERT/LEA team have any kind of internship program in place? Do you have a liaison from your team working physically with your partner?
2. Do you need any background checks or security clearance certification to work with your LEA/CERT team? If not, have you considered deploying such kind of controls? How do you build trust?
3. Is there any specialist certification or knowledge accreditation related with IT Security needed to work on your team? Does your LEA/CERT encourage team members to achieve them?
4. Do you have any information sharing or knowledge management tool in place? If yes, are you sharing it partially/completely with your LEA/CERT team? If not, why not?
5. Is your team providing early-warning information about relevant incidents/investigations, cybercrime groups or current threats/trends to CERT/LEA? If yes, do you provide this information proactively or just on-demand? If not, why not?
6. If you are a CERT, do you provide malware/incidents/crimeware intelligence reports and statistics to LEA? If you are a LEA, do you correlate that information with your cases and do you provide feedback of your findings? If yes, how do you provide this, via what channels?
7. Do you have unified operative standards or procedures between your LEA/CERT team? If yes, do you consider them strict or are they somewhat flexible to adapt to daily operative needs?
8. Do you usually consider your corresponding LEA/CERT team to participate or be involved in any of your incident response/investigation workflows? i.e. triage, containment, search & seizure, forensics, …
9. Which are the common ways of communication between both teams? Do you have any security requirements in place (classification, encryption…)? i.e. email, audio/video conference, instant messaging, physical meetings…
10. Do you provide digital forensics/investigation services to your CERT/LEA? Are you sharing any kind of software/hardware/facilities for incident response/forensics amongst both teams? If not, why not? i.e. forensics lab, evidence acquisition devices, interception probes…
11. Is there any case or task management tool in place to keep track of activities? Have you deployed collaboration tools to ease working together or support LEA/CERT team operations? i.e. ticketing systems, remote desktop sharing, remote evidence gathering…
12. Is there any tool or service that could be implemented to improve the quality of the incident response/case investigation?
13. Does your CERT team provide consultancy or R&D on-demand for LEAs and vice versa?

9.3 Cooperation/practical

1. Are you satisfied with the current level of cooperation between CERTs and LEAs or could it be improved? What in particular needs improvement? Is there a difference in the cooperation at national level, between the EU Member States, and at international level?

2. Is your team understanding the technical side of the Internet technologies/ the legal requirements behind the investigation well? A there any former law enforcement people, or people with legal investigation experience in your team? Are there any IT professionals in your team?
3. Do you perform periodic operational coordination exercises/tests between your LEA/CERT teams? If yes, how often do they run?
4. What form of cooperation do you use most frequently? Do you feel trusted contacts are important or do you consider that formal cooperation is sufficient? What are your best practices in creating this 'trusted network'.
5. Provided you are from LEA, when and where are CERTs most efficient?
    a. informing you and providing details on incidents
    b. helping to co-relate various events and incidents
    c. to securely outsource some forensics works to?
6. In case you are from a CERT, when, where and how are LEAs most helpful to you?
    a. to hand over the information which you have gathered during your work and which needs a legal assessment?
    b. to feed various events to them in hope they will see the bigger picture and will connect these events into an investigation
7. What are according to you, the roles for ENISA to support fight against cybercrime?
    a. providing the best practices and on what subject exactly?
    b. facilitate better cooperation between the CERT and LEA communities – how?
    c. Anything else?
8. Do you have clearly defined a Point of Contact (PoC) for your LEA/CERT? Is there any agreement in place that states the level of integration and collaboration?
9. Do you perform periodic technical training where both teams are involved? Is there any meeting/workshop to cover current threats and trends for these specific needs?
10. Have you developed a common report about cybercrime activity within your member state using combined data from CERT/LEA teams?
11. Are you using your CERT/LEA team as a key player for reaching trusted peers to deal with requests at your constituency (public administration, private sector)? What about international requests?

10 Annex III: Abbreviations

CCD COE – see NATO CCD COE

CERT – Computer Emergency Response Team

CII – Critical Information Infrastructure

CIIP – Critical Information Infrastructure Protection

CIP – Critical Infrastructure Protection

CIS – communication and information system

CSIRT – Computer Security Incident Response Team

DDoS – Distributed Denial of Service

DNS – Domain Name System

DPA – Data Protection Authority

DRD – Data Retention Directive

ENISA – European Network and Information Security Agency

EU – European Union

FI-ISAC – Financial Institutions – Information Sharing and Analysis Centre (Europe)

FIRST – Forum of Incident Response & Security Teams

ICT – Information Communications Technology

IP – Internet Protocol

ISP – Internet Service Provider

LEA – law enforcement agency

MS – Member State of the European Union

NATO CCD COE – NATO Cooperative Cyber Defence Centre of Excellence

NCIRC TC – NATO Computer Incident Response Capability – Technical Centre

NIS – network and information security

PoC – point of contact

TERENA – Trans-European Research and Education Networking Association

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu