enisa
European Network and Information Security Agency

Give and Take

Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime

Legal, Regulatory and Operational Factors Affecting CERT Co-operation with Other Stakeholders

Acknowledgements

We would like to thank the project team from commissioned by ENISA to undertake this study, in particular Neil Robinson and Luke Gribbon (RAND Europe), Hans Graux (time.lex), Peter Burnett (Quarter House Ltd) and Alice Reeves.

We would also like to thank the members of the informal Expert Groups established by ENISA to provide support for the review of this study, including Andrew Cormack (Janet), Vincent Danjean (INTERPOL), Wout de Natris (De Natris Consult), Serge Droz (SWITCH), Carlos Fragoso (CESICAT), Bruno Halopeau (Europol), Dr. Zoe Kardasiadou (Hellenic Data Protection Authority), Jan Kolouch (CESNET), Triin Nigul (CERT-EE), Jaap van Oss (Europol), Anto Veldre (CERT-EE) and Dan Tofan (CERT-RO). Not all members of the informal Expert Groups wished to be mentioned.

Further acknowledgement should be given to the ENISA colleagues who contributed with their input to this study, in particular: Dr. Silvia Portesi, Andrea Dufkova, Nicole Falessi, Romain Bourge, Cosmin Ciobanu and Lauri Palkmets.

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

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

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

[Deliverable: Nov. 2012]

Contents

Executive Summary 1

List of acronyms 4

1 Introduction 6

1.1 Motivation for this study 7

1.2 Target and scope of this document 8

1.3 Methodology 8

2 Background 10

2.1 Defining cyber security and cybercrime incidents 12

2.2 Understanding the impacts of incidents 14

2.2.1 Cybercrime 14

2.2.2 Incidents of national interest 15

2.3 Stakeholders that CERTs interact with 16

2.4 Policy initiatives in this domain 17

2.4.1 ENISA's activities in supporting CERT Co-operation 19

2.4.2 European policy as regards co-operation with Law Enforcement Authorities (LEAs) 21

2.5 National level initiatives 22

2.6 Examples of challenges concerning CERT-LEA co-operation 22

2.7 Strategic level challenges 26

2.7.1 Different definitions of cybercrimes/attacks 26

2.7.2 Different meaning of information sharing 27

2.7.3 Different character of community 27

2.7.4 Different objectives of each community 28

2.7.5 Different types of information 29

2.7.6 Different directions of requests 29

3 About this study 31

3.1.1 Responses from CERTs 31

3.1.2 Responses from Law Enforcement Authorities 32

3.1.3 Responsibilities of respondents 32

3.1.4 Profile of respondents....32
3.2 Experience of information sharing....33
4 Legal factors affecting interactions between CERTs and other types of organisation – empirical findings....36
4.1 CERT categorisation – legitimacy, scope, remit and competences....36
4.2 CERTs as evidence holders....38
4.3 Legal pitfalls of data sharing....39
4.4 CERTs in the prosecutorial process....40
4.5 Legal know-how and awareness....41
4.6 Laws as a barrier to receiving information....48
4.7 Practices employed by CERTs to address legal factors....49
4.8 Impact of legal challenges....51
4.9 Views from the Expert Group meeting on the importance of legal and regulatory factors....53
4.10 Conclusions on legal and regulatory factors....54
5 Operational Factors affecting CERT co-operation with other stakeholders – empirical findings....56
5.1 Governance....59
5.2 Processes....60
5.3 Personnel and Training....62
5.4 Tools and technology....63
5.5 Information....63
5.6 Existence of collaboration and supporting mechanisms....64
5.7 Operational barriers to information exchange....67
5.8 Information exchange standards....68
5.9 Views on the importance of operational factors....69
5.10 Conclusions on operational factors....70
6 Conclusions....71
6.1 Different factors affect CERTs on their path to maturity....71
6.2 Conclusions and priorities for addressing legal, regulatory and operational factors....71
6.3 Priorities for further support....72

7 Recommendations 74

7.1 Training 74

7.2 Structures 74

7.3 Facilitation & collaboration 75

7.4 Best Practice development 77

7.5 Harmonisation and clarification of legal and regulatory aspects 78

Executive Summary

In 2010 ENISA started its support for operational collaboration between the Computer Emergency Response Teams (CERTs) in the Member States on the one hand and Law Enforcing Agencies (LEA) on the other hand. Various activities have since been launched, including stock takings of legal and operational obstacles that prevent collaboration, advice resulting from that, workshops that brought together members of both communities, consultation with members of both communities, etc. It was soon realised that the process of trust building, tackle obstacles together, discussion and finally working together would need time and active, continuous support from ENISA, CERTs and LEAs, and that ENISA just embarked on a long-term trip to achieve its goals.

The document at hand constitutes a "work in progress", a snapshot of the current status of ENISAs support for CERTs and LEAs, and includes good practice and recommendations for both communities. It must be clear that while we may already be several steps closer to a smoother collaboration, we need to continue our common efforts to reach that goal.

About this document

This document contains a Good Practice Guides concerning co-operation between Computer Emergency Response Teams (CERTS) and other stakeholders, primarily Law Enforcement Authorities (LEAs) within Europe.

As Europe is increasingly dependent upon cyber-space, various types of misuse and incidents put at risk the possible economic and social benefits that we stand to gain. Examples include botnets which can be used to perpetrate a variety of cyber-crimes, but also hacking of organisational networks, frauds and other types of 'phishing' and attacks against Critical Infrastructure such as energy, water and transportation systems.

Increasingly, to deal with a variety of types of incidents affecting the confidentiality, availability and integrity of information and communications technologies and cyber crimes, CERTs are required to collaborate with LEAs.

This collaboration can be affected by the differing interests of both types of organisation. CERTs, being technical in nature, are focused on addressing issues relating to information systems. LEAs, by comparison, are concerned with a different range of activities where they suspect or there is evidence that a crime has been committed. It may be difficult with such crimes, such as fraud committed through cyberspace, to determine whether the crime involved the alteration, denial or compromise of information or information systems.

In carrying out their activities, CERTs may interact with a wide variety of stakeholders including other CERTs, other national/governmental CERTs, domestic law enforcement or intelligence agencies, national cyber-security centres and managed security service providers. They may also interact with foreign law enforcement or intelligence organisations and international organisations like Europol or Interpol.

There is little published research on co-operation between CERTs and LEAs –it is only by reviewing operational practice and consulting practitioners, that it is possible to identify how

differences between the two communities may affect collaboration. We identified several high level challenges affecting collaboration between the two communities, some of which are described in the table below.

	Computer Emergency Response Teams (CERTs)	Law Enforcement Authorities (LEAs)
Focus on different definitions of cybercrimes/attack	Unintentional incidents; attacks against the confidentiality, availability and integrity of ICT	Where there is evidence or suspicion of a crime (including fraud or crimes where the confidentiality, availability and integrity of ICT systems has not been affected)
Character of each community	Informal, problem solving based	Procedural, rules based
Objectives of each community	Remediation	Prosecution
Direction of request	Inward (CERTs more likely to have to respond to requests)	Outward (LEAs more likely to transmit requests)

In order to investigate these issues further, ENISA, in the context of its ENISA's 2012 Work Programme called for:

> *"concrete steps to assist CERTs to improve their collaboration and information exchange with law enforcement bodies tasked to prevent and fight cybercrime"*

As part of this study, we identified a number of legal and regulatory factors. As per the 2011 study "A Flair for Sharing – Legal and Regulatory Barriers for Cross Border CERT Co-operation"[1] we found from responses to an online questionnaire that a discrepancy exists between the awareness of relevant national laws compared to international legal frameworks (such as EU wide directives or the Council of Europe Cybercrime Convention). Participants in the online survey indicated that laws governing the protection of personal data were primarily seen as a factor influencing information sharing.

Regarding operational factors, there were a number of reasons identified as playing a role in hindering information exchange and collaboration. The most important reasons given for denying a request were 1) insufficient/inappropriate detail, 2) issues of security clearance and finally 3) wrong channel / addressee. Concerning the reasons for receiving a denial of a

[1] *ENISA (2011) "A Flair for Sharing: ENISA's study into the legal and regulatory factors affecting cross border CERT Co-operation"*

request, the top three were 1) (unsurprisingly) not sure; 2) wrong channel/addressee and 3) insufficient / inappropriate detail.

Following the online survey, at an Expert Group meeting in Brussels the priority accorded to these factors was tested. Participants of the meeting agreed that privacy and data protection compliance was the most important legal and regulatory issue, followed by the scope and remit of the CERT and definitions of computer and network misuse.

Regarding the operational factors, a different picture emerged, when Expert Group participants indicated that information on role and parameters for co-operation were the most important issues, followed equally by concerns over bureaucracy arising from different / unknown policies and procedures, lack of common standards, lack of clarity on what the other party will do with the information and insufficient or inappropriate detail.

During discussions at the Expert Group meeting it was agreed that some factors are particular to different stages of a CERTs lifecycle, from the early phases (when resources and understanding legal basis might be more of an issue) to later when the CERT is more mature and is fully exposed to the complexities of cross border information sharing (where, for example, awareness of relevant international legal frameworks might be more important).

In order to address these factors, we identified a number of recommendations, under the five main headings of training, improving structures to support information sharing, facilitation of collaboration, good practice development and harmonisation and clarification of legal and regulatory aspects. Specifically, these recommendations covered aspects including the expansion of training between CERTs and LEAs (e.g. by including modules covering how to work with each other in respective training programmes), establishing core competencies and indications of each stakeholder's competencies, capabilities and procedures, disseminating good practice on writing Memoranda of Understanding (MoUs) and evidence sharing agreements and further guidance and clarification for CERTs on tackling data protection issues.

List of acronyms

ACPO – Association of Chief Police Officers

APWG – Anti Phishing Working Group

BKA – Federal Criminal Police Office

BSI – Federal Office for Information Security (DE)

CERT – Computer Emergency Response Team

CII – Critical Information Infrastructures

CIIP – Critical Information Infrastructure Protection

CSIRT – Computer Security Incident Response Team

CWG – Conficker Working Group

DDoS - Distributed Denial of Service

DHS –Department of Homeland Security (US)

DIB pilot – Defence Industrial Base (Information Exchange) pilot (US)

EC3 – European Cybercrime Centre

EG –Expert Group

Europol – European Police Office

f2f – Face to face

FBI – Federal Bureau of Investigation (US)

FIRST – Forum of Incident Response and Security Teams

ICANN – Internet Corporation for Assigned Names and Numbers

ICT – Information Communications Technology

IETF – Internet Engineering Task Force

Interpol – International Police Office

IP – Internet Protocol

ISP – Internet Service Provider

ITU – International Telecommunications Union

IT-ISAC – Information Technology Information Sharing Analysis Centre (US)

JHA – Justice and Home Affairs Council (EU)

LEA – Law Enforcement Authority

MLAT – Mutual Legal Assistance Treaty

MoU – Memorandum of Understanding

MSSP – Managed Security Service Provider

n/g CERT – National/Governmental CERT

NHTCU – National High Tech Crime Unit (NL)

NIS – Network and Information Security

OCSIA – Office for Cyber Security and Information Assurance (UK)

PCSIRT – Product CSIRT

PPP –Public Private Partnership

RAT – Remote Access Tool

RfC – Request for Comments

SOCA – Serious and Organised Crime Agency (UK)

SWITCH – Swiss National Research Network

TF-CSIRT – Task Force Computer Security Incident Response Team (EU)

TI – Trusted Introducer program of the TF-CSIRT

TRANSITS - Training programme for CERTs

1 Introduction

It could be said that cyber space has evolved from a luxury to a necessity as it has become an increasingly important driver for economic growth and societal development across Europe.

However, risks from cybercrime, cyber-attacks against critical infrastructures (such as energy, transport and financial systems) may jeopardise the reliance now placed in cyber space.

For example, according to a recent report[2] by Verizon which analysed 855 cases of data breach investigations from Verizon and a number of law enforcement agencies[3], the number of compromised records stood at 174 million.

A recent Eurobarometer study investigated the levels of concern of European citizens as to cyber security.[4] Around 69% of people feel (fairly or very) confident when using the Internet for banking and purchases, while 29% of users do not. The most common concerns people have raised include third parties taking or misusing personal data and the security of online payments. These responses were answered by respondents in their own words (i.e. no prompted answers were offered as options). Generally, security and personal data concerns are higher in the EU15[5] (43% vs. 28% in the 12 New Member States). Most (73%) EU citizens have heard about online crime in the past year and some Internet users have adjusted their behaviour accordingly. Many citizens (59%) do not feel (very or at all) informed about the risks of cybercrime. Around 12% of Internet users in the EU report have experienced online fraud, while 8% have experienced identity theft. The security of online personal data that is kept by websites is of concern for 72% of citizens and 66% say they are concerned that public authorities do not keep information secure. Most citizens report that they would contact the police if they were victims of cybercrime (85% for identity theft and 78% if they accidentally encountered child pornography).

Tackling these kinds of issue requires the involvement of a number of different types of organisation. Computer Emergency Response Teams (CERTs)[6] (organisations responsible for mitigating incidents and helping their constituencies) and Law Enforcement Authorities (LEAs) (that investigate and prosecute cybercrimes) are two types of organisation, that, with appropriate skills, competencies and processes can play an important role in tackling cybercrime.

---

[2] *Verizon (2012), "2012 Data Breach Investigations Report" available at [http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf] [Accessed 11/10/2012]*

[3] *The Australian Federal Police; Dutch National High Tech Crime Unit; Irish Reporting & Information Security Service; Police Central e-Crime Unit (UK) United States Secret Service*

[4] *European Commission (2012), Flash Eurobarometer, Cyber-security*

[5] *EU-15 refers to the 15 Member States of the European Union as of December 31, 2003, before the new Member States joined the EU.*

[6] *Computer Emergency Response Teams (CERTs) aka Computer Security Incident Response Teams (CSIRTs)*

CERTs may be considered as a key stakeholder in addressing the Network and Information Security (NIS) aspects of cybercrime. They perform an important function in identifying security incidents and helping organisations to protect themselves against cybercrimes but also collaborating with LEAs to help identify victims and suspects and trace malicious activity in cyberspace. Without the work of CERTs, the risks from misuse of information and communications technology could well become significant enough to undermine the opportunity for cyberspace to facilitate economic growth and social development.

CERTs are at the sharp end of the collection of data and cyber-attack intelligence that could help deal with cyber-attacks and help address the NIS aspects of cybercrime. Whether based in government institutions, industrial firms or telecommunications providers, they fulfil an important role by identifying, collating, parsing and where appropriate distributing information regarding network security incidents and events. In some cases, they are expected to work in collaboration with law enforcement to help identify suspects and trace malicious activities through cyberspace.

1.1 Motivation for this study

Policy-makers at both the European and Member State level have increasingly recognised the role that CERTs play in helping to improve cyber-security. Three main EU policy statements have been driving this agenda in Europe: the 2009 Digital Agenda for Europe, the 2009 Communication on CIIP and the 2011 Progress Report on CIIP. In particular, Section 2.3 of the Digital Agenda for Europe outlined that co-operation between CERTs and law enforcement is essential.[7] As foreseen in the 2011 Work Programme, ENISA addressed this with an initial report in 2011 on a first collection of practices for CERTs on addressing the NIS aspects of cybercrime.[8] This specifically focused on their interactions with LEAs. The EU Internal Security Strategy[9] also articulated the need for co-operation between CERTs and LEAs.

In line with this, and as a preparatory step, ENISA and Europol held a joint CERT-LEA Workshop called "Addressing NIS aspects of cybercrime" in Prague in October 2011[10], supported by CSIRT.CZ, at which, for the first time, CERTs and LEAs gathered together for two days to run through scenarios as a way to establish first steps in co-operation.

It was decided in 2012 to further strengthen this work by commissioning the preparation of two Good Practice Guides and further work as part of the 2012 Work Programme to build upon these initiatives. WPK3.3 of ENISA's 2012 Work Programme explicitly noted the need to

---

[7] *COM (2010), "Digital Agenda for Europe", 245 of 19 May 2010*

[8] *ENISA (2011) "Work Programme 2011: Securing Europe's Information Society" available at [http://www.enisa.europa.eu/publications/programmes-reports/work-programme-2011-1] [Accessed 11/10/2012]*

[9] *Communication on the EU Internal Security Strategy (2010) "The EU Internal Security Strategy in Action: Five Steps toward a more Secure Europe; " [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF#page=2] [Accessed 11/10/2012]*

[10] *ENISA (2011), 6th CERT Workshop (Prague): "Addressing NIS Aspects of Cybercrime" available at [http://www.enisa.europa.eu/activities/cert/events/6th-workshop-cybercrime] [Accessed 11/10/2012]*

build upon work in 2011 which identified some barriers and incentives to co-operation and also deepened contacts between ENISA and other communities:

> *"In 2012, ENISA will build on this work, and will propose concrete steps to assist CERTs to improve their collaboration and information exchange with law enforcement resources tasked to prevent and fight cybercrime."*[11]

The 2011 workshop was followed up by a hands-on technical training session in June 2012 in conjunction with Team Cymru[12], hosted by the University of Malta and co-located with the Forum of Incident Response and Security Teams (FIRST) Annual Conference.[13] A further CERT-LEA workshop was held in October 2012 which focused on cybercrime jointly organised with Europol.

1.2 Target and scope of this document

The main intended target audience for this collection of practices are managers, technical staff and legal experts in or representing national/governmental Computer Emergency Response Teams (CERTs) and Law Enforcement Authorities (LEAs). In addition, this report is intended to be of benefit to decision-makers in the Member States responsible for the integration of national/governmental CERTs into the National Cyber Security Strategy and other European and international institutions dealing with the fight against cybercrime (for example Europol and the European Cybercrime Centre). In addition to this, we assume that the document will be of general use in supporting CERTs or abuse teams[14] in better understanding the demands and challenges to collaboration between the CERT and LEA communities.

1.3 Methodology

In order to conduct this study, ENISA commissioned a project team which first conducted background desk research into the literature concerning information sharing between CERTs and LEAs. The team uncovered little peer reviewed literature concerning the challenges of this kind of co-operation in the specific context of CERT-LEA co-operation.[15] The second phase involved an online survey distributed to both CERTs and LEAs through various channels (described in Section 3). In conjunction with the project ENISA convened two Expert Groups

---

[11] *ENISA (2012) "Work Programme 2012: Improving Information Security Through Collaboration" available at [http://www.enisa.europa.eu/publications/programmes-reports/WP2012.pdf] [Accessed 11/10/2012]*

[12] *Team Cymru (2012) available at: [http://www.team-cymru.org/] [Accessed 11/10/2012]*

[13] *24th Annual FIRST Conference on Computer Security incident Handling (2012) available at [http://www.first.org/events/first] [Accessed 11/10/2012]*

[14] *Abuse teams may work in ISPs and are responsible for handling reports of abuse of the ISPs own network*

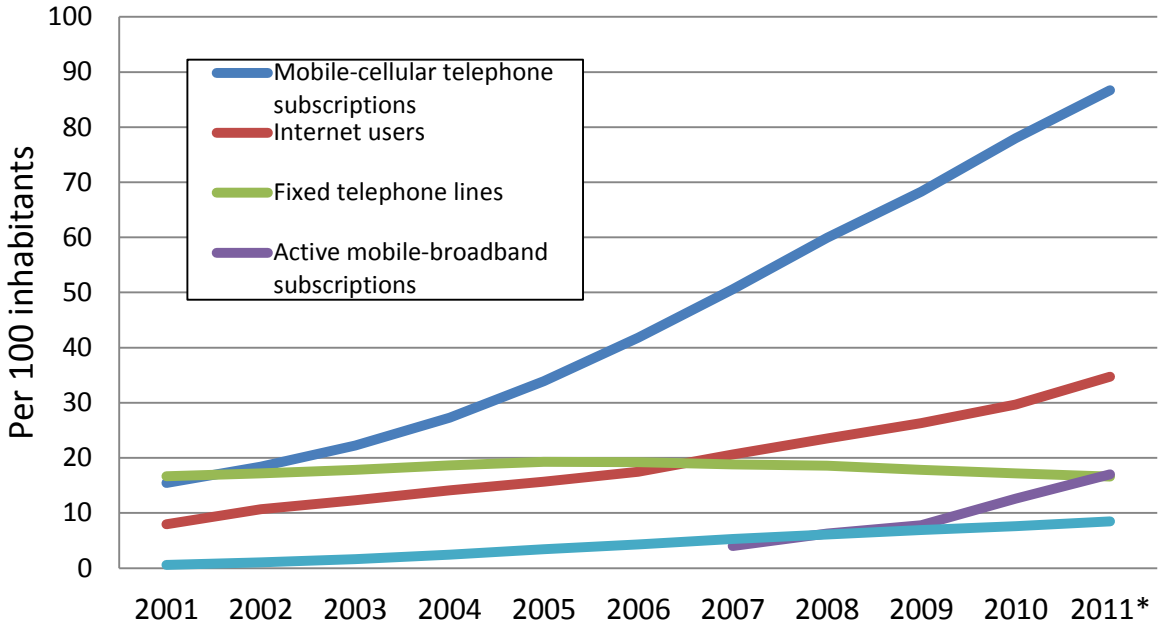
[15] *We note there is extensive consideration of these topics in the broader management literature and in other domains (e.g. public health).*

(EGs), one focused on legal and regulatory aspects and one on operational aspects. These EGs acted as a sounding board for the project. Members of the EGs attended a meeting in Brussels in September 2012 where they were asked to report on their consideration of the importance of these issues from a practitioner perspective.

2 Background

Across many parts of the world, cyberspace and Information Communications Technology (ICT) have become an important aspect of economic and social life. According to Eurostat, in 2010 over one third of all European citizens were online. Data from the International Telecommunications Union (ITU) shows the increase in usage of ICT in the last decade.

Figure 1 Global telecommunications uptake



* Estimate.

Source International Telecommunications Union (ITU)[16]

With the acknowledged importance of cyberspace to economic growth[17], the issue of whether security efforts have kept pace with the growth in the reliance on cyberspace remains a key challenge. Evidence from a range of different sources concerning vulnerabilities, threats, exploits, incidents and crimes although differing in provenance all point to a broadly similar trend that security is becoming more of a challenge.

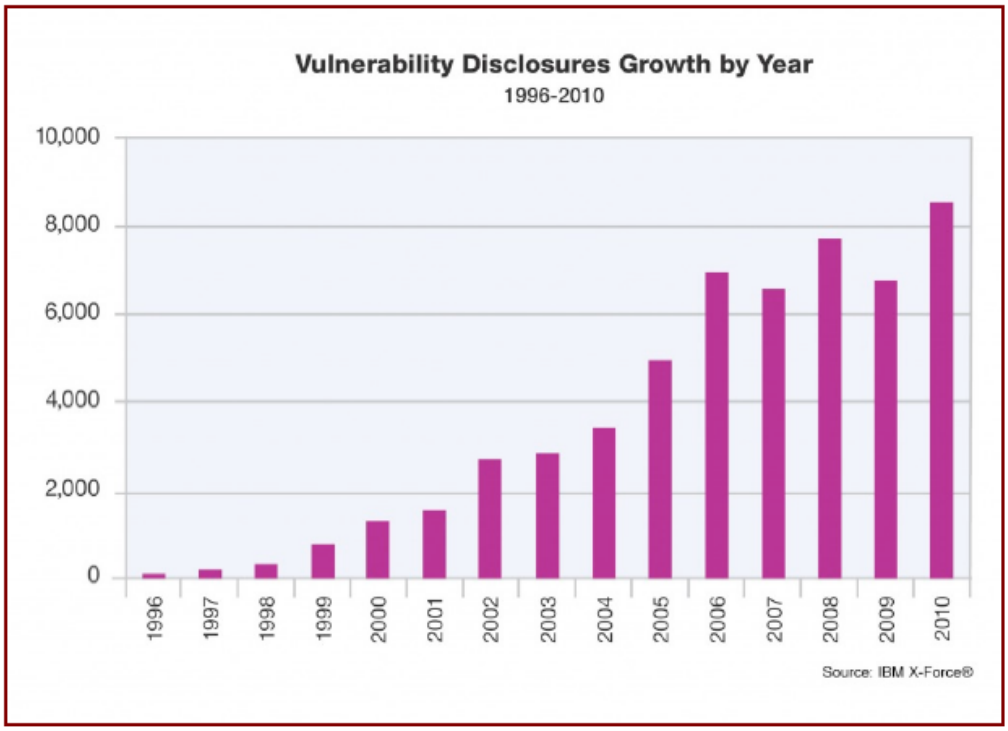
Data from IBM X-Force (at Figure 2 below) illustrates that the number of vulnerability disclosures is increasing.

---

[16] *International Telecommunications Union ICT statistics ,available at[http://www.itu.int/IT-D/ict/statistics/] [Accessed 11/10/2012]*

[17] *World Economic Forum (2012) Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience available at:http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience [Accessed 11/10/2012]*

Figure 2 Vulnerability disclosures growth by year



Source: IBM X-Force[18]

By contrast, data from criminal justice statistics, compiled in to the European Sourcebook of Criminal Justice Statistics, covering different types of cybercrime show an increase in reported cybercrimes between 2004 and 2007.[19] Between the period of 2003 and 2005, the median number of police-recorded offences varies between one offence per 100,000 population (2003) and three per 100,000 population (2005), excluding Germany as an outlier.

Finally, Volume 12 of Microsoft's Security Intelligence Report (SIR) from July – December 2011[20] shows a mixed picture with respect to vulnerabilities: although the trend for CVSS[21] severity classifications decreased between the first and second half of 2011, some exploits

[18] *IBM Threat Security Landscape (2012) available at: http://www-03.ibm.com/security/landscape.html]*

[19] *Robinson, N, et al (2012) "Feasibility Study for a European Cybercrime Centre"RAND TR-1218-EC*

[20] *Microsoft Security Intelligence Report (July – December 2011), Vol 12 Key Findings available at [www.microsoft.com/sir] [Accessed 11/10/2012]*

[21] *CVSS is a vulnerability scoring system designed to provide an open and standardised method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of a vulnerability. For additional information on CVSS v2, please see [http://www.first.org/cvss] and [http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2]*

(malicious code that takes advantage of software vulnerabilities) such as HTML/Java (e.g. the JS/Blacole family of exploits) saw an increase.[22]

Whilst cyber-space has become an important facet of everyday life, some issues appear to constitute a risk to the continued benefits that cyberspace can offer. Collaboration and co-operation may constitute one route to addressing these topics.

The sections below detail some of the important policy aspects involved in addressing this problem; notably the attempt to define it.

2.1 Defining cyber security and cybercrime incidents

The AVOIDIT taxonomy, a model proposed by Simmons et. al.[23] classifies misuse according to five characteristics: Attack Vector, Operational Impact, Defence, Informational Impact and Target. The AVOIDIT model permits a sophisticated definition of cyber-attacks, cybercrimes and misuse, being able to take into account 'blended threats' and crimes where attackers exploit a variety of different attack vectors (technological, human) to perpetrate a crime.

Defining and understanding different types of cybercrime (misuse that has been determined to be criminal in nature) is contentious and as technology evolves, so does the breadth of what cybercrime may potentially constitute. A broad three-pillar typology of cybercrime based around Articles 2-9 of the 2001 Council of Europe Cybercrime Convention (also known as the Budapest Convention) sets out a very accessible typology of the different aspects of insecurity concerning ICT systems (although it also covers accidental issues).[24]

This classification is attractive due to its simplicity and the clarity with which separates the forms of technical misuse from a broader set of crimes involving technology or having a technological aspect to them. The 2009 UK Association of Chief Police Officers (ACPO) Good Practice Guide for Computer Based Evidence espouses a similar approach (comparisons with the above model are in square brackets):

"computers can be used in the commission of a crime [Type II]; they can contain evidence of crime [Type III] and can even be targets of crime [Type I]."[25]

Using these definitions for example, allows us to differentiate cybercrimes where the computer or information system is the target; these have a closer correlation with incidents that a CERT might be expected to handle. Such types of cybercrime also have a more direct

---

[22] *Microsoft Security Intelligence Report (July – December 2011), Vol 12 Key Findings available at [www.microsoft.com/sir] [Accessed 11/10/2012]*

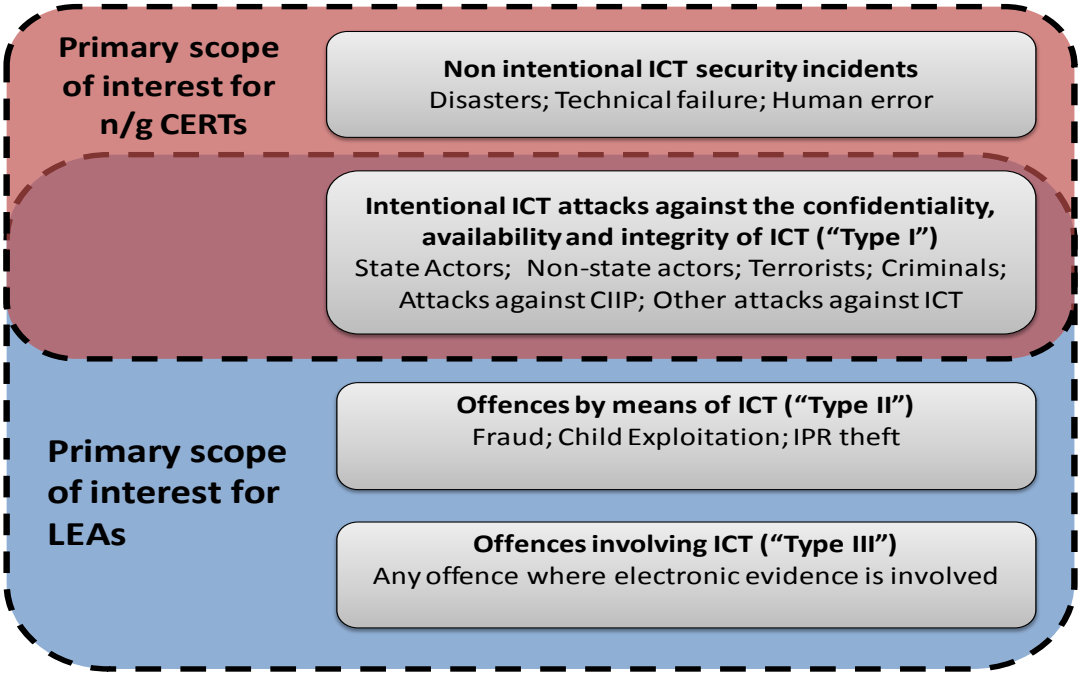
[23] *Simmons C, et al (2009) AVOIDIT: A Cyber Attack Taxonomy available at: http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf [accessed 11/10/2012]*

[24] *Council of Europe (23 November2011) "Convention on Cybercrime, Budapest, 23.XI.2001"available at[http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm] [Accessed 16/08/2011]*

[25] *UK Association of Chief Police Officers (ACPO) (2009) "Good Practice Guide for Computer Based Evidence" p.6*

relationship to poor levels of cyber security. By contrast, because of the pervasive reach of ICT into society, increasingly there is a technological component to many traditional types of crime and CERTs are less likely to add value in the investigation of these crimes.

Figure 3 A characterisation of cybercrime & cyber security incidents



Adapted from presentation given at the Octopus Conference of the Council of Europe Convention Against Cybercrime 21-23 November 2011, Strasbourg

Why are these definitions important? The work of CERTs[26] might be argued to be focused *mainly* on detecting, acting and conducting or supporting the remediation of either:

- Non intentional ICT security incidents
- Intentional attacks against the confidentiality, integrity and availability of ICT

By contrast, Law Enforcement Authorities (LEAs) may have a mandate to cover a different range of incidents (fraud, hosting or downloading of illegal content) where it is possible to determine (criminal) motivation.[27] Previous research into the focus and mandate of LEAs with a special remit for cybercrime or high tech crime illustrate a high degree of variation, with many devoting resources to addressing fraud, or types of cybercrimes involving financial or

[26] *CERT Expectations of Computer Incident Response RFC*

[27] *For example, CERTs would be interested in non-intentional (accidental, human error) incidents and those caused by the sheer complexity of cyberspace*

economic damage.[28] CERTs, on the other hand (especially national/governmental CERTs), may be more interested in incidents affecting ICT systems. This is not necessarily clear-cut, however. Botnet take-downs are an example of something that is of mutual interest to both communities since they involve the compromise of the confidentiality, availability and integrity of ICT systems and also can be used as a 'crimeware' platform to execute various types of fraud and criminal activity.[29]

2.2 Understanding the impacts of incidents

This section examines the impacts of different types of incidents. CERTs, especially those understood to be national/governmental CERTs (often the 'CERT of last resort' at the national level) are envisaged to operate with respect to addressing all these different types of incidents especially those which become either so widespread or systematic that they have national level implications.

2.2.1 Cybercrime

It is difficult to estimate the costs associated with cybercrime. Most efforts focus on costing fraud related cybercrimes. Anderson et al (2011[30]) suggest that there are over 100 different sources of data on cybercrime[31] but that the available statistics are still insufficient and fragmented. Anderson and others note that depending on who collects the data, the sources are liable to suffer from either under- or over-reporting. The costing of cybercrime is exceedingly difficult to determine and is beset by a number of challenges. A plethora of reports have been produced which aim to show the costs of cybercrime to demonstrate that it is a new form of crime and that the situation is getting worse.

For example, in 2011, Norton released a highly publicised report which estimated the global cost of cybercrime (defined broadly, including cyber-bullying, spam, identity theft) to be in the region of US$388bn for 2011.[32]

In reviewing the literature on the costs of cybercrime Anderson et. al. notes[33] that the number of phishing websites and distinct attackers has been consistently over-reported, suggesting

---

[28] *Robinson, N. et al (2012) "Feasibility Study for a European Cybercrime Centre" TR-1218-EC RAND Santa Monica, available at [http://www.rand.org/pubs/technical_reports/TR1218.html] [Accessed 11/10/2012]*

[29] *ENISA (2012) "The Fight Against Cybercrime: Co-operation between CERTs and Law Enforcement Agencies in the fight against cybercrime – A first collection of practices", available at [http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cybercrime] [Accessed 11/10/2012]*

[30] *Casper, C. (2007) "Examining the feasibility of a data collection framework. ENISA, Technical Report" Referenced in Anderson, R. (25-26 June 2012) "Measuring the Cost of Cybercrime", Workshop on the Economics of Information Security (WEIS), As of 8 August 2012*

[31] *Anderson, R., Bohme, R., Clayton,R., and Moore, T. (January 2008) "Security Economics and the Internal Market" available at [http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec] [Accessed 11/10/2012]*

[32] *Norton (2011) Cybercrime Report available at [http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/] [Accessed 11/10/2012]*

that the problem is too large and diffuse for the police, despite the fact that only a relatively small number of players are behind the majority of attacks. The same study, which challenges other industry reported estimates such as that by Detica in 2011[34], also observes that errors may be both intentional (vendors and security sector companies playing up threats) and unintentional (e.g. response effects or sampling bias).

Of course a complication arises because some types of misuse are not exclusively related to fraud or activity where the LEA can easily determine an interest, but nonetheless can provide a platform for various types of nefarious activity. Examples include botnets and malicious software.

2.2.2 Incidents of national interest

There are other types of cyber-attack which are of national interest but are motivated by different reasons. National/governmental CERTs, (in their role of 'CERTs of last resort'), may either receive reports about these incidents or be asked to support the remediation of systems because of their seriousness (something which only could be discerned by intelligence gathering on target sets, behaviour and other contextual factors) and national level impact. This is particularly the case with cyber-attacks affecting governmental systems, especially those belonging to military and national security communities. A pre-eminent historical example is the Remote Access Tool (RAT) series of attacks, examples being the use of such tools to perpetrate campaigns of espionage, information exfiltration.[35] Adversaries using such techniques have targeted and penetrated a large number of sensitive computer networks including high profile companies, embassies, government departments and international organisations.

Finally, national/governmental CERTs may either receive reports from or be asked to help mitigate the effects of cyber-attacks affecting critical infrastructure, for similar reasons. Examples of CERT involvement in such incidents include the following. In 2006, an intruder (believed to originate from a foreign country) planted malicious software in a water treatment system in Harrisburg, Pennsylvania. In 2008, in Lodz, a teenager managed to breach the security of a track control system of a city tram system derailing four vehicles.[36.] In 2003 the Slammer worm crashed the nuclear plant network in Ohio. It was able to propagate via a backdoor from the Internet that was linked to the corporate internal network. Finally, Stuxnet was a more recent but widely discussed example of a cyber-attack affecting critical

---

[33] Anderson, R et al (2012) "Measuring the Cost of Cybercrime", Workshop on the Economics of Information Security (WEIS) available at: [Accessed 11/10/2012]

[34] *Detica (2011). "The Cost of Cybercrime", A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office (UK). Available at [http://www.baesystemsdetica.com/resources/the-cost-of-cyber-crime] [Accessed 11/10/2012]*

[35] *E.g. see Alpervoich, D. (2011) "Revealed; Operation Shady RAT" v1.1 McAfee available at: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf [Accessed 11/10/2012]*

[36] *Critical Infrastructure Protection (CIP) (2009), "A Shortlist of Reported SCADA Incidents", available at [http://ciip.wordpress.com/2009/06/21/a-list-of-reported-scada-incidents/] [Accessed 11/10/2012]*

infrastructures. As stated by the Center for Security Studies Stuxnet "is a manifestation of longstanding fears. It is a targeted attack affecting the control system of a super-critical infrastructure, invisible and untraceable until it hits".[37]

2.3 Stakeholders that CERTs interact with

In order to mitigate these different types of incidents, CERTs are often required to interact with a wide variety of stakeholders – other CERTs, LEAs, network operators, academic institutions, members of their own constituencies reporting anomalies or incidents, etc. – each of whom has different expectations of what information or support they can provide or request, and for each of whom the CERT's ability to provide that information or support can vary. This implies that CERTs need a framework or methodology to determine how they can issue or respond to such requests.

The effective operation of CERTs in a pan-European context in addressing the NIS aspects of cybercrime – a context in which incidents, investigations and responses frequently span different countries and require interactions between different stakeholders – is dependent on the speed and efficiency of exchange of information. Apart from the CERTs themselves, these stakeholders include law enforcement bodies, telecommunications service providers, information society service providers, security experts and others. Koivunen identifies a range that are used to address Network and Information Security incidents including Discoverers (those reporting an incident either from the CERT constituency or general public) Incident Repositories (e.g. PhishTank; Clean-MX); Incident reporting clearing houses (e.g. malwareurl.com); National CERTs; Internet Service Providers; Victims (either individuals or organisations).[38]

The required free flow of information can however be marred by a multitude of legal/regulatory and operational obstacles. This is compounded by the large number of stakeholders that a CERT has to interact with. We list some of these examples below.

- **National cyber security centres**: many countries have set up or are considering the development of specific cyber security centres to act as a focal point for the implementation of cyber-security strategies. Examples include the Office of Cyber Security and Information Assurance (OCSIA in the United Kingdom; the Dutch National Cyber Security Centre and the German Federal Office for Information Security (BSI).
- **Domestic CERTs** (e.g. PCSIRTs, CERTs covering other constituencies) may report incidents to the national/governmental CERT, perhaps based on a certain threshold or on the understanding, derived from expert knowledge that an incident they have detected needs to be escalated to someone able to provide a national level picture

[37] *Möckli, D (ed) (2012) "Strategic Trends 2012 Key Developments in Global Affairs"; Centre for Security Studies, p.112; available at [http://www.css.ethz.ch/publications/pdfs/Strategic-Trends-2012-Cyber.pdf] [Accessed 11/10/2012]*

[38] *Erka, K., (2010) "Effective Information Sharing for Incident Response Co-ordination: Reporting Network and Information Security Incidents and Requesting Assistance", Master's Thesis, Aalto University School of Science and Technology*

- **Other EU national/governmental CERTs:** supposedly on a comparative national framework, however some are still *'de-facto'* national/governmental CERTs and may simply be so because of the fact they have oversight of significant portions of the CII of that country.[39]
- **Non-EU foreign CERTs** (whether they be national level 'CERTs of last resort' such as the US-CERT) or CERTs covering other constituencies. These CERTs may additionally be governed by unique legal frameworks concerning their operations.
- **Domestic law enforcement authorities (LEAs):** many EU countries now have national level high tech crime units, which may be reactive or proactive in tackling cybercrime. Additionally, these units may sit at the top of an organisational pyramid of regional or local level high tech crime capability, or they may be specialised in focusing on serious and organised crime (e.g. UK's Serious Organised Crime Agency (SOCA)) have another hybrid character (Dutch National High Tech Crime Unit (NHTCU)) or indeed be reflective of the politico-administrative character in the jurisdiction (the German Federal Criminal Police Office (*Bundeskriminalamt* –BKA) for example).
- **Domestic intelligence agencies** may also get involved in cases where, as the discovery phase of an incident expands, it may become obvious that the matter is of national concern and therefore the intelligence community needs to become involved. This was seen, for example, in the Remote Access Tool (RAT) series of cyber-espionage cases. Some cyber security centres have been set up to include personnel from such agencies to make communication and collaboration easier (e.g. by providing a single face to others).
- **Foreign law enforcement authorities** and **intelligence agencies** may also have a role to play, particularly where requests for Mutual Legal Assistance are concerned.[40] Here, supra-national organisations related to law enforcement such as Interpol and Europol might play a role, although the extent of direct information sharing between CERTs and these types of international entities is not known.
- **The private sector** in the form of Managed Security Service Providers (MSSPs) or malware libraries are also be another stakeholder

2.4 Policy initiatives in this domain

Policy-makers at both the European and Member State level have long recognised the role that CERTs play in cyber security in detecting and responding to the types of incidents and cybercrimes described previously. Under the heading of efforts to improve cyber security, three main EU policy statements have been driving this agenda in Europe: the 2009 Digital Agenda for Europe[41], the 2009 Communication on Critical Information Infrastructure

[39] *Flair for Sharing: Legal and Regulatory Barriers to Cross Border Information Exchange between national/governmental Computer Emergency Response Teams (CERTs)*

[40] *Mutual Legal Assistance Treaty (MLAT) regimes concern the exchange of 'letters rogatory' between judicial authorities in the interests of cross border police and judicial co-operation.*

[41] *Communication from the Commission on a Digital Agenda for Europe COM (2010) "Digital Agenda for Europe" 245*

Protection (CIIP)[42] and the 2011 Progress Report on CIIP.[43] In addition, there has been increased effort to foster co-operation between LEA and CERT communities.
At the European level, further initiatives have shaped the CERT landscape. These have been conducted in the context of the unique role that the EU plays, respecting the principle of subsidiarity. These include the 2006 Strategy for a Safe, Secure Information Society – dialogue, partnership and empowerment,[44] and in 2009 the Action Plan on CIIP.[45] The 2009 Action Plan in particular highlighted, within the Preparedness and Prevention heading, the need to establish a "well functioning network of CERTs" in all Member States by the end of 2011. Furthermore the need to improve co-operation was also emphasised under the pillar of "Reinforced co-operation between national/governmental CERTs through support (e.g. exchange of best practices) and also in expanding co-operation schemes such as the European Government CERT.

In 2009 the Digital Agenda outlined objectives under Pillar Three (Trust and Security) Section 2.3 that a wider network of well functioning National/Governmental CERTs should be established across Europe by 2012 in order to react to real-time conditions.[46] The 2009 Digital Agenda also highlighted the fact that cybercrime constitutes a major inhibitor of trust, deterring individuals from participating in ever more sophisticated online activities.[47]

The 2011 Progress Report on the CIIP Action Plan[48] noted that a minimum set of baseline capabilities, and related policy recommendations for a well-functioning network of national/ governmental CERTs in all Member States, has been developed. These developments encompassed preparedness, information sharing, coordination and response. The 2011 Progress Report highlighted the achievements of:

---

[42] *Communication from the Commission on Critical Information Infrastructure Protection (30 March 2009) "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" 149 of ('Communication on CIIP')*

[43] *Communication from the Commission on Critical Information Infrastructure Protection (31 March 2011) "Achievements and next steps: towards global cyber-security" 163 ('Progress Report on the CIIP Action Plan')*

[44] *Communication from the Commission on a Strategy for a Secure Information Society; COM (2006) "European Commission Strategy for a Secure Information Society" 251. See also "EU policy on promoting a secure Information Society", available at [http://ec.europa.eu/information_society/policy/nis/index_en.htm] [accessed 11/10/2012] for a list of reference documents*

[45] *Communication on CIIP(2009) "Communication on Critical Information Infrastructure Protection" 149;and also "EU policy on Critical Information Infrastructure Protection" [http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm] [Accessed 11/10/2012]*

[46] *A Digital Agenda for Europe" COM (245)*

[47] *e.g. see The Scotsman (2012) Millions lost in online sales because shoppers don't trust web security [http://www.scotsman.com/news/uk/millions-lost-in-online-sales-because-shoppers-don-t-trust-web-security-1-2183171] [Accessed 11/10/2012]*

[48] *Communication on CIIP: COM(2011)163 "Communication on Critical Information Infrastructure Protection: Achievements and Next Steps: towards global cyber-security" [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF] [Accessed 11/10/2012]*

- Development and agreement of minimum baseline capabilities and services for national/governmental CERTs resulting in a must have list of requirements
- Articulation of policy recommendations based on these baseline requirements
- Establishment of national / governmental CERTs and a CERT for the EU Institutions
- Stimulation and stronger co-operation between national / governmental CERTs

It called for progress on:

- Continuing to support Member States that have not yet set up National/Governmental CERTs to meet the milestone laid out in the Digital Agenda for Europe
- Discussion concerning whether to extend the baseline capabilities for national / governmental CERTs to help support Member States in ensuring the resilience and stability of vital ICT infrastructures.
- Continue to support co-operation amongst National/Governmental CERTs via an analysis of secure communications channels and operational gaps at the European level "**and report on how cross border collaboration between CERTs and relevant stakeholders can be reinforced, in particular for incident response co-ordination."** [our emphasis]

2.4.1 ENISA's activities in supporting CERT Co-operation

For many years, ENISA has been actively supporting the work of National/Governmental CERTs (in the broader context of supporting CERTs more generally). This has its origin in work of the Agency in 2005 with its CERT programme and Working Group on CERT Co-operation and Support. This work included the identification of broad baseline capabilities, and gap analysis in the area of operational considerations and legal and regulatory factors. ENISA's work in this domain is also compatible with the proposal for a revised mandate outlined in COM 2010(521)[49], which foresees an expanded role of the Agency in providing assistance, support and expertise to the Member States and European institutions and bodies by investigating and providing obstacles to cross border issues and detection and response capabilities.

ENISA's Baseline Capability Policy Recommendation report for national / governmental CERTs aimed at defining a minimum set of capabilities that a CERT in charge of protecting critical information infrastructures (CII) in Member States should possess in order to take part in and contribute to sustainable cross-border information sharing and cooperation. The necessity for this approach is underlined by the emerging need for CERTs to support incident management across a broad spectrum of sectors, and the rising importance and reliance on governmental

[49] *Communication from the Commission COM 2010 (521); "Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency"*

CERTs to implement of cyber security and critical information infrastructure protection (CIIP) at the national level.[50]

The goals of current national cyber security initiatives to strategically address incidents related to key resources and critical infrastructures, have included; "*i) establishing a national focal point within a country or region to coordinate security incident management activities, ii) analysing and synthesising information on incidents and vulnerabilities disseminated by other CERTs, vendors and technology experts to provide an assessment for their own constituencies and communities, iii) facilitating communications across a diverse constituency to bring together multiple sectors to share information and collaborate in addressing computer security problems, iv) developing protocols and mechanisms for trusted interaction with other relevant stakeholders.*" In assessing the role of CERTs, the work into baseline capabilities formulates policy recommendations in the following areas; i) Mandate and Strategy, ii) Service Portfolio, iii) Operation, iv) Cooperation.

Looking at supporting collaboration between CERTs & LEAs, in October 2011 ENISA held a workshop on CERT-LEA co-operation co-organised with Europol in Prague and supported by CSIRT.CZ. This meeting identified that informal mechanisms such as face to face meetings are important in helping to establish trustworthy relationships between these two communities. It also noted the importance of using particular specific examples (e.g. tackling bot-nets) to galvanise co-operation.

In 2012, as envisaged in the Work Programme, ENISA ran a workshop across two parts (a technical hands-on training hosted by the University of Malta in conjunction with Team Cymru in June) and an event that took place in October 2012 in The Hague jointly organised alongside with Europol aimed at furthering co-operation between CERTs and LEAs.

These initiatives (the workshops in particular) may be considered in the light of ENISA's 2012 Work Programme (specifically WPK3.3) as supporting a system of contact points between CERTs and LEAs in order to help CERTs to play their part in tackling cybercrime.[51]

In 2011, ENISA also released a first report into "good practice guide for CERTs in addressing NIS aspects of the fight against cybercrime". This study was based on a survey and in-depth discussions with practitioners. It noted the following elements:

- The importance of trust;
- Existence of both formal and informal mechanisms;
- Need for bilateral co-operation;
- Ensuring that the CERTs can remain agile in dealing with incidents.

---

[50] *See for example ENISA National / Governmental CERT Baseline Capabilities Reports (2009; 2010) v.1.0 (initial draft) available at [http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/] [Accessed 11/10/2012]*

[51] *ENISA; (2012), "European Network and Information Security Agency (ENISA) Work Programme 2012: Improving Information Security Through Collaboration"*

Also in n 2011, the report "Flair for Sharing: ENISA's study into the legal and regulatory factors affecting cross border CERT Co-operation" showed that some CERTs have different legal and regulatory challenges, which may have both positive and negative impacts on the extent of cross-border information sharing.[52]

2.4.2 European policy as regards co-operation with Law Enforcement Authorities (LEAs)

In its 2008 conclusions on Cybercrime, the Justice and Home Affairs (JHA) Council noted the importance of information exchange concerning information on cybercrime, to better inform efforts to tackle the problem.[53]

On 10–11 December 2009 the JHA Council adopted the Stockholm Programme.[54] One aspect of which is to promote policies to ensure network and information security and faster EU reactions in the event of cyber-attacks. It called, for instance, for both a modernised ENISA and an updated Directive on attacks against information systems.

These initiatives were also reinforced by the Conclusions of the European Council in April 2010, which proposed actions in the short and medium term to specify how the main points of a concerted strategy to tackle cybercrime should be implemented. Most notably for the focus of efforts to improve co-operation with CERTs, the Conclusions included the request concerning:

> "Promotion of cross-border law enforcement co-operation and Public–Private Partnership (PPP)."

Building on the Council Conclusions and the Stockholm Programme, the Commission stated in the EU Internal Security Strategy 2010[55] that the European Cybercrime Centre (EC3) should be established. A key element would be improving capacity for co-operation with other partners.

Within the aims of the EC3, as set out in this Communication, specific consideration was given to increasing co-operation between the law enforcement community and CERTs:

> "Establish co-operation with the European Network and Information Security Agency (ENISA) and interface with a network of national/governmental Computer Emergency Response Teams (CERTs)."

Subsequently, the Commission Communication on the European Cybercrime Centre issued on the 28th March 2012[56] noted that the EC3 would serve to:

---

[52] *ENISA (2011), "A Flair for Sharing: ENISA's study into the legal and regulatory factors affecting cross border CERT Co-operation"*

[53] *JHA Council Conclusions, 2899th JHA meeting (2008)*

[54] *European Union (2010), "The Stockholm Programme – An open and secure Europe serving and protecting citizens"*

[55] *European Commission, COM(2010) 673 final*

[56] *Communication from the Commission to the Council and the European Parliament (28 March 2012) "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre"140 Final Brussels, available at[http://ec.europa.eu/home-affairs/doc_centre/crime/docs/Communication%20-%20European%20Cybercrime%20Centre.pdf] [Accessed 11/10/2012]*

> "…encourage appropriate links between law enforcement authorities, the Computer Emergency Response Team (CERT) community…"

Finally, another important development at international level is the EU-US working Group on Cybersecurity and Cybercrime, which was established during the EU-US summit of November 2010. This working group focuses on:

- Cyber incident management
- Public-private partnerships
- Awareness raising
- Cybercrime

Key stakeholders within this EU-US Working Group include the European Institutions, such as the Commission, ENISA and Europol who play specific practical roles in encouraging co-ordination between CERTs and LEAs in a cross border context.

2.5 National level initiatives

National strategies include establishing cyber security centres, often based on representatives from a wide variety of different stakeholders, such as government departments, national agencies, regulators and industry. Diverse stakeholders are involved in the security process because parts of this infrastructure are managed by industry. Co-operation between these parties is mutually beneficial because sharing information is more cost-efficient and provides multiple viewpoints on the issue. To facilitate the cooperation between governments and organisations, many Member States co-operate through Public Private Partnerships (PPPs), where trust among the stakeholders is essential.[57] An insight into the functioning of different PPPs can be gained from ENISA's report "Desktop Research on Private Public Partnerships". [58]

2.6 Examples of challenges concerning CERT-LEA co-operation

Some case studies concerning instances of co-operation between CERTs and other organisations, especially LEAs, are highlighted below. Many of these examples concern actions to address bot-nets, since that is the area where the majority of publicly available data is published.

---

[57] *Desktop Research on Private Public Partnerships; [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/copy_of_desktop-reserach-on-public-private-partnerships] [Accessed 11/10/2012]*

[58] *This research was on 20 PPPs and other organisations were researched during this desktop study and they covered 12 Member States, 2 other nations and, 1 international organisation. Desktop Research on Private Public Partnerships; [http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/copy_of_desktop-reserach-on-public-private-partnerships] [Accessed 11/10/2012]*

Box 1 Case studies of the challenges to CERT & LEA co-operation

Conficker

The most comprehensively analysed example of such cooperation was Conficker. The US Department of Homeland Security conducted interviews with many members of the Conficker Working Group to derive a 'lessons learned' report[59]. The report discusses cooperation, but the role of CERTs in this episode is either minimal (only US-CERT is mentioned, and they only appear in the later stages) or perhaps deliberately not mentioned for sensitivity reasons. The report is heavily focused on the commercial organisations involved, and has little reference to intelligence or law enforcement involvement, so again this might be due to sanitisation. The importance of cooperation between industry players, and with law enforcement is clearly seen as vital, though government's lack of engagement is bemoaned by some CWG members. This is a US-centric report, though many of the Conficker Working Group players were international, but no other LE or government entities are named.

It is possible to conclude that the main players in what was clearly a very major malware incident (Conficker was not a botnet but was responsible for generating some bot-nets amongst other things) were from the commercial sector, including Software manufacturers, DNS authorities, Cyber Security Researchers, Anti-Virus and security vendors, and Internet Service Providers. The legal system and law enforcement also played significant roles, but these are not made public in any detail.

Further direct research with CERTs and LEAs would be needed to establish their true level of involvement and significance.

Some interesting observations are noted in the extracts below:

In an unprecedented act of coordination and collaboration, the cyber security community, including Microsoft, ICANN, domain registry operators, anti-virus vendors, and academic researchers organized to block the infected computers from reaching the domains – an informal group that was eventually dubbed the CWG.

This followed unsuccessful attempts by a subset of (subsequently) CWG members to eradicate the Sribsi botnet earlier in 2007.

Many of the core members of the CWG knew each other prior to the effort or were within one degree of separation through various social networks. As one interviewee said, "we all knew each other." Commercial competition and personal motivations play a role in how well these ad-hoc organisations function.

The group as a whole saw little participation from the government. One person put it as "zero involvement, zero activity, zero knowledge." A number of people recognized Conficker's

[59] *Conficker Working Group (2010) Lessons Learned Report available at [http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf] [Accessed 28/8/2012]*

threat in December and January. Members of US-CERT were not added to the Conficker Working Group list until mid-March.

The Working Group sees its biggest failure as the inability to remediate infected computers.

Bredolab[60]

A botnet that had infected at least 30 million computers globally was taken down by the Dutch National Crime Squad.

Working in close collaboration with a Dutch hosting provider, the Dutch Forensic Institute (NFI), internet security company Fox-IT, the Dutch computer emergency response team (GOVCERT.NL) seized and disconnected 143 computer servers from the internet.

This is one of the few widely published examples of CERT/LEA/Commercial collaboration to eliminate a botnet. The degree of cooperation is not unusual for Netherlands, and was illustrated again in the Diginotar incident.[61] As with the Conficker CWG, a large degree of personal familiarity and regular contact between the agencies will have contributed significantly to the cooperative nature of this episode.

Waledac

"This legal and industry operation against Waledac [botnet] was the first of its kind, but it won't be the last. With this action, done in cooperation with experts from Shadowserver, the University of Washington, Symantec, University of Mannheim, Technical University in Vienna, International Secure Systems Lab, the University of Bonn and others, we're building on other important work across the global security community to combat botnets." (Tim Cranton. Microsoft Associate General Counsel).[62]

This incident was heavily driven by Microsoft and involved close cooperation with the US legal system, though no explicit mention is made of CERT or LEA involvement (though the latter is implicit). The presence and influence of Microsoft in the US could be seen as a major contributory factor.

Usenix[63] analysis of a range of botnets 2009-2011

[60] *SC Magazine Bredolab Botnet taken down after Dutch Intervention,* ***available at:*** [*http://www.scmagazineuk.com/bredolab-botnet-taken-down-after-dutch-intervention/article/181737/*] *[Accessed 31/8/2012]*

[61] *Govcert.NL Digitnotar Dossier,* ***available at*** *[http://www.govcert.nl/english/service-provision/knowledge-and-publications/dossier-diginotar]* *[Retrieved 31/8/2012]*

[62] *Microsoft technet Blog (2010) "Cracking down on botnets",* ***available at*** [http://blogs.technet.com/b/microsoft_blog/archive/2010/02/25/cracking-down-on-botnets.aspx] *[Accessed 29/8/2012]*

[63] Usenix "*Usenix analysis of botnets" (2011)* ***available at*** *[https://www.usenix.org/system/files/conference/leet12/leet12-final23.pdf]* *[Accessed 31/8/12]*

This academic examination of a series of bot-net operations concluded that technical and legal elements are essential:

"All takedowns coordinating civil and/or criminal legal process with technical methods succeeded on first try, while those only using civil legal process or using only technical means did not."

The role of CERTs did not appear to have figured heavily in this examination, however.

Mariposa

Mariposa was another major bot-net (in 2009 having >1M and reportedly up to 12M computers compromised) heavily involved with e-crime operations and taken down through cooperation primarily between a commercial AVS company (Panda Labs) a cyber security company (Defence Intelligence), an ISP (CDmon) and an academic centre (Georgia Tech Information Security Center). They formed the Mariposa Working Group and cooperated with the Spanish Civil Guard and Slovenian police to arrest the botnet controllers. Various reports state that international LEAs were involved including the FBI. No mention is made of any CERT involvement, apart from subsequent work by the Slovenian CERT to track cyber-criminals exploiting the remnants of Mariposa.[64]

Estonia DDoS attacks

The role of the Estonia CERT in their infamous DDoS event in 2007 was highlighted as central by an industry observer. That attack was however clearly targeted against the CERT's core constituency so their prominence was inevitable.

The Estonia attack, which primarily targeted commercial financial networks, was able to bring the Estonian banking system to its knees for several days. But the effects of the attack were mitigated by the efforts of the Estonian computer emergency response team (CERT), according to Gadi Evron, an Israeli bot-net expert.

The CERT, "in cooperation with local providers and volunteer networks of IT professionals in industry and government, coordinated the emergency defense program," Evron related. "The team was immediately involved in analyzing the severity of the incident, sending abuse reports to service providers abroad, and facilitating information exchange between the affected organizations and service providers."

The team organised an online chat room, where network defenders could exchange information. The same forum also provided the Estonian authorities with real-time information on attack targets and types.[65]

---

[64] *Georgia Tech Information Security Center (2011) Cyber Threat Reportavailable at [http://www.gtisc.gatech.edu/pdf/cyberThreatReport2011.pdf] [Accessed 11/10/2012]; Panda Labs Security Mariposa Botnet available at [http://pandalabs.pandasecurity.com/mariposa-botnet/] [Accessed 11/10/2012]; Defintel; Mariposa Analysis available at [http://www.defintel.com/docs/Mariposa_Analysis.pdf] [Accessed 14/9/12]*

[65] *Evron, G. (2008). Battling botnets and online mobs: Estonia's defense efforts during the internet war. Georgetown Journal of International Affairs, 9(1), 121–126.*

In terms of sharing of lessons learned, it appears that the collaboration to tackle Conficker was the only example where public reports were released describing lessons learnt for collaboration. The Conficker Working Group[66] recommendations noted that:

- Ad-hoc collaborative response may not be scalable or sustainable
- Informal communications may not be sufficient for global incident response efforts, especially in situations where there is zero tolerance for error or omission
- Maintaining consistency, completeness and accuracy of information sharing during the course of a long incident response effort is challenging
- Scaling trust is hard

The Rendon Group report into Conficker lessons learned identified that the need for collaborative infrastructure, information sharing, early warning and taxonomy was seen as important.[67]

2.7 Strategic level challenges

Below we identify some high level challenges to on-going cooperation and collaboration between CERTs and others. It is possible to discern a number of related sets of issues concerning each community which serve to differentiate them.

2.7.1 Different definitions of cybercrimes/attacks

Firstly, there are **different definitions of cybercrimes/attacks** used between different CERTs and LEAs. Each type of stakeholder identified above has a different scope and area of interest. These differences may even exist within national / government CERTs themselves. For law enforcement, this is also the case: evidence from previous research indicates that the sorts of cybercrime that LEAs might be interested in, might be radically different from that which would be of direct interest to CERTs.[68] For example, law enforcement may be focused on a variety of types of fraud (e.g. romance scams; auction fraud) the posting of illegal content (copyright violations; online child exploitation material) or even investigations and crimes where there is an ICT element (e.g. forensic exploitation of crime scene evidence). In such cases, it would appear that the role of the CERT could potentially be of a supportive nature. This distinction is even more the case when interaction with other national level security organisations is considered. For example, understanding the interaction between a CERT and a domestic intelligence agency involved in gathering intelligence on a possible state sponsored exploitation of the ICT infrastructure of an energy company requires considerable thought.

---

[66] *Conficker Working Group available at [http://www.confickerworkinggroup.org] [Accessed 11/10/2012]*

[67] *Rendon Group (2010) "Lessons Learned in Collaboration" available at [http://www.rendon.com/conficker-lessons-learned-in-collaboration/] [Accessed 11/10/2012]*

[68] *Robinson et al (2012) "Feasibility Study for a European Cybercrime Centre" RAND Santa Monica TR-1214-EC*

2.7.2 Different meaning of information sharing

The act of sending and receiving information can itself mean different things and be open to interpretation. Three terms are often used and may be more or less of relevance regarding CERT interaction with other stakeholders, especially LEAs. These are **information disclosure**; **information sharing** and **information exchange**.

- Information disclosure implies a one-way, generally one-to-many, broadcast transmission of information.[69] The other important aspect of disclosure is that it implies the recipients are unknown and there is no expectation by the originator that he or she will get something in return.
- Information sharing would appear to concern more of a type of transmission of information where the recipients are more known or trusted to/by the originator. Within the idea of information sharing, there is an expectation of getting something in return.
- Finally, information exchange, by comparison, (in this context at least) would appear to constitute a more bi-directional, one-to-one activity where the recipient is at least known to the originator. In addition, with the phrase 'exchange' there would appear to be a consideration or expectation of something in return. The 2010 ENISA report into barriers and incentives for information exchange[70] discussed some of these issues from a socio-economic perspective.

2.7.3 Different character of community

A third major challenge is that the **character of the communities is different**. In summary, CERTs may be seen as problem solvers, compared to the investigatory character of LEAs. The 2011 report into operational and technical co-operation between CERTs and LEAs, and the Flair for Sharing report indicated that CERTs operate on an informal basis, which allegedly permits them to be agile in their response (although this is somewhat tempered by the reports from the Conficker Working Group, see below). By comparison, LEAs are generally bound by a more procedural approach of following rules and a hierarchical authority. This is partly due to the different and sometimes conflicting objectives that each community is trying to achieve but it is also bound up with the character of each community. LEAs are driven by procedures because of the different standards that pervade their work (e.g. in maintaining the evidential chain, justifying decisions). This is particularly important when a case is presented

---

[69] *A common example is in vulnerability disclosure, which can be either under a responsible disclosure (where whomever discovered the vulnerability notifies the organisation responsible for the vulnerability, potentially giving them time to close it, before openly disclosing it) and open disclosure (where the discoverer of the vulnerability publishes it openly).*

[70] *ENISA (2010) "Incentives and Barriers to Information Sharing". Available at:: http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/incentives-and-barriers-to-information-sharing [accessed on August 16 2011].*

to a prosecutor and, ultimately, arrives at a court room setting. The prosecutor must try to make sure that the evidence has been collected in line with proper procedures to maintain the integrity of the evidential chain. Having said that, trust remains a key component of developing relations common to both communities. Going further afield, intelligence agencies may be even more idiosyncratic: whilst they might be highly hierarchical they have different approaches to information management, using criteria to consider the reliability and timeliness of sources.[71] Finally, the activities of CERTs with a focus on the gathering of information to inform the "who", "what" and "why" might be more closely aligned to that of intelligence agencies that generally do not have to abide by similar stringent requirements with respect to evidence handling for example.

2.7.4 Different objectives of each community

Fourthly, there are **differing objectives** that each community is trying to achieve. CERTs, as we have seen, are focused on remediation and, to the extent possible restoration of services.[72] LEAs may be more driven (although not always) by considerations about evidence acquisition and integrity because, in conjunction with the public prosecutor, they are responsible for the presentation of the evidence in as rigorous fashion as possible in the courtroom. However, other evidence suggests that the involvement of the public prosecutor at different stages may drive how stringently law enforcement follow these objectives.[73] This may be referred to as 'the window of discretion'. LEAs will have opportunities to collect intelligence for the preparation of a case and it is not always the case (often erroneously cited in Germany, for example) that the police must open a case for each and every report made. Going even further, intelligence agencies and other national security bodies may be pursuing national level strategic goals such as the identification of a foreign adversary or other major non-state actor. Of course, these definitions presented here are necessarily simplistic: Some types of serious and organised cybercrime, for example, have become such a threat that many countries intelligence agencies are working collectively with law enforcement to address this as a national-security level threat.

Nevertheless, to a certain degree, both CERTs and LEAs are trying to work toward objectives that are both societally beneficial: CERTs by ensuring that 'their' portion of cyberspace is secure and LEAs by crime prevention and bringing to justice those exploiting vulnerabilities to perpetrate crimes.

---

[71] *In the intelligence community these are known as 5x5 matrices see for example: Mcdowell, Don (1997) Strategic Intelligence and Analysis - Guidelines on Methodology and Application: The Intelligence Study Centre; Canberra available at: [http://www.intstudycen.com/docs/strat_meth_guide.pdf] accessed 11/10/2012*

[72] *Killcrece, G., Kossakowski, K.-P. et al. (2003) "State of the Practice of Computer Incident Response Teams (CSIRTs)" Carnegie Mellon Software Engineering Institute*

[73] *Robinson et al (2012) Ch 4*

2.7.5 Different types of information

A further distinction also exists in the **type of information** being shared or exchanged. For CERTs and LEAs, this may be thought of as the difference between evidence and intelligence. Intelligence is information you can use but not present, whereas evidence needs to possess authenticity in order for it to be admissible. Going even further, within an information request there might be a different ontology which applies. Examples proposed by a practitioner[74] might include:

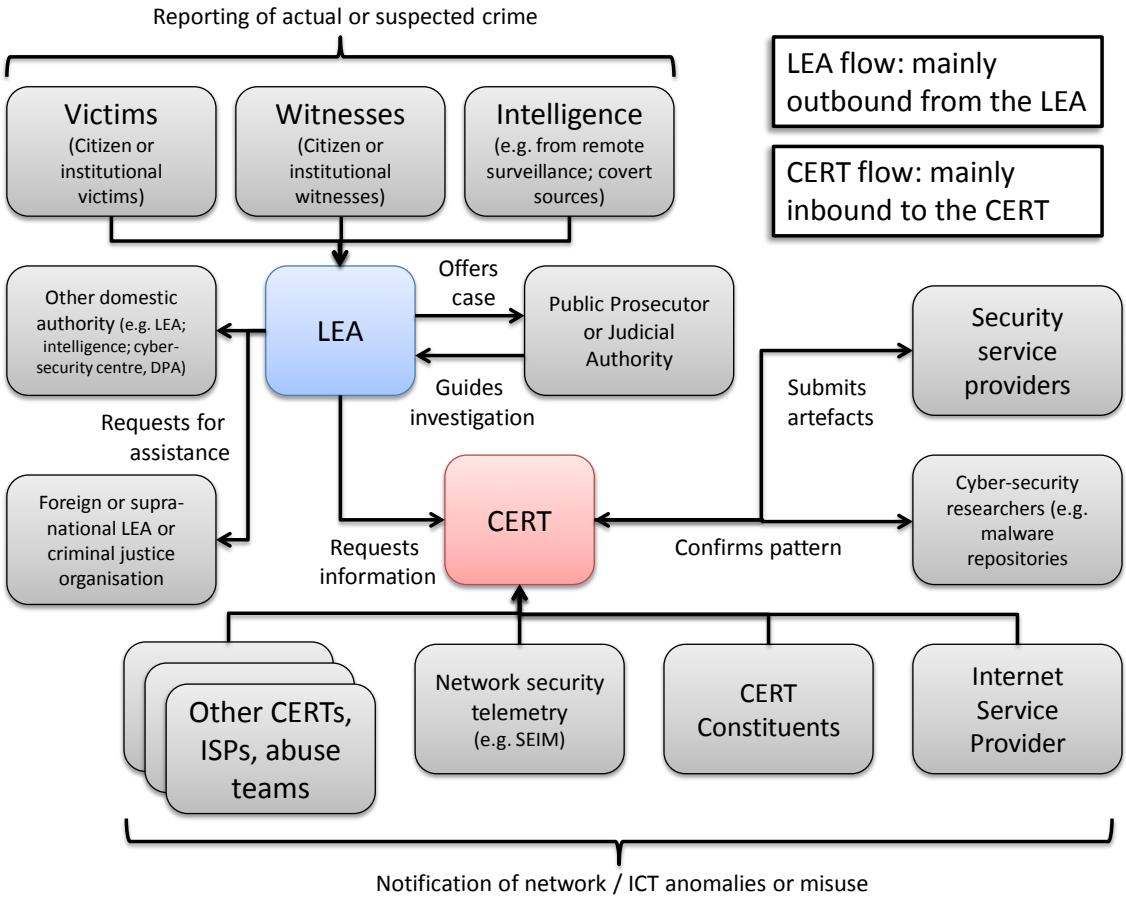
- The type of dialogue (question; response)
- Information types (number, Internet Protocol (IP) address, further info etc)
- Question types (open / closed; Y/N who, when, which IP; whether this IP seen before etc)

2.7.6 Different directions of requests

Related to the question of the different character and objectives of the two communities is a difference with respect to the asymmetric **flow of information** that may affect co-operation. CERTs are, it can be seen, generally concerned with being on the receiving end of information and inputs coming to them: either reports from their constituents, data from other sources or requests for information from other organisations. By contrast, LEAs (partly driven by the nature of their activities) might be more likely to transmit / issue requests: either for information or intelligence that would help in their investigations *to* CERTs. This asymmetric flow is a challenge for long-term collaboration because the value accrues to the recipient (LEAs) and the effort is by the CERT, and there is thus not a reciprocal need. Figure 4 below illustrates this asymmetry of information flows but also the complexity.

[74] *Anonymous interviewee, 11 September 2012*

Figure 4 – Information flows to and from CERTs and LEAs



3 About this study

The present study aims to collect empirical evidence and prepare good practice guides on the most important legal/regulatory and operational aspects of tackling cybercrime, and specifically on challenges to organise cooperation between CERTs and other actors, namely LEAs. This was called for in WPK3.3 of ENISA's 2012 Work Programme, building upon work in 2011 which identified some barriers and incentives to co-operation and also deepened contacts between ENISA and other communities:

> *"In 2012, ENISA will build on this work, and will propose concrete steps to assist CERTs to improve their collaboration and information exchange with law enforcement bodies tasked to prevent and fight cybercrime."*

This initiative progressed in two distinct but related projects:

- A project concerning legal, regulatory factors
- A project concerning operational factors

The study encompassed desk research of background peer reviewed and 'grey' literature[75]; consultations with practitioners; an online survey[76] distributed to the global CERT community via TF-CSIRT, FIRST (and other channels such as personal contact and the informal European Government CERT group) and an Expert Group meeting held in Brussels on 11th September 2012. At this meeting representatives primarily from both the European CERT and Law Enforcement communities were present as well other experts. Many of the attendees were members of two ENISA informal Expert Groups (EG) formed alongside the study.

At the informal Expert Group meeting in September 2012, it became apparent that the factors were quite inter-related and become more pressing at different stages of a CERTs maturity. Therefore it was decided to merge the deliverables from each project into one (this document).

The scope of the study was mainly focused on national/governmental CERTs, but noting that the current level of maturity of these types of CERT across Europe means that we did not necessarily restrict ourselves to this grouping. Similarly, in terms of other stakeholders, we noted that in tackling the NIS aspects of cybercrime, LEAs were the most pre-eminent other type of organisation with which CERTs would be likely to interact.

3.1.1 Responses from CERTs

Those reporting their organisation are listed below (not every organisation is represented as some expressed a wish to remain anonymous)

---

[75] *For this report we focused upon CERT-LEA interactions as a unique case and did not explore the literature in other domains of public policy (e.g. public health) where barriers to organisational collaboration may exist.*

[76] *It was challenging to engage CERTs for the online questionnaire and any conclusions must bear this in mind. Further analysis would help to shed light on these topics but it is encouraging to note that some of the findings are supportive of those from the 2011 study into Legal and Regulatory Factors to Cross Border Information Exchange.*

- CERT.LV (Latvia)
- CERT-Bund (Germany)
- CERT-Hungary / National Cyber Security Center (Hungary)
- CERT-SE (Sweden)
- NCSIRT, NRI Secure Technologies CSIRT (Japan)
- Reporting and Analysis Unit for Information Assurance MELANI (Switzerland)
- SWITCH-CERT (Switzerland)

Those reporting their country

- Australia
- Austria
- Estonia
- Germany
- Hungary
- Japan
- Korea
- Latvia
- Mexico
- Norway
- Spain
- Sweden
- Switzerland
- USA

3.1.2 Responses from Law Enforcement Authorities

Those reporting their country:

- France
- Netherlands (two responses from different organisations in the Netherlands)
- United Kingdom

3.1.3 Responsibilities of respondents

We had responses from overwhelmingly managerial and technical personnel.

3.1.4 Profile of respondents

Out of 26 respondents answering the question concerning their primary expertise, 14 described themselves as possessing technical expertise, 11 having managerial expertise and 7 with legal expertise.

The finding here is that there is less legal expertise amongst respondents. The implication is that teams still might face challenges in obtaining legal assistance and support, further

bolstering the need for some kind of platform or mechanism at the European level. The challenge of finding legal assistance was noted last year in the study concerning legal barriers to cross border CERT co-operation, which proposed the establishment of a legal helpdesk or centralised service which CERTs could call upon.

Reponses to question 5 show that most (14) were national / governmental CERTs out of a total of 25 responding to this question. Other respondents included LEAs (5) and other CERTs based in Europe 3).

3.2 Experience of information sharing

16 out of 21 respondents reported possessing some kind of information sharing policy or document. It is thus encouraging to see that most respondents possessed some type of policy or guidance.

We now turn to analysis of the questionnaire responses concerning experience of information sharing between CERTs and other stakeholders.

Table 1 Top three types of organisation to which respondents have sent information

Type of organisation	Freq
National / Governmental CERTs	20
Domestic Law Enforcement	19
Domestic Intelligence Agency	18

Table 2 Top three types of organisation from which respondents have received information

Type of organisation	Freq
National / Governmental CERTs	21
Other types of CERT; Domestic Law Enforcement	18

The responses to the questions above illustrate some differences concerning information transmission. That is to say, a broader number of organisations were involved rather than just national / governmental CERTs and LEAs in sharing information to address cybercrime. Most notably, the domestic intelligence agency appears as a common type of organisation that respondents are sending information to. This suggests that a focus on just national / governmental CERTs and LEAs in discussions about information flows with respect to tackling cybercrime may be missing a larger context. It also relates to findings from the study into sources of information relied upon by national / governmental CERTs. Further work would be necessary in this area.

Unsurprisingly, given the preponderance of national / governmental CERTs in our responses, information sharing with other CERTs more frequently than once a week was reported as the modal average of respondents.

Table 3 below indicates a summary split according to whether it sharing with CERTs happens more or less frequently than once a month.

Table 3 Regularity of sharing with CERTs

Regularity of sharing	Freq.
More frequently than once a month	12
Less frequently than once a month	8

Turning to sharing with LEAs, given the preponderance of national / governmental CERTs in our responses, information sharing with LEAs followed a broadly similar pattern. One respondent indicated they had not yet experienced information sharing with this type of organisation. Table 4 below indicates a summary split according to whether sharing with LEAs happens more or less frequently than once a month.

Table 4 Regularity of sharing with LEAs

Regularity of sharing	Freq.
More frequently than once a month	12
Less frequently than once a month	5

There was a more complex picture regarding the frequency of information sharing with LEAs. Five respondents reported that sharing with LEAs occurred once a month. Information sharing happening once a week but also once every 2-4 months were reported by 4 respondents each. The implication of this is that with, on the whole, a more fragmented pattern of information sharing, care should be taken (assuming this finding can be validated in a broader sense) that any measures that are put in place are proportional to the frequency of interactions: namely that investing considerable resources into a complex 'real-time' system, would be unnecessary (assuming the finding from question 11 is supported more broadly) given the relative slow pace of information exchange. This is also backed up by other empirical and anecdotal evidence from the LEA world which shows that the cross border processing of Mutual Legal Assistance Treaty requests for example, can take months or years to complete.

Finally, looking at information sharing with other types of organisation (e.g. MSSPs) 10 respondents indicated that they share with other types of organisation more frequently than once a week. The most infrequent occurrence of information sharing noted by the respondents to this question was once every 2-4 months. This suggests that other

organisations aside from CERTs and LEAs play a more regular role in information sharing to tackle cybercrime than is perhaps usually considered.

Table 5 Regularity of information sharing with organisations other than CERTs and LEAs (e.g. MSSPs, malware repositories)

Regularity of sharing with other organisations aside from CERTs and LEAs	**Freq.**
More frequently than once a month	15
Less frequently than once a month	3

In the context of the topic, this finding suggests that respondents are interacting with others (their constituents, MSSPs, organisations providing lists of malware, non-for-profit cyber-security research entities) on a more frequent basis than via LEAs and other national / governmental CERTs.

4 Legal factors affecting interactions between CERTs and other types of organisation – empirical findings

In determining the appropriate response to specific incidents, interactions with CERTs can be complicated by a number of legal factors that affect the extent to which information can be made available or retrieved from them. A primary concern in this respect is always the potential impact on future investigations and/or legal actions: where CERTs are involved, it is important to ensure the chain of custody, so that any evidence obtained does not become tainted because legal safeguards have not been met.

In the sections below, we will describe some of the main challenges to be taken into consideration.

4.1 CERT categorisation – legitimacy, scope, remit and competences

CERTs have become prevalent across the EU, with virtually all Member States either having established or being in the process of establishing national/governmental CERTs, i.e. CERTs that aim to act as a contact point for CIIP with other national/government CERTs and bear responsibilities for the protection of critical information infrastructure in their own country.

However, such national/governmental CERTs are not the only type of CERT; others may have a different focus or field of activities, including:

- A CERT working within an ISP or CSP whose constituents (users) are subscribers to the service.
- A CERT for a specific product, e.g. a router or particular piece of hardware, whose constituents are the users of that product. The users of products may be private users or organisations.
- A CERT within an organisation such as a company, or government department, or ministry where the constituents are employees. University CERTs may also have students and staff as constituents.

The distinction is important. Functionally, all CERTs tend to have at least one goal in common, which is problem solving in the field, rather than driving criminal prosecution or investigation. However, their formal remits can vary quite substantially: only national/governmental CERTs are likely to have a mandate established by law, whereas other types of CERTs are more likely to operate on the basis of their own statutes and/or a contract with a representative of their constituency. The difference is legally relevant: legislation can grant a national / governmental CERT certain competences or tasks which would not be available to private CERTs, e.g. to assist in criminal investigations, provide expert testimony, or otherwise collect or exchange evidentiary data with LEA or other stakeholders. These types of activities can be much more legally challenging for other types of CERTs, which legally speaking operate purely as private organisations with no further remit or mandate other than those available to any other company or private citizen.

This distinction can affect their ability to demand information from less cooperative stakeholders, as will be commented below, and can impact the value or validity of any information provided to or by them in legal proceedings.

Furthermore, the status and remit of CERTs may also impact the legal value of any evidence they provide through testimony. There is no barrier in principle that stops CERTs from providing expert testimonies or statements to LEA, judges or investigators, in the same way as any other experts might provide such testimony, and under the same conditions. However, depending from country to country, declarations and statements from public officers may have a higher legal value, such as a presumption of truth, which is not necessarily attached to statements made by private citizens, even if they are experts. Thus, the legal value of any testimony provided by national/governmental CERTs that have public officers in their ranks can be greater than that of testimonies from other types of CERTs. In the latter case, and assuming that no laws were broken by the person providing the testimony, judges will still be able to take the testimony under consideration, but he or she may have more freedom to accept or reject the veracity of the statement.[77]

Table 6 Governing mandate of respondents

Type of mandate	Freq.
Regulatory decree	12
Acts autonomously	3
Contractual basis or private for profit organisation	1

The most frequently occurring type of mandate from the respondents to this question was a regulatory decree, which is encouraging since this gives greater standing for the CERT to perform its activities, especially where complex decisions around for example the sharing of personal data are necessary. However, as other previous analysis has shown,[78] this is not always the case. In particular, some national/governmental CERTs are operating in a *de facto* capacity and may be based in university or within a governmental organisation. Thus, they may have a mandate stemming from their parent organisation but may be required (by fact of them being de-facto CERT of last resort) to intervene in a broader range of incidents.

[77] *This is an area of policy making which is governed by national law, and has not yet been harmonized at the EU level. In Belgium for instance, police reports must be drafted by legally competent officers or agents of judicial police. Their contents must be taken into consideration and recognized by the judge assessing the evidence, although this does not imply that they must be treated as absolute truth; other types of evidence can and must be considered by the judge as well, and may override the indications of the police report. The primary distinctive characteristic of the police report is therefore the fact that its findings may not be ignored by the court. G. BELTJENS, Encyclopédie du droit criminel belge, I, Brussel, Bruylant, 1906, art. 154, nr. 1-4; R. VERSTRAETEN, Handboek Strafvordering, Antwerpen, Maklu, 1999, p. 643, nr. 1535.*

[78] *ENISA national & governmental CERT Baseline capabilities document 2011*

Members of the EG discussing at the meeting placed CERTs' scope, mandate and remit as key considerations in their engagement with LEAs.

Some EG members drew on experience in the non-governmental, private CERT world and acknowledged that they had felt nervousness in both dealing with other CERTs who were not of the same standing or understanding their obligations to co-operate with LEAs.

Other in the workshop pointed to CERTs' activities and remits expanding in practice but also to a greater recognition of CERTs' role: a good example provide was the Swiss authorities recognition of SWITCH's role in tackling malware in their jurisdiction. Thus, even in the absence of a formal legal mandate through national legislation, the remit of CERTs can be strengthened through positive prior experiences.

4.2 CERTs as evidence holders

Given their role as primary contact points in case of security incidents, CERTs often have access to a significant amount of technical information that could later be used to assist in the investigation or prosecution of such incidents. Furthermore, they often have the required technical expertise to be able to interpret the meaning and significance of this information. Therefore, CERTs can be an important actor for obtaining relevant evidence, and can play this role for LEA, other CERTs and prosecutors, both within their own countries and abroad.

The value of this evidence in any future criminal proceedings can be strongly affected by the assurances that a CERT can provide with respect to its authenticity and integrity. In that respect, it is worth repeating that CERTs act as problem solvers first, with the legal qualifications and repercussions of specific incidents taking only a secondary role. Thus, it is not likely that most CERTs have implemented strong measures to ensure that potential evidentiary data is retained using processes that ensure their suitability for further criminal prosecutions. Evidence provided by the Expert Group during the meeting for this study suggested that CERTs considered themselves competent in handling evidence providing that clear guidelines were made available to them. This particular issue was flagged as a priority by 6% of the workshop group.

The workshop participants noted however that the information they collected was often not intended to be used as formal evidence in legal proceedings, but rather as mere intelligence by investigators, i.e. as information that they can use to conduct further investigations with a view of taking appropriate actions, including searching for formal evidence. In those circumstances, the de facto reliability of the information is still crucial, but legal assurances of authenticity and integrity are less important. Some experts also voiced a concern that if communication with LEAs was unidirectional or sporadic (noted as often being the case), then CERTs may unintentionally hinder evidence finding by deleting relevant information, because they are no longer aware of any on-going interest in the information. Ironically, this deletion is incentivised and encouraged by data protection rules, which require personal data to be

deleted when it is no longer necessary for the purposes of the CERT. The effectiveness of the CERTs' 'evidence holding' role was thus a function to a degree of the closeness of their relationship with the LEAs and the guidance they received: CERTs felt that they were effective partners if clearly informed and instructed.

Even if CERTs themselves have no strict ambition of acting as legally reliable evidence sources to other CERTs or LEAs, they should ideally be able to ensure that their interventions do not taint evidence held by third parties, especially entities targeted in malicious incidents.[79] This is however not as simple as it seems: an entity whose services have been knocked offline through a targeted attack is likely to be prioritising the re-establishment of its services over the logging of all relevant evidentiary data. Inversely, an entity which is currently under attack will likely value the cessation of the attack using any means necessary over the collection of suitable evidence. This is an area where the primary function of CERTs as problem solvers can be at odds with the objective of obtaining reliable evidentiary data: solving a problem quickly and efficiently can result in data being lost, e.g. when a corrupted (attacked) system is overwritten by a clean copy.

Thus, one of the key challenges is to ensure that processes are in place to allow CERTs to provide usable data. While it may not be realistic to ask for absolute assurances of integrity and authenticity of evidence in all cases (given that this is not the goal or ambition of most CERTs), the establishment of clear communications channels with LEA and other legitimate CERT partners plays a crucial role in ensuring that useful information can be provided.

4.3 Legal pitfalls of data sharing

The integrity and authenticity of information that may serve as evidence is not the only issue. As CERTs themselves are not in charge of driving criminal investigations or prosecutions, their data will inevitably need to be handed over to LEA, judges, investigators or prosecutors, or even to other CERTs, either in their own country or abroad. This raises specific challenges of its own.

A frequently recurring concern is data protection. The European legal framework covering data protection and privacy can be very stringent on when personal data can be processed; this will be particularly true when the personal data is indicative of possibly criminal activities, and when data is exported to a destination outside the EU.

CERTs already face such challenges when merely acting as problem solvers, since this often implies that they will be processing potential personal data such as IP addresses or user logs that identify specific users. In those cases, they will need to ensure they comply with data

[79] *There are analogous relationships for instance between psychologists and investigators, criminal profilers and a range of expert advisers.*

protection rules, e.g. by ensuring that the data they process is appropriately protected against loss or corruption.

However, data protection compliance becomes even more challenging when information has to be exchanged between a CERT and others who may be less known e.g. with an LEA or other CERT. This issue also came up in discussion during the informal Expert Group meeting. How can the CERT ensure that the processing involved (i.e. the exchange of information) is legitimate under the terms permitted by the Data Protection Directive? How should it ensure that the security of the data is sufficiently safeguarded? Will data be moved to a destination outside of the EU, and if so, have appropriate assurances been provided? And does the CERT have the required legal expertise to assess these issues with any degree of reliability?

At a higher level, the legitimacy of data sharing requests and any obligation to respond to these also depend on the status and mandate of the requesting party. If data (especially personal data) is provided to an entity that has no right to obtain it, then the CERT's cooperation with a request may be unlawful, and could even be criminalised as a violation of privacy. Confidentiality agreements with the constituency of the CERT can further complicate this picture, as the CERT may be barred from sharing information that another entity is requesting. Can a CERT determine in those circumstances whether a request for data is legitimate, i.e. whether the requesting party is itself authorised to receive and process the data, and whether the CERT has any overriding confidentiality obligations?

As noted above, CERTs are in general more focused on solving problems than in dealing with such questions of principle. None the less, when requests are made, CERTs will need to make a decision whether to share or not. Thus, there is a clear interest in establishing a framework for making this decision.

The expert working group ranked this as the third most important legal factor influencing CERT to LEA cooperation and placed it at the heart of a cluster of factors around legal protocols which were important for CERTs and LEAs to address in a systematic fashion. Thus, data protection compliance was clearly identified as a key concern by the experts.

4.4 CERTs in the prosecutorial process

It is worth re-iterating for clarity that CERTs generally do not play a significant steering role in criminal prosecutions, including in determining the legal qualification of incidents, identifying applicable laws or assessing the compliance of procedural/investigative measures with legal requirements in criminal procedural law. Formally, CERTs do not initiate criminal investigations or legal procedures, as this does not usually fall within their remit.

However a basic level of familiarity with legal definitions and interpretations of incident types can be useful, as can a basic awareness of existing investigative measures and competent

authorities, if only to avoid that CERTs unwittingly participate in investigations of noncriminal activity or respond to unlawful requests, which could conceivably result in the liability of the CERT itself. Furthermore, as stressed above, CERTs are often the first party to identify incidents and collect relevant information. Therefore, they are well positioned to inform LEA or criminal prosecutors of any incidents that may require further investigation or prosecution. As noted by workshop participants, this was not an uncommon occurrence, and a basic familiarity with the prosecutorial process is therefore useful to CERTs. The question of when CERTs, acting without authoritative legal advice, render amateur legal decisions which could annoy potential collaborators is also valid in this context.

CERTs outlined various experiences of involvement in the prosecutorial process. Two countries described cases where CERT action had meant that CERTs became liable through infringement of data protection laws (a point also related to legal standing, as a CERT with a clearer mandate based in legislation might have had a clearer justification for processing personal data). Nevertheless, the consensus in the room was that CERTs' domain experience in prosecutorial proceedings would continue to improve through trial and error. At the Expert Group meeting this factor was ranked fourth in importance.

4.5 Legal know-how and awareness

A first legal section of the questionnaire aimed to determine to what extent respondents were aware of the law, and which specific laws they were more/less familiar with.

With respect to **national laws**:

- Some awareness of all key legislation existed. While knowledge varied strongly from legal domain to legal domain, no domain was highlighted by any respondent as having no or only a superficial knowledge. Thus, respondents are generally confident regarding their understanding of domestic law;
- The strongest knowledge (rated as reasonable or higher by 70% or more of respondents) was in evidence concerning crime definitions, rules on digital evidence, privacy and data protection, data retention rules and national security;
- The weakest knowledge (rated as insufficient or less by 50% or more of respondents) was in evidence concerning rules on competent courts, legal value of evidence, and competition law.

All respondents reported at least "reasonable" understanding of any one specific law. 7 respondents reported 'expert' familiarity with definitions of computer and network misuse, followed by 6 indicating expert level familiarity with laws concerning investigations. Tables 7 – 9 illustrate the extent of levels of reported familiarity (from "reasonable" to "expert" for a range of different national legal frameworks amongst respondents.

Table 7 Ranking of numbers of respondents reporting "reasonable" familiarity with national laws and rules

National law or legal framework	No. of respondents reporting "reasonable" familiarity
Intellectual property protection laws	3
Laws with respect to the consequences of complaints Laws with respect to the legal competence to initiate criminal proceedings against the person[s] behind an incident Procedural measures in criminal investigations and laws for working with criminal justice community	2
Data Protection & Privacy law National security laws Laws with respect to the processes and procedures for registering complaints with LEAs	1

Table 8 Ranking of numbers of respondents reporting "mature" familiarity with national laws and rules

National law or legal framework	No. of respondents reporting "mature" familiarity
Laws with respect to the handling of complaints	7
Data Protection & Privacy law Laws with respect to the legal competence to investigate a certain incident Laws with respect to the consequences of complaints	5
Data Retention law Obligations for private sector parties	4

[ISPs, hosting providers, network operators] to cooperate with LEAs National security laws Intellectual property protection laws	
Laws with respect to the legal competence to initiate criminal proceedings against the person[s] behind an incident Laws with respect to the processes and procedures for registering complaints with LEAs	3
Definitions of types of computer and network misuse as crimes	2

Table 9 Ranking of numbers of respondents reporting "expert" familiarity with national laws and rules

National law or legal framework	No. of respondents reporting "expert" familiarity
Definitions of types of computer and network misuse as crimes	7
Laws with respect to the legal competence to investigate a certain incident	6
Laws with respect to the processes and procedures for registering complaints with LEAs Data Retention law Procedural measures in criminal investigations and laws for working with criminal justice community Obligations for private sector parties [ISPs, hosting providers, network operators] to cooperate with LEAs	5
Laws with respect to the legal competence to initiate criminal proceedings against the person[s] behind an incident National security laws	4
Data Protection & Privacy law	3
Laws with respect to the handling of complaints Laws with respect to the consequences of complaints Intellectual property protection laws	2

Thus, awareness of rules that affect the material tasks of CERTs was reasonably high, whereas rules impacting the tasks and processes associated with prosecution were relatively unknown. This is not unexpected, as it matches fairly well with the more pragmatic role and vocation of most CERTs. Experts in the working group echoed the finding of comfort with national legal

protocols and norms. This reflected that most of the CERTs involvement with LEAs was domestic and thus the protocols used were tried and tested. None the less, several experts highlighted that cross border collaborations had become increasingly more common over the recent years, and attributed this at least partly to the existence of better collaboration mechanisms at the EU level. Estonia in particular was acutely aware of domestic legal frameworks and how EU legislation could affect working practices that had been found to be effective for handling national incidents.

With respect to **international legal frameworks**[80]:

- The level of knowledge was generally much lower;
- All examined areas of law were reported as having insufficient or less knowledge by more than half of respondents;
- Respondents indicated most familiarity with respect to data protection and privacy, data retention and national security.

Tables 10 – 14 below summarise the extent of levels of reported familiarity (from "none" to "expert") for a range of different international legal frameworks amongst respondents.

Table 10 Ranking of numbers of respondents reporting "no" familiarity with international legal frameworks and rules

International legal framework or rule	No. of respondents reporting "no" familiarity
Laws with respect to the processes and procedures for registering complaints with LEAs Laws with respect to the consequences of complaints Procedural measures in criminal investigations and laws for working with criminal justice community	2
Laws with respect to the legal competence to investigate a certain incident Laws with respect to the legal competence to initiate criminal proceedings against the person[s] behind an incident Laws with respect to the handling of complaints National security laws	1

[80] *By which we mean normative international frameworks or model codes such as the Council of Europe 2001 Cybercrime Convention; the Data Protection Directive 95/46/EC or the JHA Framework Decision on attacks against information systems JHA 2002/222*

Table 11 Ranking of numbers of respondents reporting "superficial" familiarity with international legal frameworks and rules

International legal framework or rule	No. of respondents reporting "superficial" familiarity
Obligations for private sector parties [ISPs, hosting providers, network operators] to cooperate with LEAs Intellectual property protection laws	3
National security laws	2
Laws with respect to the processes and procedures for registering complaints with LEAs Laws with respect to the consequences of complaints Procedural measures in criminal investigations and laws for working with criminal justice community Laws with respect to the legal competence to investigate a certain incident Data Retention law	1

Table 12 Ranking of numbers of respondents reporting "reasonable" familiarity with international legal frameworks and rules

International legal framework or rule	No. of respondents reporting "reasonable" familiarity
Laws with respect to the processes and procedures for registering complaints with LEAs Data Retention law	5
Laws with respect to the consequences of complaints Definitions of types of computer and network misuse as crimes	4
Obligations for private sector parties [ISPs, hosting providers, network operators] to cooperate with LEAs National security laws Procedural measures in criminal investigations and laws for working with criminal justice community Laws with respect to the legal competence to initiate criminal proceedings against the person[s] behind an incident Laws with respect to the handling of	3

complaints	
Laws with respect to the legal competence to investigate a certain incident Data Protection & Privacy law	2
Intellectual property protection laws	1

Table 13 Ranking of numbers of respondents reporting “mature” familiarity with international legal frameworks and rules

International legal framework or rule	**No. of respondents reporting “mature” familiarity**
Data Protection & Privacy law Intellectual property protection laws	4
Definitions of types of computer and network misuse as crimes Procedural measures in criminal investigations and laws for working with criminal justice community Laws with respect to the legal competence to initiate criminal proceedings against the person[s] behind an incident	3
Laws with respect to the processes and procedures for registering complaints with LEAs Laws with respect to the consequences of complaints Laws with respect to the legal competence to investigate a certain incident	2
Data Retention law Obligations for private sector parties [ISPs, hosting providers, network operators] to cooperate with LEAs National security laws Laws with respect to the handling of complaints	1

Table 14 Ranking of numbers of respondents reporting "expert" familiarity with international legal frameworks and rules

International legal framework or rule	No. of respondents reporting "expert" familiarity
Definitions of types of computer and network misuse as crimes Laws with respect to the consequences of complaints Laws with respect to the legal competence to investigate a certain incident Data Retention law	2
Data Protection & Privacy law Intellectual property protection laws Procedural measures in criminal investigations and laws for working with criminal justice community Laws with respect to the legal competence to initiate criminal proceedings against the person[s] behind an incident Laws with respect to the processes and procedures for registering complaints with LEAs Obligations for private sector parties [ISPs, hosting providers, network operators] to cooperate with LEAs National security laws Laws with respect to the handling of complaints	1

As per the 2011 ENISA study "A Flair for Sharing", overall there were lesser degrees of familiarity with relevant international legal frameworks (with the exception of the definitions of computer and network misuse, personified in the 2001 Council of Europe Cybercrime Convention). The conclusions from question 16 and question 17 of the survey of 2012 remain broadly the same as the 2011 study, namely that familiarity with international efforts require further work.

Clearly, legal knowledge of CERTs is more focused on complying with national laws than on the international alignment of these rules. This was supported by the consensus in the expert meeting, where questions were raised even to the relevance of international law, especially considering that prior initiatives have virtually always required transposition into domestic law.[81]

[81] *We did not explore the extent to which respondents were aware of and could satisfactorily differentiate between national transpositions of international legal frameworks*

It is also interesting to note that awareness of national security rules scores fairly highly, both within a national context but also concerning those international legal frameworks that exist to serve similar purposes. This is likely a consequence of the fact that the majority of the responding CERTs were national / governmental CERTs, who often include CIIP as a priority of their mandate. As such, national security requirements are a higher imperative to them than might be the case for other categories of CERTs with a more restricted focus and remit. This was also reflected in the comments made by some experts regarding the important distinction between intelligence and evidence: for national security purposes, information made available as intelligence (de facto reliable but not necessarily having strong formal assurances of authenticity and integrity that would hold up in court) is more important than as evidence, where such assurances would be relevant. National security laws did not appear to unduly trouble the experts gathered for the workshop that ranked it towards the bottom end of their concerns.

This finding, compared with the responses to the question below is instructive in again supporting the analysis from the 2011 study ("A Flair for Sharing") which identified a gap between the understandings of national legislation vs. international harmonisation efforts, suggesting that further efforts at bridging the gap are necessary. At the more detailed level, respondents indicated familiarity with definitions of computer and network misuse, data retention law, laws relating to working with LEAs (competence to investigate), complaints handling, and obligations for private parties to collaborate with ISPs. Respondents still reported less familiarity with data protection and privacy law (one of the main conclusions from last year) indicating that this could remain as an issue to be addressed.

4.6 Laws as a barrier to receiving information

Table 15 illustrates the most frequently occurring law identified by the majority of respondents as being the explained or given legal reason for their request to be denied and its prevalence.

Table 15 Legal reasons given for denial and their frequency

Legal reason for denial identified by the majority of respondents	Prevalence of denial
National security laws Intellectual property protection laws	Always
Data protection and privacy law Liability concerns Confidentiality agreements	Frequently
Data Retention law Uncertainty about the consequences of information sharing	Occasionally
Definitions of computer and network misuse	Rarely

Procedural measures in criminal investigations and laws for working with criminal justice community	
Uncertainty about the identity of your organisation Uncertainty about the legal mandate of your organisation Uncertainty about the available competences in your organisation Rules with respect to the legal competence to initiate criminal proceedings against the person[s] behind and incident	Never

Uncertainties about various aspects of information relating to the identity, competence, mandate of the respondent's own organisation (following a request) appear to be less important according to the respondents. When set alongside some of the other responses (e.g. ranking of which factors are important), this suggests that the questions of uncertainty constitute a source of friction, imposing inefficiencies, but not an insurmountable barrier to information sharing. This is in contrast to data protection and privacy law; national security or IP protection laws, where barriers can be harder or even impossible to overcome.

When asked if/which legal barriers had resulted in the respondent ever being denied information in its interactions with CERTs:

- The general impression is that the invocation of legal barriers as a reason to block communications is relatively rare. Only privacy and data protection rules are indicated by more than half of respondents to be an occasional or common reason for refusing to provide information to the CERT.
- While other legal barriers occurred as well, they were reported as being rarer by respondents.

Thus, data protection compliance indeed appears to be the major legal challenge for CERTs when requesting information. Guidance on complying with this point is thus advisable. This was reflected in the working group which requested that best practice in this area would be useful to them organisationally.

4.7 Practices employed by CERTs to address legal factors

The questionnaire showed that an information sharing policy, disclosure policy or guideline document existed within 12 out of 17 respondent organisations; four had none, and one respondent was unaware of such documents.

However, as to whether these covered legal aspects, a further question concerning the mechanisms to address legal aspects of information sharing showed that only two respondents indicated that a legal guideline document existed. Four others relied on internal

legal expertise, and four on external legal expertise. Thus, ad hoc legal support through local expertise appears to be more prevalent than standardised guideline documents.

The respondents were also asked to indicate which legal factors they considered to be important in some way when dealing with other CERTs. Table 16 indicates the legal measures identified as in some way either important or unimportant by the majority of respondents. No legal measures were identified as being unimportant or very unimportant by a majority of respondents.

Table 16 Legal measures and their importance

Legal measure identified as being important when dealing with other CERTs by the majority of respondents	**Importance**
Availability of assurances from the [other] CERT with respect to data protection/privacy, i.e. on how they will process the data Existence of trust frameworks [e.g. confidentiality agreements or data sharing policies] with CERTs Certainty about the legal mandate of the [other] CERT Existence of customs, arrangements or practices [possibly merely informal] that have worked well in the past Availability of legal expertise	Very important
Familiarity with the general legal culture of the country of the [other] CERT Similarity of the general legal system of the [other] CERT Existence of customs, arrangements or practices [possibly merely informal] that have worked well in the past Certainty about the legal mandate of the [other] CERT Availability of guidelines that help your organisation to decide when data can be shared	Important
A clear internal structure within your organisation that determines who makes decisions/takes responsibilities for data sharing Similarity of the general legal system of the [other] CERT Use of disclaimers of liability to manage your organisation's responsibilities	Neutral

Responses to question 24 detailed above suggest that the existence of trust frameworks (such as the TF-CSIRT TI scheme, or participation in FIRST) are accorded the most importance. TF-CSIRT and FIRST were noted as the touchstone events for the Experts at the workshop; in the case of CERTs, the drum beat of conferences and very nature of their rapid use of technology meant that the community felt interconnected. However, some recognised that increasing size and scope meant face-to-face contact was becoming less feasible and less important, raising the need for more structural collaboration mechanisms.

There was more ambivalence about the availability of guidelines, use of disclaimers, and existence of common customs, practices. Paradoxically (reviewing this in relation to question 17 and question 18) we see that the similarity of the legal system is not accorded that much importance, yet this would be the very 'avenue' to overcoming the uncertainty between national legislation and international legal frameworks. A possible explanation for the limited value accorded to this factor by the respondents is their lesser familiarity with international legal frameworks as discussed above, implying perhaps that they are unable to assess similarities with a reassuring degree of certainty. Given the complexity of law in this domain, this would merit further investigation aside from purely looking at these factors from a single perspective (i.e. detailed analysis to explore whether there is an observed cause and effect between first understanding national laws and then international legal frameworks.

This would seem to support the assertion that prior experiences, agreements and personal contacts are the major factor for establishing trust, from a legal perspective as well.

Given the limited numbers, conclusions are hard to draw at this stage, but it seems clear that CERTs have only limited access to legal expertise or guidance. This implies a real risk of noncompliance with the aforementioned legal rules. However, expert feedback from the workshop indicated that some CERTs felt comfortable in this position, relying primarily on the instructions that they may receive from LEAs and other partners, and furthermore understood the process of collaboration with LEAs as one where mistakes would be made. Experts voiced a call for frameworks for co-operation that were more error-tolerant, in which minor mistakes would not necessarily result in significant (legal) consequences thus permitting more opportunities for learning.

4.8 Impact of legal challenges

Noncompliance with legal rules theoretically creates the risk of future legal proceedings being disrupted or derailed entirely. From the perspective of the CERTs themselves, it is equally important to ensure that their actions are sufficiently compliant with applicable laws to avoid their personal implication in any legal procedures (i.e. to avoid being accused of any wrongdoings themselves). To determine to what extent this issue really manifests itself, the questionnaire inquired whether the CERTs had any experiences in this respect themselves, or whether the respondents had any awareness themselves of such issues occurring with other CERTs.

The questionnaire yielded insufficient replies to indicate whether this occurs in reality with any level of frequency. The present responses indicate only one case known by an LEA respondent where a CERT has been confronted with legal challenges as a result of its decision to share information with third parties. The workshop did not result in further examples: two cases were identified in which a CERT itself got into legal difficulties for not complying with data protection rules; however, the impact on any further legal proceedings was unknown.

While the data obtained through the questionnaire is too limited to draw extensive conclusions, some provisional observations can be made:

- Replies suggest that CERTs are not commonly confronted with legal barriers, other than data protection compliance. Thus, data protection legislation appears to be a major legal factor. This perception may be affected by the current revision of the European legal framework with respect to data protection[82], via the proposed new Data Protection Regulation[83] and the proposed Law Enforcement Data Protection Directive[84]. This proposed Directive is expected to fill a gap not covered by the existing Data Protection Directive, namely the problem that the latter does not apply in the law enforcement sector, which can include some CERTs. From that perspective, the newly proposed Directive could be beneficial by setting a number of common ground rules for all CERTs. Furthermore, the general Data Protection Regulation, which would apply to private CERTs, also currently contains a recital specifically addressing CERTs[85], supporting the legitimacy of their activities. This would provide much stronger assurances as to the legal basis of the CERTs' work and the resulting information, and could help overcome some of the challenges that CERTs encounter, as noted above.
- The data suggests that positive **legal awareness of national laws exists** amongst respondents (no respondent reported as having 'insufficient' or 'no knowledge' of the

---

[82] *See European Commission's website on Data Protection Review (2011) available at: http://ec.europa.eu/justice/data-protection/review/index_en.htm [accessed 11/10/2012]*

[83] *Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data; see http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf*

[84] *Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data; see http://ec.europa.eu/home-affairs/doc_centre/police/docs/com_2012_10_en.pdf*

[85] *Recital 39 of the proposed Regulation, noting that "The processing of data to the extent strictly necessary for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the concerned data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems."*

identified relevant national laws), but international harmonisation efforts are less known. Thus, cross border collaboration in particular may be complicated.

- Standardised approaches for dealing with legal challenges are relatively rare. Policies and guideline documents addressing legal problems were virtually non-existent, and legal expertise was not commonly available. Thus, there is likely a lack of legal know-how with CERTs.
- As a way for addressing legal problems, the CERT community values prior experiences, cooperation agreements and personal contacts over more formal instruments.

4.9 Views from the Expert Group meeting on the importance of legal and regulatory factors

Those participating in the Expert Group meeting were requested to vote on the importance of legal and regulatory factors, on the basis of their own working experiences. Some of the main findings and observations were integrated in the sections above. Table 17 below provides a full overview of all votes cast by the meeting participants themselves:

Table 17 Ranking of legal factors from the Expert Workshop

Legal Factor	Votes
Privacy and data protection compliance	14
CERT categorisation: Scope of mandate and remit	12
Specific legal pitfalls on scope: definition of computer and network misuse	9
CERT in prosecutorial process	7
Data retention law Laws with respect to the legal competence to investigate cross border incidents	6
Obligations for private sector parties to cooperate with LEAs	5
CERT as evidence holders: intelligence means it can b e used far more flexibly	4
Laws with respect to the legal competence to investigate a certain incident	3
Laws with respect to the legal competence to imitate criminal proceedings against the person behind an incident Procedural measures in criminal investigations and laws for working with criminal justice community	2
Intellectual property protection laws National security laws – certs with CNI remit have a wider competence	1

Confidentially agreements Laws with respect to handling complaints Laws with respect to the consequence of complaints Laws with respect to the processes and procedures for registering complaints with LEAs Laws with respect to the safekeeping of evidence	0

4.10 Conclusions on legal and regulatory factors

The section above introduced some of the primary legal challenges that CERTs can face in their day to day operations. Obviously, the reality and impact of these legal barriers depends to a large extent on the mandate, legal basis and contact network of the CERT, including particularly any status as/link to law enforcement bodies. Depending on this mandate and legal background of the CERT, it might be able to avail itself to similar investigation and information exchange rights as a law enforcement body, e.g. because it is itself part of such a law enforcement body, or because it has sufficient formal or informal ties to a law enforcement body to organise any legally ambiguous activities through that body, thus legitimising information exchange activities.

The reality is however that the CERTs' focus on efficient problem solving leaves limited time and resources for legal questions and challenges. Legal expertise is not ubiquitous within CERTs, nor do CERTs generally consider legal assessment to be a part of their core tasks or responsibilities. Information exchanges thus far are organised more on the basis of subjective trust as established through prior interactions than on the basis of any formal legal assessments. In effect, personal contacts and individual familiarity with other bodies plays a significant role in deciding which of these bodies can/should be cooperated with. Finally, CERTs are keenly aware that the information they provide to third parties (LEAs or other CERTs) is typically intended to be used as intelligence that triggers further investigations, rather than as evidence to be introduced in legal proceedings. Therefore, while their own compliance with the law is a concern, rigorous procedures to safeguard and ensure the legal value of collected information are generally less of a priority.

This also implies that information exchanges or other forms of collaboration with other CERTs, LEAs or other stakeholders are likely to occur in a gray area, especially in an international context where the mandate and applicable rules are not always uniformly known. In those cases, legal compliance is not systematically assessed, which can ultimately call the legal value of the information as evidence into question. The legal impact of unlawful exchanges may vary from country to country and from case to case, but the overriding concerns will always be the suitability of the information as evidence in further proceedings, and of course the

civil/criminal/disciplinary liability of the participants in an unlawful exchange. Especially on this front – international exchanges – further guidance to ensure compliance is advisable.

5 Operational Factors affecting CERT co-operation with other stakeholders – empirical findings

Aside from the legal basis covering the mandate and framework of interactions and co-operation between CERTs and LEAs, operational co-ordination is an important characteristic. Collectively working on a number of activities or measures helps to smooth co-ordination and thereby increase trust, both between CERTs and also between CERTs and LEAs. Experts in the workshop held for the research noted the intertwined nature of operational factors and legal factors. Moreover they noted that the importance of operational or legal varied with the situation.

As has been noted, it is important to consider the different cultural and organisational character of these two different stakeholders. These differences become more apparent when considering operational co-ordination.

- CERT teams tend to work on an informal basis with frequent direct communication. Trust is built up on an ad-hoc basis and stimulated by observed characteristics of credibility and intellectual knowledge. CERTs value flexibility, rapidity and scalability of response
- LEAs, by comparison, as a general statement, work more on the basis of procedures, policy and rules. Although trust also exists and is built from interpersonal relationships, formal procedures takes a more substantive role in their activities, because of LEAs' mandate and the fact they might be the first in a long chain of stakeholders (resulting in a court appearance).

Undoubtedly, trying to address these two viewpoints in the interests of collaboration is a complex and tricky task. Indeed, the divergent objectives may be irreconcilable. A first approach which can build trust is the exchange of information relating to operational conditions or scope of what parameters governing collaboration. Such information can help reduce uncertainty and create a more realistic set of expectations. Similarly, the fact that information can go into a 'black hole' once it leaves the CERT can inhibit information sharing. Anecdotal evidence in the specific context of CERT-LEA collaboration[86] suggests that such sharing can increase if the originator has feedback on what happened to the information, whether it was of use and what contribution/added value it made to the activities of the recipient. However, there might be good reasons for this. From the LEA perspective (e.g. where the information becomes part of a criminal investigation), certain operational rules might apply which would prevent this feedback from being provided.[87]

Articulating the added value for both sides in respect of operational co-operation will be key in any respect: whether that be passing on IP addresses from CERTs to LEAs, helping to isolate

[86] *Anonymous interviewee May 2012 and 21 June 2012*

[87] *E.g. see the companion report into Legal/Regulatory Factors affecting co-operation between CERTs and other stakeholders, specifically the discussion on procedural rules for investigations*

and disrupt incidents (e.g. compromised home PCs via bot-net remediation activities) or the LEA passing on details of malicious activities or modus operandi to a CERT.

The **physical exchange of personnel** between CERTs and LEAs is another case in point. Examples in some countries (e.g. the Netherlands, Germany) illustrate that LEAs working alongside non law enforcement personnel may be beneficial. This could be either via permanent liaison posts, secondments or other mechanisms. In a similar vein, the participation of CERTs and LEAs in joint exercises and training may be another operational factor which could be used to encourage information exchange and co-operation.

Another operational aspect relating to trust is that of onward **use of data provided by CERTs**. This situation is made more complex by the fact that the LEA may only be at the start of a procedural chain resulting in the prosecutor taking the decision to bring the evidence to court. Across Europe, in different countries there is a different threshold or decision point for the public prosecutor to become involved once the police have received a report, conducted further gathering of information and intelligence and prepared a case. In some jurisdictions the police officer can progress these preparations quite far, whilst in other jurisdictions this may not be the case and the public prosecutor takes a decision early on to proceed with the investigation. These decisions all affect how and what type of feedback may be returned to a CERT as a provider of information.

There is the question about the extent to which the LEA is duty bound by law to prepare a case on each and every victimisation or witness report. In the case of cybercrimes and incidents this could constitute some considerable workload. There is uncertainty about the level of discretion LEAs possess in following up on victimisation / witness reports (which may constitute an operational barrier to sharing of information).

If the LEA provides assurances of anonymity in order to obtain the participation of the CERT (or the organisation that has been victimised or is the target of attacks), there is a risk that this may not be upheld if and when the case gets to the public prosecutor. The public prosecutor, after reviewing the merits of the case, could be driven by bringing the case to court, subject to the judicial requirements of transparency and a fair trial, rather than respecting the anonymity of the witness (in this case the CERT).

Other issues may concern **security clearances** (particularly criminal intelligence analysis function and CERTs) – LEAs may not be authorised to disclose information about criminal activity to CERTs. By way of example, this aspect came up in the general context of information sharing in the United States concerning information sharing between the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI) and IT-ISAC where classification levels proved an obstacle to information exchange. This is subsequently being explored in the Defence Industrial Base (DIB) Information Exchange Pilot.

There is also the question of **information exchange** and the use of common taxonomies and classifications. This factor is made more complex by the fact that although some parts of information about an incident may be different for CERTs or LEAs (e.g. the LEA might want to know how much the victim lost) there is still a lot of information in common but it is used for

different purposes. Efforts by the Anti-Phishing Working Group (APWG) to create a set of 'e-Crime' extensions (initially focusing upon phishing) to the IODEF RfC 5901[88] are suggestive of a possible solution to this approach – where the same framework for collection of information is used by different parties for different purposes.

Evidence acquisition may also be considered one of the most important issues, especially in complex cases involving remote access of a suspects PC, drop-zone or bullet proof hosting service. In particular, this may be a barrier in respect of whether the CERT is aware or can easily obtain advice on the required standard of evidence that the LEA / prosecutor would need. There is also the question of **access to suitable forensic capability** at the national and European level.

The table below expands some operational factors identified from the preparatory phases of the study, classifying each factor into a group. It is interesting to note how this grouping differs from that which came out of the Expert Group meeting in September 2012. For example, the Expert Group meeting clustered them around internal/external factors and those affecting a CERT in its early phases of operation compared to when it might be more mature. Table 18 below summarises our own initial clustering.

Table 18 Grouping of operational factors

Group	Factor
Governance	Different / unknown policies and procedures
	Absence of clearly defined policies
	Financial burden / opportunity cost
Processes	Security clearance/certification
	Language barriers
	Different / incompatible/unknown workflows
	Duplication
	Lack of standards in reporting
	Wrong channel / addressee
Personnel and training	Lack of known & trusted personnel / inexperience
	Previous poor experience in sharing information
	Lack of confidence/clarity in your/their official status
Tools and technology	Lack of early warning / Knowledge Management tools

[88] *Extensions to the IODEF-Document Class for Reporting Phishing http://www.faqs.org/rfcs/rfc5901.html*

	Lack of common case management tools
	Lack of secure communication channels
	Administrative problems: inappropriate time stamp
Information	Lack of clarity on what the other party will do with the information
	Insufficient / inappropriate detail
	Lack of service catalogues
	Lack of information on understanding of role and parameters for co-operation

5.1 Governance

We define governance as consisting of the set of customs, policies, laws and institutions affecting the network of agencies/institutions involved in operational aspects of cyber-safety. Governance is an apt descriptor in this situation as it describes the activities of parties with limited control/censure ability over one another, differing goals but some interdependence such that there is a requirement to have a relationship arrangements in place[89].

Different /unknown policies and procedures

Interviews with CERT practitioners[90] suggest that more established CERTs, operating within the open source/public domain have little issue with extracting information from un-sourced areas, regardless of sourcing and policies and procedures: "CERTs have traditionally been open to information sharing and have had little or no reservations towards receiving information from open and previously unknown sources. Or from sources that will remain anonymous forever. That is especially true with CERTs that are tasked with protecting public and unclassified networks."

In the domain of communications between CERTs and their peers, there is evidence that practitioners through multiple interactions have come to be less concerned about others' policies and procedures. A Finnish practitioner suggests that this is through continuous interaction and the benefits it has reaped: "I have an opinion that this is something of cultural thing that has evolved through the discovery of the added value of sharing". Moreover benefits are often indirect "There appear to be more or less hidden networks of data exploiters that build on top of data donated by others and eventually feed the augmented/modified/enhanced data back for circulation - for the other exploiters to churn away". Finland's CERT-FI point to the development and greater use of their Autoreporter tool

[89] *James N. Rosenau, (1995) Governance in the Twenty-first Century, Global Governance , Vol. 1, No. 1*

[90] *Anonymised interviews conducted in (May 2012)*

as manifestation of their success in concentrating upon achieving a clear set of internal mechanisms.[91] Regarding information they obtain, CERT-FI receive normalised and correlated cyber incident information about Finland through various intermediaries that in turn have obtained the information from various donors and other intermediaries. Many of the original donors quite probably don't have any expectations for the eventual use of the data and might never hear direct feedback about what was achieved by exploiting the data.

In CERT-LEA interactions however there is evidence that an **absence of clearly defined policies have a negative impact on sharing information**. In the case of some CERTs they are concerned with what the LEA will do with the information if they haven't worked with them before. In the case of police they are concerned with evidential record and are unlikely to share if the sensitivities of their investigation are exposed. A culture in the police is to establish Memorandum of Understanding (MoU) prior to information sharing in order to ensure that they are covered under data protection legislation. The key aspect with the question is 'unknown' procedures; if LEA and CERT communities are informed of the processes and policies of the organisation, or pilot an information exchange, the salience of the issue is mitigated.

Financial burden, opportunity cost or competing priorities

Financial burden of information-sharing involves costs relating to the work to ensure information is packaged so it can be shared; consultation/legal costs to ensure that the CERT/LEA is within its mandate to share the relevant information. Competing priorities and opportunity cost are different ways of considering scarce resource allocation. In an era of austerity and cutbacks these considerations may have a significant at both the macro and organisational level. Evidence of such barriers is probably most telling in the LEA domain where issues of public spending retrenchment and the need to surge to meet operational priorities are keenly felt. There is a concern in the LEA community that budget cuts may affect their ability to operate effectively in this space and to collaborate effectively with cyber partners.

5.2 Processes

We define processes as the administrative and security-driven actions CERTs and LEAs must undertake to facilitate information-sharing.

Security clearance / certification

Security clearances are clearly felt to be significant by practitioners in security-related CERTs/national agencies and in the LEA world where activity relates to national security and serious crime. Interview evidence suggests that classified environments bring added requirements that tend to limit the flow of information outside it. Legal requirements for

[91] *Koivunen Erka, (2010) Effective Information Sharing for Incident Response Co-ordination: Reporting Network and Information Security Incidents and Requesting Assistance Aalto University School of Science and Technology Master's Thesis*

personal information, communications privacy, criminal investigations, corporate secrets and national security work counter to the "return of giving" principle.

Clearances can be advantageous and engender greater sharing between 'cleared' agencies/individuals because that 'kite-mark' of trust is mutually recognised. However these environments of trust and information sharing may be separated from one another and operate as islands of information sharing: what one interviewee called 'trusted circles'.[92] The potential for failure to share appropriate information is clear (as if you are not in the right island then the other party might have significant institutional and bureaucratic barriers to overcome to co-operate), although it may be the case that these environments encourage cross-organisational working behaviours; this is particularly true in the intelligence agency/cyber CERT context.

A "need-to-know" policy also limits distribution to those not only with the requisite clearance level but those with a subject matter interest. This environment implies that data is only requested for a given purpose and through documented procedure. There are certainly examples in the CERT environment where this is required, however there was some misgivings that adequate scrutiny must be in place to ensure information is not "over-classified" and if there genuinely A Need to Know Principle at stake.

Language barriers

The language in the CERT community, driven by the technology, is English. This proves to be little problem in the CERT world engagement but may be more problematic when LEA activity is required from a country of a different jurisdiction. Scholarly reporting on police information flows[93] cite the importance of informal levels of communication between police agencies as expediting action and increasing the flow of information.

Different/incompatible/unknown workflows

Processes of working are established in the CERT community but the police's practices are a 'known unknown' to many CERTs. The LEA workflows are also driven by investigative, or prosecution priorities which can mean that addressing the CERTs concerns may be a second order priority for them.

Duplication

This arises when there is more than one bilateral CERT to LEA relationship and multiple CERTS may be feeding LEAs with reporting or vice-versa. This can lead to circular reporting where a duplicated report of an incident X may be interpreted as a corroborating piece of reporting regarding incident X.

Lack of common standards in reporting

[92] *Anonymised interview 31 May 2012*

[93] *Information Flows and Fusion Center Guidelines (2006) United States Department of Justice.*

Technical reporting can be difficult to interpret between CERTs and LEAs. LEAs in each country often have established protocols for rendering information so that it can be held within their corporate records effectively or to comply with legislation. This means important information can often be buried in reporting and not highlighted – as police are required to caveat and cushion their findings as appropriate.

Wrong channel/addressee

CERTs sometimes misdirect information.[94] On the other side, LEAs are also not always aware of which CERTs is best placed to deal with problems; LEAs tend to go to CERTs they are in contact with in first instance in order to establish which CERTs may be best placed: this 'validation' through contact should be borne in mind as a behavioural feature that can be harnessed.

5.3 Personnel and Training

These factors concern personal relationships, and the importance of front-facing staff competence in understanding their roles and responsibilities to ensure information sharing occurs.

Lack of known & trusted personnel/inexperience

There are considerable fixed costs associated with initiating a relationship with an unknown party. Scholars of police information sharing note the tendency for police agencies to trust those with pre-established reputation[95] in a particular investigative/technical/research expertise amongst police agencies. An example in the United States is the Milwaukee Police Department (PD) which undertook investigative research in domestic violence cases and became recognised as a centre of best practice. Milwaukee PD also engaged in extensive 'road shows' outlining what they'd learnt and getting in front of audiences. In short, LEA practitioners tend "work with who they know" either by reputation or personal experience. This is less pronounced on the CERT side where networks may be more established. Personal relationships however do matter, and it is the 'messenger as much as the message' that it important.

Previous poor experience in sharing information

The literature on CERTs suggest that particularly in their inception phase their information sharing strategies can be misdirected or that they have a poor experience of info sharing. This however is understood as learning by doing. When CERTs reach maturity in their relationships and their expectations of a partner are not fulfilled and they have a 'poor' experience' it is likely that they will be less forthcoming in future.

---

[94] *Koivunen Erka, (2010) Effective Information Sharing for Incident Response Co-ordination: Reporting Network and Information Security Incidents and Requesting Assistance Aalto University School of Science and Technology Master's Thesis*

[95] *Alexander Wiess, Northwestern University, (1998) Informal Information sharing among Police Agencies https://www.ncjrs.gov/pdffiles/fs000233.pdf*

Lack of confidence/clarity in your/their official status

If the information recipient is unsure in their role or their status is unclear it is likely that this will impact on the confidence that the information emitting agency will place in them.

5.4 Tools and technology

These factors relate to the differing standards in place between LEAs and CERTS and amongst them which may impact on information sharing

Lack of early warning/Knowledge Management tools

Without clear corporate records of organisational information which can be exploited, there is potential for communication to be ineffective or lacking in vital detail. Practitioner's lack of confidence in their corporate records may make them reluctant to engage others or share information because they believe that they are only telling 'half the story'.

Lack of common case management tools

Different CERTs track cases in different ways however at some level there is a commonality because they follow a similar cycle. For LEAs, different jurisdictional and legal frameworks have inhibited common case management. Between LEAs and CERTs there is a considerable gulf between case management systems: often the LEA's case management system will focus on the evidential requirements and sequence cases in a way which makes extracting relevant information for CERTs difficult.

Lack of secure communication channels

A particular challenge in instances of communication between public facing agencies and those involved in the security world is bridging security domains. The process of transferring relevant information from a non-secure to secure system for examination or vice-versa is time-consuming and involves frictional costs.

Administrative problems: inappropriate time stamp

A global system of CERT-LEA co-operation involves such technical problems such as inappropriate time stamps that appear trivial but can have significant consequences for evidential enquiries involving careful piecing together of a timeline of activity.

5.5 Information

This group refers to the structure and content of the information delivered through information-sharing mechanisms

Lack of clarity on what other party will do with information

This is a symmetric barrier in that LEAs are concerned with the evidential process and can therefore be reluctant about sharing information when they have little control over its use. On the other hand, CERTs feel that their information goes into a 'black hole' of evidential enquiry and is not being acted on. This feeling can deter CERTs to make the effort to share as

they are given little insight into their information's insight. However, this information may prove critical to an investigation or spur a new avenue of enquiry.

Insufficient detail/inappropriate detail

Without significant context as to an LEA's or CERT's remit and character, it is likely that information received may lack the requisite detail and thus have limited utility. Following up by requesting more information may cut across sensitivities for LEAs or seem unlikely to reap dividends from a CERT perspective

Lack of service catalogues

Service catalogues consist of a list of services that an organization provides, and have use for that organisation's interlocutors. In the CERT space they are updated to reflect roles and responsibilities – in the LEA domain they are less prevalent: this may be problematic for CERT interlocutors who have expectation levels around service catalogue form and function.

Lack of information on understanding of role & parameters for co-operation

Understanding roles and how information is used is key for both LEAs and CERTs. Although many CERTs highlight their role on their websites and communications (e.g. via the IETF RfC 2350 model[96]) and use information generically in a similar way, this is not the case with the LEAs who may not be able to provide clear cut information on how data exchanged will be treated and what the roles and timelines of a relationships will be.

Having described in the previous section what the operational factors are, we now present evidence from the questionnaire responses, supplemented by analysis of the Expert Group workshop, as to their prevalence in a real world context.

5.6 Existence of collaboration and supporting mechanisms

We began by trying to understand the extent of regular collaboration between CERTs and LEAs.

A majority (10 out of 13) of respondents indicated some form of regular collaboration with LEAs in the online questionnaire. The expert working group appeared to treat information exchange with the police as a routine part of everyday business. Two CERTs were cited (historically in France and currently in Romania) as having LEA officers seconded within their CERT. Additionally CERT professionals worked as part of LEA at the supranational and national levels (e.g. Interpol and SOCA in the UK).

We then asked about types of collaboration mechanisms used.

---

96 *Brownlee, N. and E. Guttman (1998). "Expectations for Computer Security Incident Response", IETF Request for Comments (RFC 2350); available at: http://www.ietf.org/rfc/rfc2350.txt [accessed on 11/10/2012].*

Table 19 Prevalence of different collaboration mechanisms

Type of collaboration mechanism	No. of respondents reporting its use
Unstructured / informal communication	8
Collaboration in f2f or remote forums	6
Joint exercises	5
Structured / formal communications Production of common material	4
Secondments/attachments	3
Joint training	2
Common workflows Other	1

Out of those reporting the presence of a mechanism of regular collaboration, unstructured / informal communication was the most prevalent form of collaboration mechanism, followed by collaboration in face to face (f2f) or remote forums and exercises. Whilst informal/unstructured collaboration was prevalent as a form of interaction, experts at the workshop agreed that as the CERT and LEA network increased in size and scale, remote and more formula-driven interaction would increasingly become the norm

A majority (10 out of 14) of respondents reported the existence of a case ticketing system which is encouraging. However there was lukewarm endorsement in the Expert Group that this was a priority concern.

Perhaps surprisingly, there was a majority (12 out of 14) reporting the existence of a digital forensics capability. Although this might be obvious for LEAs, for CERTs (with a remit of remediation), the presence of a forensic tool set is somewhat surprising. However, the responses might be coloured by a different understanding of the term. Digital forensics was not a subject of major discussion with the Expert group, potentially reflecting the make-up of the expert group as national governmental CERTs rather than other non-governmental CERTs with an investigative function.

11 out of 21 respondents indicated that their digital forensics capability covered 'attacks against information systems'. Four respondents respectively indicated that their capability covered either crimes facilitated by computers or imaging and forensics associated with crime scene evidence.

Responses to this question are insightful with respect to the different scope and interests of national/governmental CERTs and others, especially LEAs, where evidence suggests that many have a remit covering frauds and other content related crimes where the computer is the means and not the target. Although this only applies to digital forensics, it may be seen that this area is one of the most obvious where practical co-operation is required. This needs to be explored further.

We then asked about which factors were the most important with respect to co-operation. Table 20 illustrates the most frequently identified operational factor alongside its importance. Four respondents indicated that common tools were unimportant and three that common standards were unimportant.

Table 20 Importance of operational factors

Operational factor identified as being important when dealing with other CERTs by the majority of respondents	**Importance**
Known and trusted contact Understanding of the other party's role and parameters for co-operation	Very important
Clear and transparent policies and procedures Technical capabilities [e.g. encrypted communications] Clear and transparent mechanisms for information sharing	Important
Common tools [e.g. workflow/case management/knowledge management] Common standards [e.g. for reporting of incidents]	Neutral

The factors judged to be of most importance were the known and trusted contact and an understanding of the role and parameters for co-operation of the other party. This was reflected in the Expert Group which accorded 'information on role and parameters for co-operation the most votes, making this the highest ranked factor. Whilst some of these can be addressed via existing mechanisms (support for national / governmental CERTs' face to face interactions and working sessions), some of the others may require a more 'interventionist' style approach, especially concerning establishing clear and transparent policies – levelling the playing field for interactions as it were.

Nonetheless, this seems to show that uniformity of tools and standards is not as important; informal links are very important; as are secure communications. Although the latter was not prioritised by the Expert Group which instead saw this as a sign that the CERT and LEA relationship lacked maturity or capacity to understand how they could effectively ensure their messaging was secure.

5.7 Operational barriers to information exchange

We then asked about what operational factors were identified as a reason to deny an incoming request. Table 21 illustrates the ranking of the frequency of those reasons identified by respondents.

Table 21 Operational factors identified as a reason to deny an incoming request

Operational factor identified as a reason to deny an incoming request	Freq.
Insufficient detail/inappropriate detail	7
Security clearance / certification Wrong channel/addressee	6
Lack of known & trusted personnel/inexperience Financial burden, opportunity cost or competing priorities Previous poor experience in sharing information	4
Lack of secure communication channels	3
Lack of clarity on what other party will do with information	2
Different /unknown policies and procedures Different/incompatible/unknown workflows Information on understanding of role & parameters for co-operation Duplication Lack of confidence/clarity in your/their official status Administrative problems: inappropriate time stamp Not sure/Don't Know	1

The responses to this question can be contrasted with those to question 35 (see below). In particular, it seems that the question of insufficient detail in the response is a challenge across both, as is security clearance (again supporting the contextual issue identified earlier regarding the focus of national government CERTs). Other more well-known popular reasons include wrong channel/addressee and lack of known/trusted personnel. Activities to address these might include providing greater detail and specifying who can do what in the numerous contact lists; what channel is suitable (e.g. information concerning widespread cyber-attacks on critical infrastructure might need to go through classified channels) and stimulating further initiatives to help peers get to know each other.

Table 22 Operational factors identified for the respondents own request to be denied

Operational factor identified as a	Freq.

reason for the respondents request to be denied	
Not sure/Don't Know	5
Wrong channel/addressee Insufficient detail/inappropriate detail	3
Security clearance / certification Lack of known & trusted personnel/inexperience Lack of confidence/clarity in your/their official status	2
Different /unknown policies and procedures Lack of service catalogues Information on understanding of role & parameters for co-operation Financial burden, opportunity cost or competing priorities Communication barriers Administrative problems: inappropriate time stamp	1

Understandably, respondents reported that they were unsure as to why their request was rejected (indicating perhaps poor transmission of justification or mistrust of plausible and detailed explanations). After this, the next two most popular reasons were wrong channel/addressee and insufficient / inappropriate detail. We may draw two conclusions out of this: firstly that the provision of network lists is not necessarily enough, and secondly that the requests need further detail. Perhaps, in addition, further guidance should be created on teams providing some type of keyword to use if they communicate that the request was rejected (e.g. 'rejected due to xxx').

Paradoxically, in both responses to question 34 and question 35 mechanisms accorded policy interest and support either received low recognition or were not mentioned (e.g. lack of common management tools and lack of early warning mechanisms). Lack of common case management tools came a relatively high (5 or 6th) in the expert's listing of factors and lack of early warning/KM tools joint 6th.

5.8 Information exchange standards

Bespoke structured data formats appear to be the most popular model for IE standards. Three out of seven respondents indicated that this was their preferred format. One respondent indicated using bespoke XML and one the IODEF INCH format. Whilst limited, this supports a view either that efforts to create common standards are useful and aiming at plugging a gap, or that CERTs prefer to do things their own way (a view supported by anecdotal evidence from discussions at the FIRST Conference in Malta in June 2012). The implication is that perhaps creating common exchange standards may be a waste of effort (given the numerous initiatives that have been in existence for some years now in this field). There was an appetite from practitioners in the expert working group for greater common standards in reporting

and some saw this as an area where best practice guidelines would be welcome. Nonetheless, this question had low number of responses so care must be taken in interpretation of this finding.

5 out of 9 respondents indicated that they have rendered assistance in cases requiring sophisticated digital evidence preservation techniques.

Respondents reported that such assistance was rendered reasonably infrequently – only two indicated once every 2-4 months, or it had never happened, or they had other remarks that this was rare or that it had happened "maybe once or twice in the past 8 years". The low number of responses to this question means that this data should be treated with great caution.

5.9 Views on the importance of operational factors

Below we represent the results of the voting from the Expert Group meeting on the identified operational factors. As can be seen, in comparison to the answer to question 33, there exists less of a correlation between those factors deemed as important in the online questionnaire and those that attendees of the Expert Group meeting voted for. For example, lack of common standards received a large number of votes at the Expert Group meeting but was not regarded as important by respondents to the online questionnaire.

Table 23 Ranking of operational factors from the Expert Group workshop

Operational Factors	Votes
Information on role and parameters for co-operation	11
Different/unknown policies and procedures – bureaucracy Lack of common standards in reporting Lack of clarity on what other party will do with info Insufficient or inappropriate detail	7
Lack of common case management tools	5
Security clearance – classified environments Incompatible workflows – driven by different priorities Lack of confidence in your/their official status Lack of early warning/KM tools Lack of service catalogue	4
Previous poor experience in information sharing	2
Financial burden, opportunity cost and	1

competing priorities Duplication Lack of known & trusted personnel/inexperience Time stamps on computers	
Communications barriers – common de facto language Proper channels/addressees Lack of secure comms channels	0

5.10 Conclusions on operational factors

Based on our analysis of the online questionnaire, mechanisms for collaboration between CERTs and LEAs do exist and are primarily based on trusted informal contacts and sharing of experiences.

Although this can be effective in terms of being flexible and adaptable, such trusted networks can be fragile and take a time to set up. Furthermore the differing character of each community can pose challenges.

No respondent indicated that they participated in a joint CERT-LEA team.

There was a low degree of interoperability seen with case ticketing systems, although they did exist they were not really conforming to the procedures or systems used by others.

The scope of digital forensics capability is primarily concerned with 'c-i-a' (confidentiality, integrity and availability) types of cyber-attacks for CERTs, but is broader for LEAs. Digital forensics capabilities appear to be mainly provided in-house.

Clear and transparent mechanisms for Information sharing were seen as the most important, as was an understanding of the other party's role and parameters for co-operation, and the presence of a known and trusted contact.

The single reason appearing as most prevalent for the respondent denying an incoming request from a third party (LEA, CERT) was due to security clearance/certification. The next most prevalent reason was wrong channel / addressee. If this finding were substantiated more broadly, then a possible solution might be twofold –firstly by considering again the security clearance / certification and secondly by providing better quality rather than more information.

In terms of information provided to the respondent as to why their request was not dealt with, respondents reported that they generally were either not sure or didn't know the reason. The next most popular reason concerned the issue of clearances, and then lack of confidence in official status, or insufficient detail.

6 Conclusions

Using the analysis of the results from the discussion at the informal Expert Group meeting in September 2012, we place the factors identified above into further context, indicating how the practitioner community (from which members of the Expert Group were taken) consider these factors to relate to one another.

6.1 Different factors affect CERTs on their path to maturity

Discussions at the Expert Group meeting were instructive in illustrating that many of these factors apply at different stages in a CERTs maturity. Some factors are internal or cover things which the CERT has some authority over. Other factors, however, would not be applicable until a CERT is up and running and has reached a certain level of maturity and they are exposed to the full complexity of cross border co-operation (particularly given the low awareness about relevant international legal frameworks). Below we present a clustering of these factors based on discussion at the Expert Group meeting in September 2012.

6.2 Conclusions and priorities for addressing legal, regulatory and operational factors

For the legal factors, participants identified privacy & data protection law; data retention law; laws with respect to the legal competence to initiate criminal proceedings; intellectual property protection law as falling under a cluster of '**Legal Frameworks'**

Participants suggested that: specific legal pitfalls on definitions of computer and network misuse; CERTs in the prosecutorial process; CERTs as evidence holders; laws with respect to the competence to investigate; procedural measures in criminal investigations; laws with respect to the handling of complaints; laws with respect to the consequences of complaints; laws with respect to the processes and procedures for registering complaints with LEAs and laws with respect to the safekeeping of evidence all fell under a cluster of '**legal/procedural**' issues.

Finally, participants argued that legal factors concerning a cluster that could be termed '**categorisation**' included: CERT categorisation: mandate & scope of CERT and national security frameworks (since national/governmental CERTs may have a wider remit to cover more different types of categories of incidents). Confidentiality agreements also fell into this category.

Obligations for private sector parties to co-operate with LEAs were seen as an ancillary '**other**' issue.

Four legal areas were considered specifically as being ripe subjects for further exploration of best practice:

- Privacy and data protection compliance
- CERT categorisation: Scope and mandate of CERT
- CERTs in the prosecutorial process

- Data retention law

Turning to the operational factors, **'bureaucracy/Legal standing'** was identified by participants as a cluster of topics that included: Information on role and parameters for co-operation; different/unknown policies and procedures; lack of clarity on what other party will do with information and finally lack of confidence in your/their official status.

Factors grouped by participants into a cluster of **'team capacity / competence'** included: lack of common case management tools; security clearance – classified environments; lack of early warning/KM tools; lack of service catalogues; previous poor experience in information sharing; financial burden, opportunity cost and competing priorities; lack of known & trusted personnel/inexperience; time stamps on computers and finally lack of secure communication channels.

The remaining factors were grouped by participants as being concerned with **communication flows**: lack of common standards in reporting; insufficient or inappropriate detail; incompatible workflows; duplication; communications barriers (language); proper channels/addressees.

Three factors were identified as having specific legal cross-over: Information on role & parameters for co-operation; different / unknown policies and procedures; and lack of clarify on what the other party will do with the information.

Finally, our research did not uncover specific issues concerning legal and regulatory challenges associated with co-operation and information sharing with non-EU countries (third countries). This topic would benefit from further case-by-case research. As shown by the differences in awareness of national laws and international legal frameworks, it would be erroneous to point out that even within Europe there is a suitable level of harmonisation and suggest that attention should be directed to 'third countries'. Research here would need to be undertaken on an even more careful case by case basis, taking each country's legal framework in detail.[97] However, it would be possible to specifically discern some countries (on the basis of criteria such as which countries frequently co-operate or would benefit the most from support for co-operation).

6.3 Priorities for further support

In order to support our consideration of recommendations, we also asked the respondents to our online questionnaire specifically about who they thought would be the highest priority to benefit from support.[98]

[97] *This was indicated in ENISA's 2012 Work Programme WPK 3.3 p47*

[98] *We did not specify greater detail on this question e.g. whether it should be a short, medium or long term type of support*

Table 24 Highest priority for beneficiaries of further guidance with respect to information sharing to tackle cybercrime

Stakeholder identified by the majority of respondents	Priority (1 = highest priority / 5 = lowest)
National/governmental CERTs	1
Other types of CERT Domestic Law Enforcement	2
Foreign Law Enforcement Agency Domestic Intelligence Agency	3

Respondents (unsurprisingly, as most were CERTs) felt that national/governmental CERTs and Domestic LEAs were the highest priority in terms of needing assistance. This supports the assumption that ENISA appears to be meeting a demand by focusing on these issues in its 2012 Work Programme. However, it also shows the complexities of rendering assistance at the national level, since this requires understanding of each national context. Interestingly domestic intelligence agencies were also rated as requiring assistance. Given the national focus of some national / governmental CERTs, with a scope of dealing with CIIP related issues, this appears to be an area for further investigation.

7 Recommendations

Based on the review of the inputs received via the questionnaire, and discussion at the Expert Group meeting, a number of recommendations are offered. The feedback shows that legal know-how and awareness is limited in most CERTs, and focused on their core tasks.

It is important to note that whilst some of these recommendations can be more or less narrowly linked to the research, others must be read in context with efforts underway from other stakeholders not directly covered as part of this study, specifically the law enforcement community. This is also backed up by the way in which some of the analysis further illuminates findings from the 'Flair for Sharing' study conducted in 2011 into "Legal and Regulatory Barriers for cross border CERT co-operation".

7.1 Training

Several training recommendations were proposed. Many of these can also be seen in the light of other initiatives, especially through the EC3, European Cybercrime Training and Education Group (ECTEG)_and other initiatives like the 2-CENTRE[99] and B-CCENTRE[100] projects. Specifically these addressed building training, including both **expanding joint training between CERTs and LEAs** but also training that each community may individually have been developing or providing. Common / joint training should include real-life cases where possible. The Training Competency Matrices and Scenarios that form part of the outputs of this study are key in this respect. A key part of strengthening training provision would be ensuring that language reflects the skills and understanding of both sides: e.g. agreed definitions of terms 'malware', 'phishing' etc.

- For CERTs, including a **training element on how to deal with LEAs as part of CERT training syllabus (for example the TRANSITS programme)** would assist in strengthening capability for co-operation.
- For LEAs, at the national level there may be opportunities for improvement but also within the **context of additional training envisaged as part of the work of the EC3.** Training modules should be developed on how to deal with CERTs and what data CERTs may possess which might be of use to LEAs (e.g. broader intelligence that might help them to understand trends). The EC3 would need to take this forward given its additional role in strengthening training for LEAs.

7.2 Structures

In terms of infrastructure for co-operation the following recommendations are more obvious.

[99] *The 2-CENTRE Cybercrime Centres of Excellence Network* http://www.2centre.eu

[100] *Belgian Cybercrime Centre of Excellence for Training, Research and Education* http://www.b-ccentre.be

Core competencies for certified CERTs would see those CERTs as being certified (e.g. under the TF-CSIRT Trusted Introducer scheme) having their core competencies with respect to LEA co-operation better defined and identified. This could logically follow on from the 2012 national/governmental CERT baseline capabilities reports[101] and could be a task that ENISA in conjunction with the national / governmental CERT community and others (e.g. TF-CSIRT) would be able to take forward.

The Expert Review group also discussed a **single system for sharing of information between CERTs and LEAs.** Such a system might include trusted channels, correct and complete information lists, including contact lists and other useful information.

Other recommendations affecting structural improvements included the **definition of capabilities and types of information CERTs and LEAs can provide to each other**. As has been noted before, it would appear that evidence from the Expert Group suggests that LEAs often do not realise the different types of information that could be provided by CERTs, if only they had to ask.

It would be valuable to conduct more research in two specific areas that would help improve the structural mechanisms for information sharing between CERTs and LEAs. These are:

- Comparative **analysis of judicial powers** of embedded LEAs working in CERTs: the French & Romanian experience (which have/had LEA officers seconded within their CERTs with varying degrees of judicial power) can be instructive as an example of organising effective processes. The European Commission would be best placed to investigate this further via commissioning research.
- Comparative **analysis of the requirements for digital evidence at the national** level - what mechanisms (digital signature etc) are present/used within each Member State to verify authenticity of evidence? This could be instructive for establishing good practice mechanisms that ensure the usability of digital information within CERTs as evidence in legal proceedings. As above, such a study could be carried out by the European Commission.

Separately, the continual evolution of technology was noted as a constant factor and there would perhaps be an opportunistic role for an organisation to offer a technology watch function to **monitor how criminals are exploiting technologies** and offer advice for 'crime proofing'. ENISA, in collaboration with the EC3, would be best placed to take this forward.

7.3 Facilitation & collaboration

Some recommendations envisaged with respect to generally improving facilitation/collaboration included examples listed below. These can be seen in a broader

[101] *See ENISA National / Governmental CERT Baseline Capabilities Reports (2009; 2010) v.1.0 (initial draft) available at: http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities*

context of other initiatives that ENISA is pursuing (e.g. the aforementioned 7th CERT-LEA workshop).

- **Consider if and how CERTs can take on an investigative role for LEAs, e.g.** in the way Environmental Inspectors have an enforcement role - learning from other policy domains where non-LEA organisations with regulatory powers can assume investigative activities.[102] Other examples include National Regulatory Authorities for telecoms (associated with the Art 13a Breach Notification Regime) and Data Protection Authorities, who have similar investigative powers in some countries. In particular, further comparative research would be needed on what enforcement competencies other relevant across Europe bodies possess, and if/how similar competences could be established with CERTs that have been given an appropriate mandate under national law. as this very much relates to the national situation regarding powers of investigation, Member State governments would need to take this forward.
- **Further clarifying via regulation the depth and breadth of investigations CERTs can undertake**, specifically related to different types of incident (see Best Practice below), and taking into account specific investigative activities (e.g. search and seizure of stored computer data via networks, including at a cross border scale, in accordance with the requirements of international collaboration rules and data protection law). In some of these frameworks, clarification would be need to be undertaken by the European Commission as this relates to expanding on the practical implications of interpretations of points of law.
- **Prepare a guide in LEA language and using LEA terminology for working with CERTs** – including how CERTs work, what are the key features of a CERT and what type of data they can provide. This might be a common output of work between ENISA and the EC3.
- **Acknowledgement for partners when information sharing takes place** – for example, where possible the LEA could inform the CERT as to the status of the investigation (specifically whether it is still on-going or has concluded) and where information / intelligence provided by the CERT has led to arrest or conviction. This would be primarily a behavioural or psychological benefit as a softer measure to help strengthen trust, since CERTs appear to be motivated at least in part by altruism and so providing information that they have helped someone else might strengthen mutual trust. Furthermore, such updates (which could be made without communicating any personal data so as to fully respect data protection law and any investigative secrecy requirements) would allow the CERTs to determine when retention of incident data is still required or useful, and whether their intervention in prior files has been effective. CERTs and LEAs should be encouraged to act on this.

[102] *e.g. for example CERT.EE has been recently established in a role which gives it more of an investigative capability to work on behalf of LEAs*

- **Greater understanding of each other's procedures and capabilities.** A key point noted in the Expert Group meeting was that this understanding might be more effective (because it would offer reassurance) if it was phrased negatively – for example, "if you fulfil our request we agree *not* to do x, y or z with the following types of information you might provide". Further examples of specific means to improve understanding of policies and procedures include:
    - **Prepare an equivalent of 'RFC 2350' for LEAs** ("Expectations of computer security incident response) for LEAs, covering for example, what incidents/crimes they primarily focus on, whether they have a 24/7 Point of Contact; existence of forensic capability). This could be taken forward by National governments and LEAs with input from the national/governmental CERT community.
    - Preparation of a **guide in LEA non-technical language describing what types of data CERTs might have available** and the implications for different types of crimes would be something that ENISA could take forward, with input from CERTs
    - **Setting out a checklist or clarification of the right sort of questions for LEAs to ask CERTs** for example: "do you collect x, y, or z types of information"; "do you possess a remote search capability"; "what mandate do you operate under?" ENISA would be able to take this forward.
- The expected benefit of the EC3 in building on existing efforts to bring together **ENISA and the LEA community**, alongside other important international stakeholders like the Internet Corporation for Assigned Names and Numbers (ICANN) LEA constituency group was also noted: this recommendation would span the medium term once the EC3 is fully functional.
- The quality of reporting of metrics regarding incidents and crimes is a recurring theme and this was also noted as a recommendation that **standardisation of reporting incidents** (albeit an ambitious ideal) would support the pan-European tracking of incidents. A first step would be the sharing of overviews of incident statistics. ENISA might be in a role to act as a trusted third party in taking this forward.
- **Prepare a CERT> LEA dictionary** covering different terms – this would be included as an annexe in those documents written for CERTs aimed at interaction with LEAs and vice versa.

7.4 Best Practice development

A number of recommendations became evident with regard to best practices development. These would likely represent sensible follow on from the existing study. Recommendations here include:

- establishing **good practice guide on writing information / evidence sharing agreements** (which would need to include the difference between, information as evidence, and information as intelligence, and clarification on the LEA meaning of the term 'for evidence') – an effort the EC3 and ENISA might jointly pursue;

- **best practices on privacy/data sharing** (which may also benefit from specific input from the Article 29 Working Party in respect of data protection compliance – see below);
- building a common **consensus as to what constitutes a cyber-incident,** given the aforementioned divergence and fragmentation between those types of cyber security incident that CERTs are interested in, and the broader set which LEAs might be interested in (this would need to be taken forward by ENISA, the EC3, national governments and the European Commission);
- Preparation of **guidance on risk based models for information exchange/disclosure** helping CERTs to apply risk frameworks concerning the disclosure of information to others. This could be based on the impact/likelihood of sending certain types of information, to help CERTs make suitable decisions regarding the balance between differing obligations e.g. protection of personal data versus assisting law enforcement. ENISA would be best placed to take this forward with input from the CERT community.

7.5 Harmonisation and clarification of legal and regulatory aspects

At the European level there are certain other initiatives that could be developed in the domain of public policy. Some of these strengthen the recommendations from last year's ENISA study which considered the legal and regulatory barriers in detail. Taking these recommendations forward would largely fall to ENISA, in conjunction with Data Protection Authorities and the CERT community.

- **Data protection compliance** remains the largest open issue for CERTs. Therefore, it could be envisaged to provide CERTs with specific guidelines and standardised templates (e.g. in the form of pragmatic checklists) for:
    - **Assessing whether information requests pertain to personal data; and, if so, how to handle them.** This would include checking for information on the scope and nature of the requested information, its intended use and intended recipients.
    - **Submitting requests for personal data** to other entities. This would include information on their own status and mandate, requested information, intended use and intended recipients. This would help the recipients of such requests to assess the legitimacy thereof.
    - **Responding to requests for personal data** from other entities, via a series of important questions to assess.

  These guidelines and templates should take into account the European data protection rules as they evolve. Presently, they would thus largely be based on the Data Protection Directive (95/46/EC), whereas in the future they may be based on the recently proposed Data Protection Regulation and the Law Enforcement Data Protection Directive, depending on the mandate and activities of the CERT. Furthermore, the guidelines and templates will need to consider whether the

contemplated exchanges of personal data are purely national (and thus subject to purely national data protection rules), within the EU/EEA (possibly resulting in the applicability of multiple national data protection laws), or international (possibly requiring further guarantees in order to comply with European data protection rules on the export of personal data to third countries outside the EU). Such guidelines would allow CERTs to assess more systematically and correctly where information exchanges are possible, and can also assist policy makers in identifying gaps where international collaboration is possibly excessively complex to organise in practice.

- Further discussion about establishing a **clear regulatory footing** for national/governmental CERTs to encourage smoother information flow, as per the Danish example where the CERT has been according specific powers in national law.
- More generally, high level **collaboration / information sharing policies** should be established which account for legal issues. This would allow CERTs and collaborating organisations to semi-formalise their working arrangements and understanding, beyond mere data protection compliance. Relevant aspects might include any measures that have been taken by the CERT to ensure the accuracy and comprehensiveness of the information at the time of collection, any measures to safeguard the integrity and authenticity of the evidence, the availability of the CERT to attest to the reliability of the information, its mandate and competence to lawfully collect and transfer the information, etc. In this way, the recipient of such information could more easily assess whether the information is merely useful as intelligence, or whether it could also be potentially useful as evidence. This would provide a greater degree of legal assurance, as recipients could then determine the extent to which they can rely on the information, both factually (i.e. as a basis for its own investigations) and legally (i.e. as support for any legal proceedings).

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