A flair for sharing – encouraging information exchange between CERTs

A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe

Initial Edition 1.0

November 2011

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For contacting ENISA or for general enquiries on this study on Legal and regulatory aspects of information sharing and cross-border coordination of national/governmental CERTS in Europe, please use the following details:

Dr Silvia Portesi, CERT Relations Team

Email: cert-relations (at) enisa.europa.eu Internet: http://www.enisa.europa.eu

Acknowledgements

We would like to thank the study team from RAND Europe and time.lex commissioned by ENISA to undertake this study, in particular Neil Robinson and Hans Graux.

We would also like to thank the members of the informal Expert Group established by ENISA to provide support for the review of this study, including Hans Bøgesvang Riis (GovCERT, Denmark), Andrew Cormack (JANET(UK)), Daniel Drewer (Europol), Alessandra Falcinelli (European Commission), Marco Fernandez Gonzalez (European Commission), Zoe Kardasiadou (Hellenic Data Protection Authority), Jan Kolouch (CESNET), Christopher Kuner (Hunton & Williams), Thomas Kristmar (GovCERT, Denmark) and John Morijn (Ministry of the Interior and Kingdom Relations, the Netherlands).

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

Supervisor of the study and contributor: Silvia Portesi (ENISA).

Legal notice

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

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

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

Reproduction is authorised provided the source is acknowledged.

Disclaimer

This initial edition of this document, Version 1.0 of November 2011, has been prepared by RAND Europe and time.lex, commissioned by ENISA according to the ENISA tender ref. ENISA P/04/11/TCD.

This document is to be considered a work-in–progress that will undergo necessary changes in the future in accordance with an ongoing dialogue with all relevant stakeholders, which is reflecting the ongoing changes taking place in the European Network and Information Security Domain. As an example of the fast moving nature of developments in this field, since this report was finalised the UK released its new Cyber Security Strategy on 25th November 2011.

Contents

Executive Summary

Introduction

Cyberspace has become an important asset for economic growth. According to the OECD, between 2000 and 2009, ICT investments were more important for growth than non-ICT investments in a majority of OECD countries (OECD, 2011). In addition, cyberspace is becoming increasingly crucial for the creation of broader societal benefits. According to Eurostat, in 2010 41% of all Europeans aged between 16 and 74 had interacted with the government online.[1] The role ICT plays was also recognised in the milestone Communication from the European Commission: A Digital Agenda for Europe,[2] a major policy initiative which emphasised that the Internet now represented a 'vital medium of economic and societal activity: for doing business, working, playing, communicating and expressing ourselves freely' and was an important route to returning Europe to economic growth. The 2009 Communication from the Commission on Critical Information Infrastructure Protection[3] reiterated that these economic and social benefits might be put at risk by poor security, such as the growth in cyber crime or major forms of 'cyber attack' against Critical Information Infrastructures (CII). A further challenge has also become clear, where those entrusted with providing cyber security must also find a way to respect fundamental human rights, such as the protection of personal data.

Computer Emergency Response Teams (CERTs)[4] have long been recognised as playing an important role in helping to mitigate the impacts of such attacks, by detecting, supporting the investigation and responding to incidents. They can be thought of as 'digital fire brigades' for cyberspace. Data provided by CERTs may also help industry and government to better understand threat patterns and attack trends, thereby improving the application of preventative measures and reducing the scope for future attacks. Because such attacks often exploit the global nature of cyberspace, by definition they do not respect national and organisational boundaries. Therefore, in order to mitigate the impact of such attacks, responses may require extensive cross-border coordination between national/government CERTs and others (such as CERTs in financial institutions). This coordination can include the sharing of certain types of data, in real time, concerning the source or destination of attacks (usually IP addresses) or log files of suspicious types of Internet traffic. Much CERT cooperation and sharing takes place informally on the basis of trustful relationships.

---

[1] Eurostat Structural Indicator 2010 – Percentage of individuals aged 16 to 74 who have used the Internet, in the last 3 months, for interaction with public authorities (i.e. having used the Internet for one or more of the following activities: obtaining information from public authorities web sites, downloading official forms, sending filled in forms) [accessed 22 August 2011]

[2] COM (2010) 245 of 19 May 2010 ('Digital Agenda for Europe')

[3] 2009 Communication from the Commission on Critical Information Infrastructure Protection: 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' (COM (2009) 149) 30 March 2009 ('Communication on CIIP')

[4] For a definition of CERT, see ENISA (2009b: 8ff) and ENISA (2010a: 10ff)

National/governmental CERTs are a particular type of CERT playing an important role at a national level in supporting such cross-border coordination.[5] They are primarily concerned with incidents affecting national Critical Information Infrastructure. They can act as a contact point for sending and receiving cross-border requests concerning different types of information to help them detect, react and mitigate an incident. The 2011 Communication from the Commission on Critical Information Infrastructure Protection[6] noted that as of March 2011, over 20 national/governmental CERTs had been established across Europe.

Nonetheless, the complexity of legal factors surrounding this cross-border collaboration could present issues. CERTs in different countries may have differing legal grounds to request or transmit such information to other teams. Furthermore, Internet Protocol (IP) addresses may be accorded the status of personal data and therefore be subject to a specific set of legal obligations. Similarly, information which national/governmental CERTs might require could be subject to Freedom of Information or re-use of Public Sector Information (PSI) rules. This might present challenges to investigation, particularly where criminal involvement is suspected.

The aim of this study was thus to identify these legal and regulatory factors and perform an assessment of what effects they had on cross-border information sharing between CERTs, with a focus on national/governmental CERTs.

In order to investigate these issues, ENISA commissioned RAND Europe and time.lex to: conduct a targeted literature review; perform seven Key Informant Interviews with CERT practitioners, lawyers and domain experts and finally design and administer a lengthy online questionnaire aimed primarily at national/governmental CERTs between June and July 2011.

Legal and regulatory factors for information sharing

We identified a number of substantive legal frameworks and common horizontal issues that may positively or negatively affect the extent of cross-border information sharing. It is important to note that these factors may be seen in a positive or negative light: for example, CERTs may be more inclined to share information knowing that the peer operates under a legal framework affording the same protections to personal data. Indeed, as we shall explore below, a number of legal initiatives have been taken specifically to facilitate and encourage information sharing, such as the provisions on mutual assistance requests and international cooperation in the Council of Europe's Convention on Cybercrime, or the rules with respect to cross-border exchanges of information in the Council Framework Decision on attacks against information systems. While these rules do not apply uniformly to all CERTs, as will be discussed below, they are indicative of an increased recognition at the policy level of the importance of cross-border information exchanges for information security incidents.

Nonetheless, these legal and regulatory factors can complicate the delicate balancing act that CERTs have to perform between investigating, managing and mitigating incidents

[5] For a definition of national/governmental CERTs, see ENISA (2009b: 8ff) and ENISA (2010a: 10ff)

[6] 2011 'Communication from the Commission on Critical Information Infrastructure Protection: Achievements and next steps: towards global cyber-security' (COM (2011) 163) of 31 March 2011 ('Progress Report on the CIIP Action Plan').

and contributing to a better understanding of the relative state of cyber security, and protecting those rights and obligations provided for by certain legal and regulatory frameworks.

Clearly, the exchange of information (including in cross-border scenarios) should not be examined as a risk to certain fundamental rights (for example, privacy), without also acknowledging that these exchanges are a precondition for responding effectively to ICT incidents. Poor cyber security could undermine the exercise of other rights enshrined in the Charter of Fundamental Rights of the European Union[7] such as the protection of integrity of the person, personal life, data protection, freedom of expression and information, the freedom to conduct a business and the right to property.

Legal factors we identified as being primarily of relevance include:

- Definitions and criminal sanctions concerning different types of computer and network misuse;
- The European legal framework governing data protection and privacy;
- Freedom of Information (FoI) and Public Sector Reuse of Information (PSI) legislation;
- Criminal procedure;
- Intellectual Property Rights;
- Confidentiality obligations;
- Determining applicable law;
- Mandate and competences of the CERT.

In addition, other legal frameworks noted include rules governing working with law enforcement, national security laws and competition law.

A number of harmonising initiatives have aimed at reducing differences between the Member States for most of these topics, including with respect to data protection and retention, defining crimes against information systems, re-use of public sector information, and determining applicable laws. Nonetheless, as the sections below indicate, these initiatives leave a significant margin of national policy in the Member States, meaning that CERTs are still confronted with ambiguities and differences in national laws and policies. This creates uncertainty when determining if data sharing is permissible and lawful.

A commonly recurring element in this uncertainty is the variety of mandates for CERTs. Not all CERTs will have comparable mandates to intervene in any type of computer emergency. Their competences can be strongly affected by their national laws, but also by their own statutes or operating rules, depending on the legal basis of their formation (e.g. as independent entities or as part of an interior or economic affairs ministry). This also affects how they can address each of the challenges above: a national CERT with a clear legal remit defined by law may, for example, have a clearer legal basis for collecting and processing personal data relating to suspicious activities than a purely private sector CERT that oversees the security of a single communications network. Ignoring these

[7] The Charter of the Fundamental Rights of the European Union is a statement of fundamental political, social and economic rights granted to citizens and residents of the EU. The Charter includes such rights as the right to life, dignity, liberty and security, and the protection of private life and personal data. It became legally binding through the entry into force of the Treaty of Lisbon, on 1 December 2009.

bounds can result in evidence being tainted and/or the CERT risking its liability. Thus, for a CERT it is vitally important to have a clear mandate, and to be able to communicate this information clearly to its peers before engaging in information exchanges.

Whilst the literature review and Key Informant Interviews (KII) conducted for this study identified a number of challenging legal concerns, at the practical level not all of these concerns were noted as being of direct impact with respect to cross-border information sharing.

The research found that a degree of uncertainty remained with respect to the legal basis of much CERT cross-border coordination. Interviewees reported that CERTs' cooperation operates on an informal basis which sometimes perceives legal involvement as hampering swift and effective cooperation. CERTs participating in this study reported having participated in cross-border information exchange. Many of the respondents to the online questionnaire indicated they had managerial or technical, rather than legal expertise.

Evidence from our research indicated that in practice, **data protection, data retention, and obligations to work with law enforcement** constituted the greatest set of challenges for cross-border CERT cooperation. The respondents to our questionnaire were most familiar with their own national legal frameworks in these areas, whereas they were less familiar with international harmonisation initiatives in the same domain. For example, with respect to their own legislation 15 out of 17 respondents reported that they had at least some knowledge of *definitions of computer crime* or *data protection and privacy law*; 14 out of 17 respondents reported some knowledge of *data retention rules; procedures for preserving computer data as evidence* or *national security rules* and 13 out of 17 respondents reported at least some knowledge concerning laws about *working with law enforcement*.

With regard to international aspects, however, the situation is different. Here, 9 out of 17 respondents reported some understanding of international efforts to harmonise *computer crime definitions* (as afforded by the Convention on Cybercrime, for example). Eleven out of 17 respondents indicated some understanding of international efforts to harmonise *data protection and communications privacy*, whilst 9 out of 17 respondents reported some understanding of international efforts concerning *national security* laws.

There was least familiarity with international efforts governing rules determining the competent court, applicable law for specific incidents or legal value of evidence: only 7 out of 17 respondents indicated any degree of understanding with international harmonisation regimes in this regard.

Regarding the specific legal frameworks cited as justification for their own request being denied, 12 out of 14 respondents cited *data protection and privacy law* as having been used as a reason to justify a declined request by a peer. On the other hand, 5 out of 13 respondents indicated that with some degree of frequency *data protection and privacy laws*; *rules concerning computer data as evidence*; *laws concerning cross-border mutual legal assistance*; *laws concerning working with law enforcement* or *rules concerning the legal value of evidence* were all cited as a justification to withhold information in a cross-border request. Of course, this should not be taken as clear proof that such exchanges would certainly have been in clear breach of these laws, but rather that sufficient doubt existed on the legality of the exchanges to withhold them.

Recommendations

The evidence gathered during our study (especially from the online questionnaire) should not be taken as entirely representative of the entirety of the European national/governmental CERT community. Nonetheless, below we identify some recommendations which may further improve the work of CERTs based on the material gathered during this study. We split these up into short, medium and long-term recommendations. In the short term:

- A.1 Identify **ways to support operational coordination** between CERTs – for example by the provision of a one stop shop or legal helpline, modelled perhaps on the European Judicial Network (EJN) 'legal helpdesk'. Other approaches include the provision of checklists.
- A.2 Disseminate **Declared Level of Service templates** building upon the establishment of common 'declared level of service' templates (based on the RFC2350[8] model) to help set expectations as to legal factors which may affect cross-border information exchange;
- A.3 Investigate measures to **encourage cross-border information exchange** for example via sanitisation of data, confidentiality charters or means to limit liability of CERT incident response activities (such as the 2011 Danish law concerning Incident Response).

Over the medium to longer term, more extensive recommendations concern policy intervention:

- B1. Address **legal uncertainty** concerning requests via clarification of the differences between relevant national legal frameworks to remove uncertainty and create a common baseline for cooperation.
- B.2 Designate national/governmental CERTs on a **specific regulatory basis** to provide them with a clearer mandate.
- B.3 Ensure EU-level legislation takes account of the **scope of national/governmental CERTs** particularly with the current revision of the Data Protection Directive 95/46/EC noting principles for the use of personal data in the fight against terrorism and serious and organised crime.
- B.4 Specify a threshold for incidents requiring national/governmental CERT response and sharing – that **incidents must pass some certain threshold** according to agreed indicators for them to be considered as within the competence of being addressed by a national/governmental CERT.
- B.5 Articulate why CERTs **need to process personal data** to the relevant authorities so that guidance may be prepared to establish clarity on under what circumstances personal data used by CERTs may be shared across borders.

Finally, three long-term recommendations concern research activities or projects.

- C.1 **Incorporate information on the legal basis** for an information request (e.g. via coordination with structured information exchange initiatives such as those run by the IETF or ITU).

[8] Brownlee, N., Guttmann, E. (1998) 'Expectations for Computer Security Incident Response', IETF Request for Comments (RFC 2350); Available from: http://www.ietf.org/rfc/rfc2350.txt [accessed 17 August 2011]

- C.2 Further **foster R&D into privacy enhancing Security Event & Incident Monitoring** (SEIM) tools, for example anonymisation infrastructure.
- C.3 Conduct further empirical **research into the mechanics of cross-border CERT cooperation** to explore the logic and process of cross-border incident response.

1. Introduction

In this chapter we present an overview of specific background information related to Computer Emergency Response Teams (CERTs), specifically: the rationale, the policy context and the role of national/governmental CERTs.

The aim of this study is to identify whether there are any national and/or international legal and regulatory factors affecting cross-border information sharing between CERTs. The primary focus of the study is on those CERTs that have an important role to play, at the national level, in terms of Critical Information Infrastructure Protection (CIIP).

1.1 Rationale

The sharing of information regarding cyber security threats, vulnerabilities, exploits, incidents and risks is regarded as an important facet of improving security in cyberspace (Dependability Development Support Initiative, 2002). This is because sharing of information helps information security professionals to investigate incidents, mitigate them and develop technical and organisational responses to prevent further occurrences. In addition, policy-makers can better understand the relative state of cyber security and craft suitable policy responses if such information is shared between public and private sectors.

Evidence from previous research concluded that there are three main reasons why information on cyber security should be shared (Dependability Development Support Initiative, 2002):

- Governments and policy-makers require this information to better formulate policy;
- Industry may view the sharing of information as necessary for risk management, corporate governance and compliance;
- Citizens need this information to take appropriate measures, particularly in respect of the rising types of financially motivated attacks.

CERTs are at the sharp end of receiving and analysing this type of data,[9] according to the European Commission's Progress Report on the CIIP Action Plan. In addition, the results of the European Network and Information Security Agency's (ENISA) 2005 Working Group on CERT cooperation and support stated that CERTs play a 'key role in the field of network and information security' (ENISA, 2006b, p. 3). Their activities include: preventing security breaches, limiting the damage resulting from a breach and recovering from a breach as quickly as possible. CERTs can also provide assistance to victims of attacks, prepare vulnerability assessments, conduct awareness-raising activities and promote best practice (ENISA, 2006b).

Whether based in government institutions (e.g. GOVCERT.NL in the Netherlands), private sector firms (e.g. CERT-Society General in France CERT) or telecommunications providers (e.g. British Telecommunications CERT) CERTs provide an important role by identifying,

[9] For example see the ENISA page on CERTS for full descriptions at http://www.enisa.europa.eu/act/cert/background/coop/terms-definitions-1/certs [accessed 22 August 2011] and ENISA (2010a; 2009)

collating, parsing and sometimes onward distributing information regarding network security incidents and events. This information is used to base decisions on, for example, both proactive (understanding attack mechanisms identified by monitoring computer systems intentionally made vulnerable to abuse) and reactive measures (whether to throttle bandwidth or quarantine some Internet Protocol (IP) addresses in order to protect the functioning of the overall network).

Through this role in collecting and exchanging crucial information with respect to IT security incidents, CERTs contribute to enable an effective response. While this role also often exposes them to concerns about infringing data protection and privacy rights, CERTs also act as a guardian to the exercise of various rights enshrined in the Charter of Fundamental Rights of the European Union that could otherwise be encumbered by such incidents, including the protection of integrity of the person, personal life, data protection, freedom of expression and information, the freedom to conduct a business and the right to property.

A useful example was in the well-known incidents in Estonia in 2007 when CERT operators from Germany, France and Finland helped to identify and mitigate the impact of politically sparked Distributed Denial of Service (DDoS) attacks against the Estonian Information Infrastructure (Evron, 2008). This monitoring and collection of data may also be used to collect evidence as part of further law enforcement, internal or security investigations. In the case of the DDoS attacks instigated against Georgia in 2008, the Estonian and Polish CERTs all worked together to try and solve the problem by exchanging data on the origin of the attacks.

The cooperation evidence in addressing the Code Red/Nimda threat in 2002 is another relevant case where UK, US and European CERTs cooperated in order to detect and notify those IP addresses which were a source of malicious traffic in an attempt to resolve the situation.[10]

1.2 National/government CERTs: CERTs with special responsibilities

The focus of this study is mainly on 'national/governmental CERTs' (ENISA, 2009b; 2010a). This term is thus taken to include any type of CERT (including national or government CERTs) where they:

- Generally support the management of security incidents for systems and networks within national borders;
- Bear or are involved in the responsibility for CIIP within the borders;
- Act as official or *de-facto* Point of Contact (PoC) for national/governmental CERTs in other Member States.

It is important to consider the implications of this definition: national/governmental CERTs are responsible for incident management for CII – therefore it may be seen that a different set of principles (national security) could be relevant in understanding the legal implications of their activities.

A previous ENISA study looked at the incentives and challenges to information sharing and found that there are a number of issues regarding information sharing (ENISA, 2010b). Poor quality of information and poor management of information sharing were

[10] Anonymous research interviewee 26/04/2011

found to pose a barrier to cooperation, as did misaligned economic incentives stemming from reputational risks. Trust thus appeared to be a key issue. Nonetheless, the study found the situation to be even further complicated by uncertainty about senior-level awareness of cyber security. For example, the question of trust and the socio-economic and behavioural aspects of information sharing may manifest itself in the 'front line operator' contradicting or otherwise trying to overcome legal and regulatory barriers towards the onward disclosure of certain forms of network data, in the interests of preserving the health of the network and information systems of the CERT community as a whole (ENISA, 2010b). Moreover, the private sector may be dis-incentivised to disclose such information when there is a perception of possible reputational damage or potential loss of a commercial advantage to certain competitors. Nonetheless, firms might be comfortable in disclosing such data if they knew others were doing so, or if legal or other schemes existed which they could trust to prevent the further transmission of such information outside of specific circles or regulatory involvement (e.g. exclusion of liability).

It was also clear from the ENISA study into Incentives and Challenges to Information Sharing (ENISA, 2010b) that the legal and regulatory landscape was an important factor determining the extent and format of information sharing under different conditions. This is especially true in the case of information sharing at the national and international levels, where there are complex issues concerning the equivalence and difference in laws across different jurisdictions (Valeri et al, 2005). Because of the nature of information sharing between CERTs, the reality is likely to be that much of the information exchange occurs in a grey area, which could undermine the legal value of the information in court. 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.

A multitude of instruments has been created, especially at the European level, that would support effective collaboration (including particularly information exchange) with respect to legal investigations into cyber crime incidents. These efforts fall to a certain extent within the scope of CERT collaboration. We describe below some of them which relate to the European context, national initiatives and European and international projects.

1.3 The European policy context

At the European level, the importance of sharing information, and of CERTs in doing so, has been broadly recognised across a number of policy documents. This includes the 2006 Communication from the Commission on a strategy for a Secure Information Society: Dialogue, partnership and empowerment (COM (2006) 251) of 31 May 2006 ('Strategy for a Secure Information Society'); and the Action Plan for CIIP.

The 2009 Communication on CIIP in particular noted under its heading of 'Preparedness and Prevention' the need to establish well functioning national/government CERTs in all Member States by the end of 2011. Furthermore the need to improve cooperation was also highlighted under the pillar of 'Reinforced cooperation between National/Governmental CERTs' through support (e.g. exchange of best practices) and also expanding cooperation schemes such as the European Government CERT group.

In 2010 the Digital Agenda for Europe outlined objectives under the pillar on Trust and Security, section 2.3, that a wider network of well functioning CERTs [at national level] should be established across Europe in order to react to real-time conditions.

Finally, the 2011 Communication on a Progress Report on CIIP, 'Achievement and next steps: towards global cyber security', noted a number of achievements with respect to CERT Cooperation in Europe since the 2009 Communication on CIIP. These included:

> – In 2009, ENISA, together with the Computer Emergency Response Team (CERT) community in Europe, developed and agreed on a minimum set of baseline capabilities and services that National/Governmental CERTs need to have in order to function effectively in support of pan-European cooperation. A consensus was achieved on a list of 'must have' requirements in the areas of operation, technical capabilities, mandate and cooperation.
> – In 2010, ENISA worked with the CERT community in Europe to turn the above operationally oriented requirements into a set of policy recommendations for National/Governmental CERTs to act as the key component of national capability for preparedness, information sharing, coordination and response.

According to this Communication as of March 2011, 20 Member States had established national/governmental CERTs and the others had plans to establish them.

The recognition of the importance of information sharing is undoubtedly also reflected in the existence of other policy instruments across the law enforcement and criminal justice domain. Examples include the:

- Communication from the Commission to the European Parliament and the Council: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010) 673 of 22 November 2010 ('Internal Security Strategy'), which is the EU's shared agenda to address security challenges affecting the social market economy proposed in the Europe 2020 vision;
- Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (the 'Swedish Initiative'), which aims to 'enhance the effective and expeditious exchange of information and intelligence between law enforcement authorities';
- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which details the conditions under which personal data may be processed for the purposes of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty;
- Cooperation obligations established under the Council Framework Decision 2005/222/JHA on attacks against information systems which sets out the common definition of types of computer crime and minimum sanction and is at present subject to a Proposal for a Framework Directive on attacks against information systems and repealing Council Framework Decision 2005/222/JHA;
- the European Cybercrime Platform (ECCP) managed by Europol, which brings together law enforcement, the private sector and Internet Service Providers and tries to establish a wider and more coordinated approach to addressing cyber crime;
- more tangentially, the Prüm Decision (a framework for Member States to gain access to one another's automated DNA analysis files, automated fingerprint identification systems and vehicle registration data) and the European Criminal Records Information System (ECRIS), which will permit the interconnection of criminal records via a decentralised IT architecture linking databases in each Member State;

- In addition, the centralised Schengen Information System (SIS) and its second generation (SIS II) are key examples of common, EU-level, systems set up to share information to support the European Area of Freedom, Security and Justice (AFSJ).

1.4 National initiatives

At the national level, cyber security strategies often note the importance of incident response – these include a number of EU Member States:

- The 2009 Cyber Security Strategy of the United Kingdom which established the Cyber Security Operations Centre to 'actively monitor the health of cyber space and co-ordinate incident response' (Cabinet Office, 2009)[11];
- France, similarly, has recognised the role of incident response communities through the formation of Agence nationale de la sécurité des systèms d'information (National Agency for Information Systems Security – ANSSI) and the elaboration in its 2011 Défense et sécurité des systems d'information Stratégie de la France (Defence and Security strategy for strategic information systems of France) that incident response was an important property and characteristic of resilience and being able to withstand cyber attacks (ANSSI, 2011);
- Similarly, the Netherlands in its recently released National Cyber Security Strategy 'Success through cooperation' outlined plans to 'expand and reinforce the current GOVCERT.NL and place it within a National Cyber Security Centre' (Ministry of Security and Justice, 2011);
- In Germany, the 2011 Cyber Security Strategy noted that the IT Planning Council would have a stronger role in facilitating the establishment and functioning of CERTs (Bundestag, 14/8/2009);
- The Cyber Security Strategy of the Czech Republic for 2011–2015 was published in June 2011 (Parlament České republiky, 2011). It notes the importance of incident response and describes plans for establishing a National CERT Agency as a government coordination agency able to respond immediately to computer incidents. This agency will become part of both the national and international cyber threat early warning systems;
- In Denmark on 1 June 2011, the Act on Processing of Personal Data when Operating the Governmental Warning Service for Internet Threats was passed (Folketinget, 1 June 2011). This established a clear legal basis governing the processing of personal data by the Danish National IT and Telecom Agency for the purpose of running the Governmental Warning Service. It indicates that no court order is required to 'process, including collect, register, analyse and store […] incoming and outgoing packet and traffic data of connected authorities and private enterprises'.

1.5 European and international projects

In addition to government policies, there are a number of European and international projects and initiatives that are also relevant to information exchange. Chief amongst these are the networks of incident response teams, but there are also specific initiatives,

[11] Since this report was finalised the UK released its new Cyber Security Strategy on 25th November 2011 and can be found at: http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy (accessed 30 November 2011)

policy interventions and other activities of relevance. These include (but are not limited to):

- TERENA's TF-CSIRT – Task Force on Computer Security Incident Response Teams (TF-CSIRT) – is perhaps, at the European level, the most well known grouping of those from the incident response community. It is hosted by the Trans-European Research and Education Networking Association (TERENA). There are around 148 different teams in TF-CSIRT from the national and private sector. TF-CSIRT hosts community meetings three times a year and has had discussions on the legal aspects of improving cross-border collaboration;[12]
- European Government CERTs (EGC) group is a small, informal group of governmental CSIRTs that aim to develop effective cooperation on incident response matters between members. Their focus is on large-scale or regional network security incidents and they aim to jointly develop measures to address such incidents, identify areas of specialist knowledge and expertise, identify areas of collaborative research and development, encourage formation of government CERTs in European countries and communicate common views with other initiatives and organisations;[13]
- FIRST – Forum of Incident Response & Security Teams (FIRST) is a worldwide network of incident response teams. FIRST has an annual conference and a number of mailing lists and working groups dedicated to, for example, Law Enforcement Co-operation Special Interest Group (LECC SIG);[14]
- Cybersecurity Information Exchange Framework (Cybex) is a set of related specifications concerning incident response, information assurance and forensics being progressed by the International Telecommunications Union-Telecommunications (ITU-T) in Geneva. Dating from 2010, this aims to pull together a number of 'best practices and standards for platforms' to achieve the minimisation of vulnerabilities, capture of incident information for analysis and facilitation of evidence for enforcement action;[15]
- Messaging Standard for Secure Information Exchange (MS3i) was a project funded by the European Union for a messaging standard for Information Exchange (Symantec LIRIC, 2009);
- The Traffic Light Protocol (TLP) is an informal mechanism to support trusted information dissemination (Stikvoort, 2009), primarily for higher-level cyber security information exchange (such as information on best practice and successful approaches to mitigation). The TLP was initiated in the UK by the Centre for the Protection of the National Infrastructure (CPNI) but has now been adopted by other countries such as Germany (Federal Ministry of the Interior, 2008);
- Finally, a number of industry initiatives regarding botnet mitigation are underway. These include, for example, efforts by Eco, the German association of Internet Service Providers (ISP) to investigate the legal barriers in Germany governing what network data (traffic and packets) can and cannot be shared in order to

[12] See http://www.terena.org/tf-csirt [accessed 22 August 2011]

[13] See http://www.egc-group.org [accessed 22 August 2011]

[14] See http://www.first.org [accessed 22 August 2011]

[15] See http://www.itu.int/ITU-T/ [accessed 22 August 2011]

respond to incidents.[16] The Abuse Helper project[17] is an open-source initiative to help in the automatic processing of incident information from a wide range of high-volume information sources which is now being developed by the CERT community. Another interesting commercial example is the Abusix initiative, which aims to report network abuse back to the originators via a common Abuse Report Format (ARF) message as a way to shed light on providers who are responsible for malicious network traffic.[18]

1.6 ENISA's activities in the field of information sharing

ENISA has had an established series of activities on the work of CERTs since 2005. Beginning with the CERT Cooperation and Support Working Group, the Agency subsequently published a guide for CERT cooperation (ENISA, 2006a). Even in 2005, the CERT Cooperation and Support Working Group noted that very often legal issues are raised as an important question in the context of the absence of information sharing between CERTs (ENISA, 2006b).

In 2009 ENISA produced Part 1 of its national/governmental CERT Baseline capabilities Document (ENISA, 2009b), which represented a first attempt to define a minimum set of capabilities that a CERT in charge of protecting critical infrastructure should possess. This was followed up in 2010 by Part 2, which considered policy recommendations (ENISA, 2010a) aimed at establishing a suitable framework that will enable national/governmental CERTs to operate properly.

To help advance this work, ENISA noted in its 2011 Work Programme[19] that the legal factors confronting those involved in cross-border collaboration should be explored. This ties in with the proposal to revise ENISA's mandate, which envisages an expanded role of the Agency in providing assistance, support and expertise to the Member States and European institutions and bodies by investigating and helping remove obstacles to cross-border issues and detection and response capabilities (European Commission, 2010b). This follows on, for example, from the work of the Agency in 2005 with its CERT programme and Working Group on CERT Cooperation and Support.

1.7 Structure of the remainder of this report

Chapter 1 of this study is an introduction. The remainder of this report is divided into three chapters:

- Chapter 2 – About the study – describes the scope, audience, research aims and approach of the study;
- Chapter 3 – Legal and regulatory aspects – describes the findings from our research and analysis, highlighting the key legal factors in cross-border information sharing between CERTs, distinguishing where relevant between types of information source (e.g. literature review, survey or interviews);

---

[16] See http://www.eco.de [accessed 22 August 2011]

[17] See http://www.abusehelper.be/about [accessed 22 August 2011]

[18] See http://www.abusix.com [accessed 22 August 2011]

[19] ENISA (2011) Work Programme for 2011; Available at: http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/work-programme-2011/ [accessed 22 August 2011]

- Finally, Chapter 4 – Recommendations – sets out a number of recommendations at the European level, at the national level, and by the private sector. We also formulate a number of key questions that remain to be addressed in future research.

2. About the study

2.1 Scope and audience

ENISA commissioned a study team from RAND Europe and time.lex to explore the legal and regulatory aspects of information sharing and cross-border collaboration between national/governmental CERTs in Europe. This exploration was necessary in order to identify what efforts could have a high impact on CERTs' likelihood and ability to share information. The study also provides some analysis of other relevant aspects, for example who in CERTs has responsibility for addressing cross-border information exchange and the prevalence of cross-border requests. This study does not look at other aspects of information sharing, such as issues of trust or information exchange between entities other than CERTs addressed in other similar studies (see for example ENISA, 2009a; 2009b).

The primary stakeholders for the questionnaire carried out to gather data for this study were national/governmental CERTs, as defined in the ENISA Baseline Capability for National/governmental CERTs (ENISA, 2009a; 2010a) summarised thus:

- **National CERT:** a CERT acting as a national Point of Contact (PoC) for collaboration and information sharing with other national CERTs in EU Member States;
- **Governmental CERT:** a CERT responsible for the protection of governmental and public administration networks.

The term 'national/governmental CERT' is thus taken to mean any type of CERT (including national or government CERTs listed above) where they:

- Generally support the management of security incidents for systems and networks within national borders;
- Bear or are involved in the responsibility for CIIP within the borders;
- Act as official or *de-facto* PoC for national/governmental CERTs in other Member States.

Nonetheless, in order to capture as many perspectives as possible (and given the somewhat blurred nature of how some national/governmental CERTs are assigned responsibilities) we did not necessarily exclude input from other stakeholders with experience in incident response. This is because in some countries CERTs may have been specifically empowered by national authorities to act as the national or government representative.

In addition, it should be noted that the focus of this study is on the cross-border aspects of information sharing: that is to say the extent to which differing legal frameworks prevent or inhibit the sharing of information between CERTs in different countries.

The key stakeholders for this report include public sector representatives responsible for drafting legislation and CERT teams, including CERT managers responsible for setting policies and procedures for cross-border information sharing. The public and private sector representatives who benefit from the information shared will also be interested in this report in order to understand the context in which this information is passed on and the limits to this exercise.

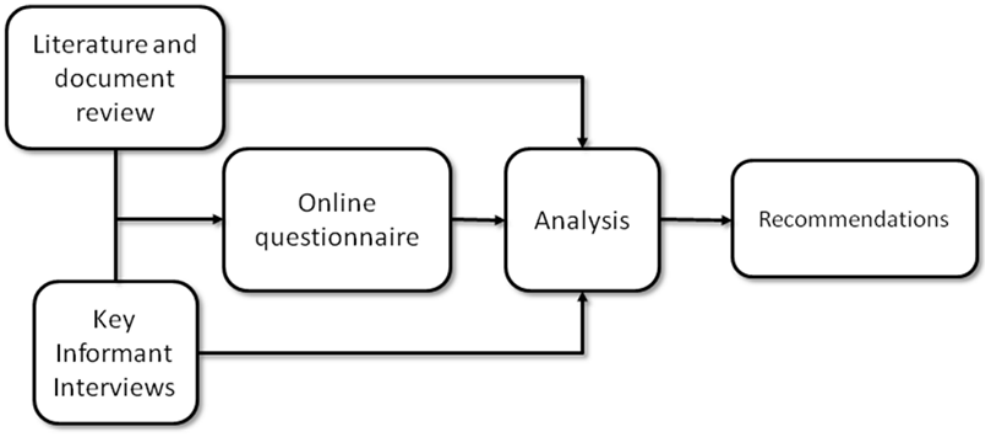
2.2 Research aims and approach

This study aims to identify the key legal and regulatory barriers and facilitators of cross-border information sharing between CERTs, in order to inform those responsible for drafting legislation or setting policies and procedures for CERTs how information sharing could be intensified and enhanced. As has been found in previous research (ENISA, 2010b), legislation and regulations pose a challenge to information sharing, especially when this is done trans-nationally. While some instruments have been developed to address this issue, this has tended to be addressed to law enforcement agencies, which CERTs are not. This research aims to address this gap by identifying those instruments that could strengthen and enhance cross-border information sharing among CERTs specifically.

The study sought to gain a comprehensive understanding of the situation affecting CERTs by applying multiple research methods to gather a large sample of the knowledge on the issue. This research was conducted in four stages as shown in

Figure 1.

Figure 1: The study team's research approach



2.2.1 Literature and document review

The study began by conducting a structured literature and document search according to the principles of the systematic review, across the peer reviewed and 'grey' literature. As a first stage we executed keyword searches on Google Scholar and the ISI Web of Science using common search terms for this topic.[20] After reviewing the abstracts or summaries of returned results we identified 43 sources of interest.[21] This was supplemented by inclusion of other material known to the study team, conducted via hand searching of the Association for Computing Machinery (ACM) Digital Library,

[20] Including: 'data OR information AND sharing AND CERT'; 'data OR information AND sharing AND CSIRT; 'data OR information AND sharing AND CERT'; 'data OR information AND sharing AND CSIRT AND law'; 'Data OR information AND Sharing AND CERT AND regulation'; 'Data OR Information AND sharing AND CSIRT AND regulation'.

[21] With GoogleScholar we reviewed the first 5 pages of results as there were over 110,000 hits for these terms. ISI web of science returned 234 results.

combined with in-house knowledge of the researchers. We excluded sources before 2001 from our targeted search and those not in English.

2.2.2 Key informant interviews

In order to explore some of the issues raised by the literature in further detail, we then conducted a total of seven key informant interviews (KIIs). Key informant interviews were used to test and validate some of the findings from the literature and document review. During these discussions members of the research team investigated the impact of legal and regulatory factors on how CERTs perform their activities, which specific legal and regulatory issues arise during the sharing of incident response across borders and what, if any, solutions had been put forward to overcome these. Each interview lasted for between 45 to 60 minutes and was conducted on a 'Chatham House rule' or un-attributable basis.[22] The individuals we consulted included representatives from operational CERTs, legal experts and policy practitioners specialising in information sharing.

2.2.3 Online questionnaire

Having gathered data on the current state of the art regarding the understanding of legal factors concerning information sharing, the final data source was an in-depth online questionnaire aimed at CERTs and organisations supporting CERTs. The focus of this questionnaire was national and governmental CERTs, but we did not exclude responses from other CERTs. The questionnaire was split into sections for those reporting themselves as 1) managers, 2) technical personnel or 3) legal experts across a) CERTs and b) organisations supporting CERTs.

The questionnaire was open from 1 June to 17 July 2011. Invitations consisting of an email message and a link to the survey were sent to the following communities of interest:

- European Task Force Computer Security Incident Response Team (TERENA TF-CSIRT);
- FIRST Law Enforcement CSIRT Co-operation Special Interest Group (LECC SIG);
- European Government CERT community (EGC);
- Legal experts from the EU Member States with knowledge of information and communication technology (ICT) and computer misuse legislation.

Reminders were sent approximately three weeks after the original invitation.

In total 50 unique browser visits to the survey link were recorded. Usable responses, however, decreased from 34 at the first set of questions (Q2: 'Your organisation') to 9 at the last question (Q72: 'Please indicate your email address'). Efforts were made to encourage responses via participation in the 23rd Annual Forum of Incident Response Teams (FIRST) Conference in Vienna from 12–17 June 2011. Telephone follow-up with members of the EGC was undertaken between the European Public Private Partnership for Resilience (EP3R) meeting mid-June and the end of July 2011, encouraging participation. Aside from the more common aspects concerning online questionnaires

[22] In the context in which the 'Chatham House Rule' is invoked in semi-structured key informant interviews, remarks made by interviewees are un-attributable and neither the identity nor the affiliation of the speaker(s) may be revealed; for more information see http://www.chathamhouse.org/about-us/chathamhouserule [accessed 23 August 2011]

(Schonlau et al, 2002), evidence derived from limited follow-up with some declining to respond was insightful in the specific context of this study. These follow-up communications illustrated the gaps in knowledge that continue to characterise the domain of CERT cooperation and the legal basis upon which they operate. Many of those responsible for operational activities in CERTs indicated they were uncomfortable in answering the legal questions due to a lack of knowledge, whilst legal experts indicated that as they did not represent a CERT they felt the survey was of no relevance for them.

Received responses included those from the following European countries (where the respondent self-reported their country):

- Austria
- Belgium
- Czech Republic
- Denmark
- France
- Germany
- Luxembourg
- Malta
- Poland
- Spain
- Sweden
- Switzerland *(noting that Switzerland is not a Member State of the EU but participates in the EGC group*)

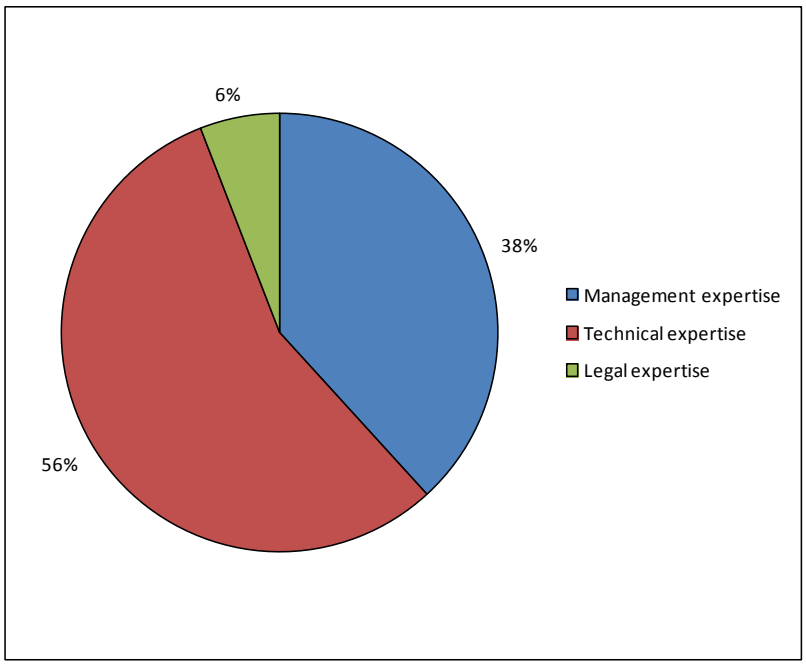
We also received responses from participants reporting their country as being outside the EU, including the United States and Georgia. Others did not report which country they were from, or represented themselves as from industry.

Examples of the types of respondents to the questionnaire include: CERT Manager; Head of CSIRT; Team Lead; Executive Director; Engineer and Analyst.

Finally, an informal Expert Group was established and administered by ENISA to provide critical review and input into the content of the preparation of drafts of the initial edition of this report.

Figure 2 indicates the split of respondents with respect to their principal role: 56% of respondents reported having a role involving technical expertise, 38% managerial expertise and 6% legal expertise.

Figure 2: Type of expertise of respondents



Source: RAND Europe and Time.Lex survey (2011) n = 34

2.3 Scope and limitations of the data

Overall, from our literature and document review, we found that the theoretical evidence base is rather scarce concerning the exact nature of the topics under discussion. The evidence identified as closest to the topic of this study in the peer reviewed literature concerned specifically communications secrecy (particularly in the United States, under e.g. the Stored Communications Act) (Burstein, 2007) and a grey literature document which was identified during hand searching on the Data Protection Directive 95/46/EC and information sharing, delivered at an incident response conference (Cormack, 2011). However, even this paper did not concern itself with the specific cross-border aspects of these challenges.

Other work identified in previous ENISA studies (e.g. Gal-Or and Ghose, 2004) covers the legal and regulatory ramifications of information sharing more generally (including different mechanisms like CERTs) but also Information Sharing and Analysis Centres (ISACs) in respect of liabilities, tax breaks and so on.

The literature on more generalised information sharing (e.g. see Bessant, 2009; Thomas and Walport, 2008) is in some ways closer to the topic of our discussion in that some of the relevant legal frameworks (e.g. the Data Protection Directive 95/46/EC; Directive on Privacy and Electronic Communications 2002/58/EC as amended by the Citizens Rights Directive 2009/136/EC) are discussed, but not in the specific context of computer security incident response. Indeed, the way in which these legal frameworks act as an

impediment or enabler for the sharing of a variety of other information (e.g. for the delivery of healthcare, social care, tax administration or broad criminal justice policy) is considered. Literature on the world of intelligence more generally may also be seen as a possibly useful area of further interest.[23]

More broadly, there could be other parallels in other highly regulated domains (noting the different objectives and rationales): for example, incident response with respect to nuclear safety or air safety (for example the 'airprox' reporting system[24] established by the UK's Civil Aviation Authority), which could have an inherent cross-border aspect to it in respect of the reporting and sharing of information regarding safety-related incidents.

From a competitive perspective the question of misaligned incentives concerning information sharing (i.e. competitors are dis-incentivised to share information due to concerns that peers will gain some kind of advantage from disclosed information) may also be observed in the highly competitive domain of cancer research. As an example, a specific non-competitive platform called the International Cancer Research Portfolio has been set up to address such concerns.[25]

Nonetheless, regardless of the domain, the literature very much characterises this issue as a trade-off between a set of laws or frameworks (data protection, privacy, etc.) and a set of organisational or socially beneficial objectives (addressing terrorism, crime, misuse of computer networks). Clearly, the exchange of information (including in cross-border scenarios) should not be examined as a risk to the fundamental right to privacy, without also acknowledging that these exchanges are a precondition for responding effectively to ICT incidents. Therefore, they act as an enabler to the exercise of various rights enshrined in the Charter of Fundamental Rights of the European Union that could otherwise be encumbered by such incidents, including the protection of integrity of the person, personal life, data protection, freedom of expression and information, the freedom to conduct a business and the right to property.

Concerning the literature on CERTs specifically, there is relatively more documentation (particularly in the grey or non peer reviewed literature) concerning the complexities of establishing CERTs and incident response functions. The literature (e.g. Killcrece, 2003) notes the issue of legal issues and the importance of getting legal expertise but does not go into further detail (e.g. on the specific aspects of what these exact concerns are and what substantive legal issues the teams may be confronted with). In addition, there are other quoted dilemmas, such as the difficulty of matching legal definitions of crime to technical understanding of a typology of misuse (Valeri et al, 2005).

---

[23] Research into how intelligence and legal frameworks relate may of course be difficult to conduct and access for security reasons. However, in a recent public broadcast for the 2011 BBC Reith lectures, Dame Eliza Manningham-Buller, former Director General of the British security service, MI5, referred explicitly to some of the benefits and challenges of working under a clearly defined legal framework. And in referring to information sharing she said, 'Sharing intelligence is not always straightforward because of differing approaches and legal frameworks, but at that meeting [between the USA's CIA and the UK's MI5] we were all among friends whom we trusted.'

[24] See the Civil Aviation Authority: UK Airprox Board – http://www.airproxboard.org.uk [accessed 30 November 2011]

[25] See http://www.cancerportfolio.org/index.jsp [accessed 22 August 2011]

Moving to the empirical evidence, the questionnaire used in this survey gathered responses from practitioners directly involved with the work of CERTs. The responses highlighted the key tension in this study: that cross-border information sharing between CERTs operates on an informal basis and gaps remain concerning the involvement of legal experts. The questionnaire was not intended as a comparative data-gathering exercise since the intent was not to attribute or evaluate the performance of CERTs in specific EU Member States. Rather it was intended to identify issues and those factors which appear in practice. Nonetheless, the evidence derived from our questionnaire should not be taken as representative of the views of all those CERTs in Europe classifying themselves as a national/governmental CERT.

3. Legal and regulatory aspects of information sharing and cross-border collaboration of CERTs in Europe

In this chapter we consider the legal and regulatory aspects of information sharing in detail. We use the broad term 'legal and regulatory aspects' to include not only specific legislative instruments but also softer coordination measures which may be 'self-regulatory' in nature.

We begin by highlighting the key arguments for what CERTs must do and why their activities may raise legal questions. We then briefly touch upon information sharing practice in other policy domains. Then we detail each of the different legal frameworks that may affect the practice of cross-border information sharing in relation to the activities of national/governmental CERTs. Finally, using evidence from the key informant interviews and online questionnaire, we then present empirical evidence as to the extent that these legal frameworks are considered as barriers or facilitators of cross-border information sharing between CERTs, in particular national/governmental CERTs.

Legal factors exist within a set of concerns and possible inhibitors of cooperation that also include, according to ENISA (2006a):

- necessity for confidence;
- financial resources;
- lack of Service Level Agreements (SLAs);
- differences in legal systems;
- lack of political/executive support;
- adoption of standards.

Killcrece (2003) indicates that generally the role of the CSIRT or CERT often focuses on technical issues of an incident – the 'what' and the 'how'. Sometimes they will need to become involved in the investigative processes ('who' and 'why'), which is where knowledge of legal systems becomes particularly relevant. However, any involvement in investigations and interaction with law enforcement may be outside the formal mandate of handling computer security incidents and supporting recovery. ENISA (ENISA, 2010a) notes that cooperation with Internet Service Providers (ISPs) is a crucial step in cooperation with law enforcement to address cyber crime (which can indirectly undermine Critical Information Infrastructures).

3.1 The balance between achieving operational objectives whilst respecting legal obligations

3.1.1 Operational considerations

In this section we elaborate on the first aspect of this debate: those considerations regarding the activities of CERTs which may present legal concerns.

The main tension inherent in understanding these aspects associated with cross-border CERT collaboration is that of meeting legal obligations without undermining the activity and effectiveness of informal collaboration and cooperation which characterises cross-border CERT interaction. This speaks to the heart of the policy objectives for this study: it was reported by a key informant interviewee that cross-border collaboration between CERTs is generally regarded to be effective because it works on an informal basis.[26]

[26] Anonymous interviewees: 11/05/2011 and 11/07/2011

Although legal issues and concerns do appear (mainly in relation to the legal basis for CERTs), in the main, cooperation and collaboration takes place in a practical, informal manner between operators who have trusted relationships rather than because of any strictly formalised legal agreement. This has been regarded as a strength of the CERT community in that such trusted relationships which have been built up over time are considered as key to rapid and effective collaboration (even in a cross-border context).

Kenneally and Claffy (2010) identify this as a 'purgatory' formed by the gaps in regulation and law, commercial pressures and evolving considerations of both threat models and ethical behaviour.

This informal collaboration is based on a number of socio-economic factors, mainly relating to the presence of trust (ENISA, 2010b). Messenger (2005) discusses how trust plays a role in different public–private partnerships (of which national/governmental CERTs are but one example):

- Credibility – technical credibility may be seen as an enabler of trust. When technical staff interact with each other psychological assessments may be undertaken as to whether the other party 'knows what he is talking about';[27]
- Frequency of contact – if individuals see their counterparts on a regular basis then this increases trust, further fostering cooperation. This is particularly emphasised through social interaction at face-to-face meetings (ENISA, 2006b). This is often seen as a major sociological or financial stumbling block in achieving cross-border cooperation since holding physical meetings requires funding to cover travel and subsistence costs;
- Identification and sharing of common intentions – particularly the case where cyber security professionals and those working in incident response are generally working toward the same objective (resolution of a problem and improvement of levels of security on the network).

Silicki and Maj (2008) identified the following barriers to CERT cooperation:

- Lack of service level agreement between CERTs – although CERT culture works on the basis of informal cooperation, the absence of rules for strict reaction time can slow down cooperation;
- Differences in legal systems – different CERTs work in different legal environments and must fulfil the requirements and operate in accordance with the legal regime of their own country, which affects when and with whom they can share data;
- Lack of standards – still under-developed standard of CERT cooperation (despite existence of best practices like the IETF, 1998);
- Insufficient organisational, political and financial support – more cooperation necessarily incurs greater financial costs and CERTs are often not seen as 'mission-critical' by their parent organisation – also for private sector based teams management may regard cooperation as impossible due to concerns about breaching anti-trust law.

CERTs must collect and analyse traffic data and other information that may assist in the response and management of security incidents (for example 'Netflow'[28] data) as part of

[27] Anonymous interviewee: 15/07/2011

fulfilling their operational obligations regarding handling security incidents (ENISA, 2009b) (NB: national or governmental CERTs may not be directly connected to networks to analyse this data).

It is important to collect this kind of data for two main reasons: for the management of incidents with a national, regional or large-scale implication for National or European Critical Information Infrastructures and to aid in understanding the nature and challenges of the security concerns (for example, by understanding common attack routes in the constituency of the CERT).

These obligations stem in part from Article 13a of Directive 2009/140/EC amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associate facilities, and 2002/20/EC on the authorisation of electronic communications networks and services ('Revised Telecommunications Regulatory Framework 2009'), which covers measures that electronic communication service providers must take to guarantee the security and integrity of public communication networks. This chapter imposes a requirement upon all public electronic network and service providers to 'take appropriate steps to ensure the security of public communications networks and services'.

The IP address is undoubtedly of pre-eminent significance for incident response (Cormack, 2011), as an example of personal data that is frequently used to identify the source of an incident; however, according to the Article 29 Working Party opinion on the concept of personal data, IP addresses can be considered as personal data because of the possibility (and in this context relative likelihood) of such IP addresses being linked to a natural person (Article 29 WP Opinion 4/2007).

Cormack (2011) argues that the collection and use of IP addresses by CERTs should be justified under Article 7 of the Data Protection Directive 95/46/EC. This article specifies the conditions under which the processing of personal data is legitimate (including the collection of IP addresses with the intent of using these to identify individual subscribers of the internet account). Even in the absence of consent of the data subject (i.e. the subscriber), data collection by CERTs could indeed be justified under some of the options offered by Article 7. The primary possibility would seem to be Article 7 (e), which allows processing of personal data if this 'is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed'. Obviously, this option would only apply if the CERT has been given a specific legal mandate to that effect.

If this is not the case and no legal mandate is available, a CERT might still try to appeal to other options permitted by Article 7, for example by invoking a legitimate interests pursued by the CERT or by the third parties to whom the data are disclosed (such as law enforcement bodies), as permitted under Article 7 (f). This possibility was also indicated by Cormack with reference to Recital (53) of the Citizens Rights Directive 2009/136/EC, which discusses this option, noting that '[t]he processing of traffic data to the extent strictly necessary for the purposes of ensuring network and information security […] by providers of security technologies and services when acting as data controllers is subject

[28] NetFlow is a network protocol developed by Cisco Systems for collecting IP traffic information http://en.wikipedia.org/wiki/Netflow [accessed 22 August 2011]

to Article 7(f) of Directive 95/46/EC'. However, the legitimacy of appealing to Article 7(f) is subject to the consideration of the interests for fundamental rights and freedoms of the data subject. As indicated in the Recital, this consideration is to be judged favourably when the appeal to Article 7(f) is made by network operators themselves, and by providers of security technologies and services to the network operator. However, the result is much less likely to be favourable with respect to private CERTs looking to exchange personal data with third parties. Given the rather serious privacy impact of the collection and retention of personal data under this legitimate interest (i.e. that the intent of the use of the data is to initiate or support law enforcement investigation), undertaking such activities without a clear and unambiguous legal basis (such as national data retention laws or telecommunications privacy laws) is likely to raise legal concerns (Brown 2010).

The applicability of personal data legislation to the exchange of information by or between CERTs creates legal challenges in other respects as well. An important example is the restrictions imposed by the Data Protection Directive and its national transpositions on the transfer of personal data to destinations outside the EU and EEA. In principle, such transfers are forbidden, to avoid European personal data becoming subject to laws with less stringent data protection requirements. A series of exceptions to this rule exist, with the most appealing option to CERTs being that the transfer could be argued to be necessary or legally required on important public interest grounds (Article 26.1 (d) of the Directive). However, as with the appeal to Article 7(e) above, this exception is likely to be applicable for national or governmental CERTs with a clear mandate; but much less so for private CERTs without such a mandate. In their case, other exceptions may apply, such as a finding of adequacy of the foreign law through a Commission Decision, the consent of the data subject, the use of specific pre-approved contractual regimes or (for destinations in the USA) the voluntary adherence by the data recipient to the so-called 'Safe Harbor' regime. However, for private European CERTs looking to exchange personal data with destinations outside the EU (e.g. to non-European CERTs or law enforcement bodies), these options are likely to be unavailable or administratively prohibitive. As in other contexts, EU data protection regulations in this area are relatively demanding and may serve as a clear disincentive to the exchange of personal data by CERTs in international incidents that transcend the European context.

It is important to understand how the activities of the CERT relate to incident response and the sharing of information. CERTs act as monitors of network traffic data between source and destination IP addresses. In addition, in certain circumstances (e.g. where the use of Deep Packet Inspection is necessary to handle an incident), packet data (broadly speaking the content of the traffic) may be monitored. National/governmental CERTs may handle this data themselves or, if they act as a portal or aggregator, may receive this kind of data from their constituents. CERTs therefore will need to analyse this information themselves and may need to share it to alert others to the presence of a threat or attack. However, these other stakeholders could include not just peers (other CERTs) but also banks, individuals, Internet and other service providers. These other types of public and private stakeholders may be located in the same country or may be in other countries. Given the CIIP remit of national/governmental CERTs, with regard to the sharing of information between these specific types of CERTs and their teams, specific considerations may apply (i.e. that there might be an overriding national security interest in sharing this information which may envisage a proportional but necessary abrogation of fundamental human rights as defined in the European Convention on Human Rights).

In any case, CERTs must be familiar with any privacy laws that provide protection to others (Killcrece, 2003b) in order to 'avoid the possible suppression of any improperly gathered evidence that is intended to be presented in a court of law, as well as to avoid potential criminal or civil liability'.

There is also another issue concerning the obvious tension between the need for a CERT to meet its operational obligations concerning formulating and effecting a response to a security incident, versus the requirements that may be imposed by the intervention of those responsible for enforcement of the law (either in a civil or criminal sense) such as the police. Sommer (2009) discusses this in relation to digital forensics in an organisation where the priority of the organisation might be to keep the system running, whilst the main focus of law enforcement might be to shut down the system as way of preserving evidence (essentially, freezing the scene of a crime), or monitoring as part of a broader intelligence effort aimed at reaching further up a criminal enterprise. This has also been recognised elsewhere by interviews from the public and private sector. In addition, new business drivers such as cloud computing may complicate this (Grobauer and Schreck, 2010). This is because, in a cloud computing environment, it may be impossible to separate out data identified of interest for the purposes of an investigation from other customer data (Robinson et al, 2011).

3.2. Information sharing in other domains

The tension between meeting legal obligations concerning what information can and cannot be shared is also common in other domains where the requirement is to proportionally balance utility goals with privacy risks for data seekers and data providers (Kenneally and Claffy, 2010). In this section we briefly describe information sharing and exchange practice in other policy domains.

3.2.1 Information sharing, personal data and societal benefits

Writing about information sharing for the public sector more generally, Thomas and Walport (2008) discuss how the legal framework concerning privacy and data protection in the UK may affect information sharing for a wide range of societally beneficial tasks including the provision of social services, law enforcement, medical research and so on.

Bessant (2009) also describes relevant legal frameworks with respect to generalised information sharing across a number of different policy domains in the UK. These include counter-terrorism, law enforcement and the provision of social benefits (e.g. social security). This illustrates the complexity and divergent requirements of information exchange, especially as it concerns the achievement of broader societal objectives.

3.2.3 Information sharing and national security

Miller (2005, p. 14) highlights similar tensions with respect to information sharing between the law enforcement and intelligence communities, as with the War on Terror: as he puts it, 'criminal intelligence is governed by constitutional rules of evidence [while] national security is not'. These two communities do not have the same legal training and skills, and from this arise cultural differences including: interest in sharing information, extent of secrecy about information, and level of detail of information.

Willis et al (2009) also discuss information sharing with respect to national security efforts to protect critical physical infrastructures. This infrastructure protection domain also requires extensive information sharing between the public and private sector. Willis et al (2009) note the perception that the private sector is concerned about what happens to information once it reaches the public sector. This focuses on leaks to proprietary

information, losing customers or investors if vulnerabilities are made public, issues of liability, and the inadvertent promotion of new regulatory procedures. The public sector concern is mainly about failure to protect methods and sources. To overcome these barriers, the authors recommend clearly establishing the relative advantages of sharing information; consolidating efforts in information sharing (e.g. joint working groups); being creative in avoiding legal pitfalls; introducing firewalls to limit liability; and empowering chief security officers.

3.2.4 Information sharing for pharmacovigilance

Others (Pirmohamed and Darbyshire, 2004) have discussed the need for information sharing in the context of monitoring new drug safety. Systems that, for example, enable postmarketing surveillance of drugs, could be used as hypothesis-generating tools in further pharmaco-epidemiological studies. Almenoff et al (2007) provide a modern example of such systems-based platform that supports prioritisation of safety issues, in-stream review and data retrieval, aggregate-level analysis of data patterns and knowledge management. Pirmohamed and Darbyshire also highlight the importance of sharing information across prescribers, researchers, regulators, the industry and the general public and that legislation must not discourage sharing of information that is needed to protect public health. On the other hand, they stress the need for safeguards for appropriate interpretation of the data in order to avoid potential controversy and mistrust because of inappropriate focus on potential harms, as was the case with the measles, mumps and rubella (MMR) vaccine.

3.2.5 Information exchange in the nuclear industry

In 1986, Collins et al argued that 'similar provisions [concerning information sharing] should be expected for any nuclear facility or activity where there exists the possibility of harm in the event of a serious plant malfunction, nuclear accident or radiological emergency' (Collins et al, 1986).

Following the Chernobyl accident in 1986, most European countries established or enhanced their national radioactivity monitoring and information systems. To date, the most significant safety-related cooperation internationally is through the World Association of Nuclear Operators (WANO). WANO was formed following Chernobyl to maximise the safety and reliability of nuclear plant operation. With regional centres in Atlanta, Moscow, Paris and Tokyo and a coordinating centre in London, WANO links all 115 operators of nuclear power plants in 34 countries. Today, WANO also involves private sector operators of nuclear power plants, reactor designers and vendors, so that there is better feedback of experience.

WANO focuses on four major programmes: peer reviews; operating experience; technical support and exchange; and professional and technical development. WANO peer reviews are the main proactive way of sharing experience and expertise. They are focused on operations, not the design (or location) of power plants.

Information exchange on operating experience is the basis of WANO's various programmes. Information and event reports are submitted by each operating organisation to its regional centre, where they are reviewed for clarity and completeness and then distributed to all WANO members using an international exchange system. If particular trends or concerns become evident a Special Operating Events (SOE) report may be drawn up and circulated, and this has the force of a recommendation arising from peer review. The type of event reports produced by WANO include:

- Event Notification report, for reporting significant consequential events even if causes are not yet fully known, and where immediate action is required to avoid the same action occurring elsewhere;
- Event Analysis Reports, for reporting significant consequential events once full analysis has been completed and consequences, together with direct and root causes, understood;
- Event Topic Reports, for two or more events that contain a similar theme or problem areas. These reports are prepared by members directly or by WANO regional centres;
- Miscellaneous Event Reports, for events that do not meet the above criteria but which are likely to be of interest to other members.

3.2.6 Observations

Thomas and Walport (2008) note that the central consideration in regard to the sharing of personal data is the question of proportionality: when is it proportional to use or share data? Whatever the circumstances, they emphasise that clear guidance, professional skills and rigorous training are important in matters regarding the sharing of personal information.

In the context of hazards and public protection, we found from the literature and documents that communication among parties is termed 'information exchange' rather than 'information sharing'. The term 'information exchange' implies a two-way information flow among the participating parties within a formalised framework that could include special assistance missions in case of an emergency, training programmes, technical guidance, etc. Information exchange regarding timely implementation of measures to protect the public against both natural and man-made hazards (e.g., typhoons, dam failure, high-volume storage of toxic gaseous materials) and accidents is a well-established practice.

Having reflected upon the considerations of the 'why' that legal issues may pose challenges for CERTs, we now turn to a summary of specific relevant legal frameworks; both those that may enable cross-border information sharing and, perhaps more importantly, those that present challenges.

3.3 Relevant legal frameworks and regulations concerning information sharing between CERTs

A paper published with regard to legal lessons learned from the 'cyber attacks' in Georgia highlighted pertinent ongoing questions about the relevant legal frameworks applicable to major incidents affecting national-level CIIs in a cross-border context (Tikk et al, 2008). Relevant legal lessons in the context of this study[29] (which may support cross-border information sharing) focused on two areas:

- With regard to addressing the problem through legal frameworks covering criminal justice, two possibilities of relevant legal frameworks apply: international and national criminal law. International criminal law may have been used as a

[29] The NATO CCDCoE report also noted Law of Armed Conflict (LOAC) considerations, namely that the complexities of attribution and difficulty of measuring the impact of incidents makes it difficult to determine the applicability of LOAC – namely jus ad bellum (rules governing the criteria for engaging in armed conflict) and jus in bello (rules governing the conduct of armed conflict). Such rules might provide justification in international law for any subsequent measures or mitigation taken to protect or defend against such an attack.

way to gain political support for the investigation and prosecution of those responsible if Georgia had ratified the Convention on Cybercrime. National criminal law in conjunction with a request to the country where the attacks were identified as originating from under the European Convention on Mutual Assistance in Criminal Matters and Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters would be another possibility. However, given the noted inefficiency, ineffectiveness and reluctance of nation states to cooperate in public international legal obligations in general (due to the absence of sanctions) this route would also likely yield insufficient results.

- Another option for management of such major incidents (which implies a degree of information sharing) is via the legal framework governing ICT more generally. This might include, for example, obligations on providers of e-communication networks to provide for the security and integrity of their communications services (as detailed in Article 13a of the Revised telecommunications regulatory package 2009); provisions regarding the protection of personal data (which creates a clear understanding of the terms of using data available about the incidents for the purposes of investigation and further prevention) and legal obligations governing data retention.

With regard to data collected by CERTs as being useful for prosecutions (Sherman, 2004) states that e-evidence is either computer generated or computer-stored which means that its source needs to be ascertained as well as whether it is 'original' and therefore subject to hearsay, or if individuals need to be brought in to re-ascertain the point. CERTs may interact with various types of evidence which may carry different weight and credibility.

Sherman (2004) notes that CERT incident analysis procedures have been put in place to favour this ideal scenario by contacting the right people at the right time and protecting the evidence. There are examples of where these procedures are not followed, however; which means it is then harder to bring cyber criminals to justice.

In addition, CERTs also use 'management information systems' that include ticketing systems to allow administrators to keep on top of the progress of incidents.

We now turn to consideration of some specific legal concerns.

3.3.1 Definitions of computer and network misuse

Valeri et al (2005) indicated that significant divergence continued to exist regarding the definition of different types of computer and network misuse across European Member States. At the international level, a certain degree of harmonisation has already been attempted via the Convention on Cybercrime. However, while it was signed by 47 countries, the Convention has thus far entered into force in just 31 countries; only 17 of these are EU Member States.[30] In the European Union, the 2005 Framework Decision on Attacks against Information Systems 2005/222/JHA brings this into EU law and defines

[30] As of July 2011 30 have it in force – 31 including the UK on 1 September: Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, the former Yugoslav Republic of Macedonia, Ukraine, USA. For a full overview of signatories, ratifications and entry into force, see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=05/08/2011&CL=ENG [accessed 22 August 2011]

minimum sanctions for each type of offence. Nonetheless, full harmonisation of definitions and sanctions was not achieved (or envisaged) by these initiatives.

This could be perceived as a barrier because in the absence of consistent definitions in law, there may be difficulties in sharing information – for example, a request from one CERT to another might be acted upon, only to find that in the third country jurisdiction the type of misuse being identified is not prohibited by law, or the maximum permissible sanction is so low as to make it more trouble than it is worth. Although this is primarily a law enforcement and prosecution concern, a possible secondary effect may be that CERTs are dis-incentivised to invest in information exchange if they see that no action is taken.

Similarly, CERTs need to take into account the sometimes broad definitions of certain types of cyber crime, including for example the definitions of illegal access to information systems (hacking), illegal system interference, and illegal data interference (e.g. see Vermeulen and De Bondt, 2009). This presents a dual challenge to them: in the absence of formal investigative mandates, there is a risk that activities they have engaged in to obtain or exchange information may themselves qualify as illegal activities as illegal activities, both tainting the information for further use by other CERTs or investigative bodies, and opening them up to legal liabilities. The risk of personal legal liability becomes greater when CERTs have no clear mandate from their national government to conduct specific investigations or collect new information, as this implies that their actions or requests have no official authority or basis in law. Thus, CERTs need to make sure that the information in their possession is lawfully obtained. In case of doubt, they are unlikely to make the information available to other CERTs or third parties.

The Framework Decision on Attacks Against Information Systems 2005/222/JHA is expected to be repealed and replaced in the course of 2011 by a new Directive on Attacks against Information Systems,[31] which intends to provide closer harmonisation of the definitions and penalties related to certain types of crimes, and focuses on newer types of cyber crime, such as the use of botnets. However, as a Directive (which inherently leaves a margin of appreciation with respect to national implementation), it is not yet clear to what extent this will be capable of aligning national laws. Additionally, the Directive also aims to strengthen the existing structure of 24/7 national contact points, which should improve and facilitate cross-border communication.

3.3.2 The European legal framework governing data protection and privacy

Perhaps the most often quoted and arguably most pertinent example of a legal framework having an implication with respect to incident response is law governing privacy and personal data protection. This challenge is not necessarily unique to one country or another: the question of achieving a 'balance' between meeting legal obligations concerning privacy of user and subscriber data versus network security obligations is by no means unique to Europe.

In Europe this boils down to the complexity of the implementation of the regulatory framework governing the use and protection of personal data.

We use the term 'European legal framework concerning the use and protection of personal data' to refer collectively to data protection and eprivacy regulations, as

[31] For the current draft, see Council of the European Union, 24 February 2005.

regulated by the Data Protection Directive 95/46/EC, the Electronic Communications Privacy Directive 2002/58/EC as amended by the Citizens Rights Directive 2009/136/EC ('ePrivacy Directive 2002/58/EC') their national transpositions and associated instances of policy implementation.[32]

Evidence from the interviews suggests that the provisions regarding personal data (specifically IP addresses) are overly burdensome and present a clear barrier to CERTs exchanging data. This problem is exacerbated by the uneven interpretation at the Member State level, which is the key challenge. This is borne out by a recent study commissioned by the European Commission Directorate General Information Society and Media (Graux, 2011, p. 40) which described the different circumstances under which IP addresses have been qualified as personal data. According to this report,

> 'the trend at the aggregate level is clearly to take a broad interpretation and to qualify IP addresses as personal data when there is any likelihood of the IP address being linkable to a natural person on the basis of the available infrastructure (specifically additional information such as log files) or on the basis of the intended or expected use of the IP addresses (specifically the intent to identify a subscriber). Rulings to the contrary tend to relate mainly to cases where the judge (rightly or wrongly) believes that such use is not reasonably possible or likely.'

Thus, whenever IP addresses are to be exchanged between CERTs, data protection law is likely to be found applicable.

This can, however, put CERTs in a complicated position. Specifically, if CERTs manage to obtain information that may lead to the identification of a harmful actor (e.g. logged IP addresses, traffic data, usernames/passwords, deep packet inspection), it is likely they will have to comply with the provisions of national data protection laws. Moreover, it is quite likely that they may not be permitted to exchange this information freely with other CERTs (or other third parties), as it qualifies as personal data that may not be processed without appropriate justifications as described in Article 7 of the Protection Directive 95/46/EC. Furthermore, it should be noted that some Member States[33] have implemented specific legal protections with respect to judicial information, which will be subject to additional safeguards under applicable national law. Ignoring these obligations may result in the information being rejected by a court as being unlawfully acquired, thus undermining any subsequent investigations. This applicability of specific protections is subject strictly to national laws, meaning that CERTs may be confronted with diverging national restrictions.

Several instances of this problem were mentioned in the aforementioned IP addresses report, which contained a sample of 49 cases in which IP addresses had been processed. In 41 of these cases, the IP addresses were considered by courts to be personal data,

[32] For example, intervention by national independent supervisory authorities, or the authoritative Opinions of the Article 29 Working Party, which was established through the Data Protection Directive and acts as an independent European advisory body on data protection issues.

[33] For example in Belgium, where Article 8.1 of the Privacy Act contains a prohibition in principle on the processing of personal data concerning disputes presented to courts or administrative tribunals with respect to suspicions, prosecutions or convictions relating to crimes, or with respect to administrative sanctions or security measures. A comparable rule is enshrined in Section 21 of the Italian Personal Data Protection Code.

which has led to evidentiary material being rejected in a number of instances (Graux, 2011).

Cormack (2011) discusses the implications of Article 7 of the Data Protection Directive 95/46/EC regarding the sharing of IP address data. Specifically, it should be noted that the collection and analysis of data for internal uses within a CERT is a separate purpose from the sharing of information with third parties. Thus, even if a CERT can successfully explain why it has a mandate to process IP addresses under its national implementation of Article 7, this does not necessarily imply that the sharing of such personal data with third parties is also lawful. This issue is made even more complicated by the cross-border aspect, where a CERT may not have a clear insight in the exact nature and competence of the third party who would receive the information. Indeed, CERTs would need to be aware of what the limits of their mandate are, and what this implies with respect to the processing (including the sharing) of personal data, including potentially of IP addresses. CERTs should naturally be cautious on this point, as a violation of national data protection rules may expose them to liability, or invalidate their efforts by tainting the legal validity of the data as evidence, as commented above.

However, the activities of CERTs may also be regarded in the light of meeting security-orientated objectives of the European legal framework governing privacy and data protection: namely the obligation to provide for security of storage and processing. This, however, depends largely on their mandate and remit, and specifically whether they have been given official authority to investigate incidents and exchange data. Furthermore, it must also be recognised that the exchange of information (including in cross-border scenarios) should not be examined as a risk to the fundamental right to privacy, without also acknowledging that these exchanges are a precondition for responding effectively to ICT incidents and thereby supporting the exercise of other rights enshrined in the Charter of Fundamental Rights of the European Union, such as for example the protection of the integrity of the person and freedom of expression.

Two additional relevant legal texts are the frameworks for electronic communications (the aforementioned ePrivacy Directive 2002/58/EC and Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ('Data Retention Directive 2006/24/EC'). Collectively, these texts govern the data that may be (or is required to be) stored by providers of a publicly available electronic communications service such as ISPs and telephone companies. Under the Data Retention Directive, this includes for example the data necessary to trace and identify the source of a communication (user ID, IP address and (if applicable) phone number), similar data with respect to the destination of the communication, and data necessary to identify the date, time and duration of the communication.[34] Thus, they serve as a common basis at the European level to determine which information is likely to be available with such service providers established in the European Union. However, the harmonising effect of the Data Retention Directive should not be overestimated, as its implementation in practice has been 'met with serious legal resistance in a number of Member States' (Brown, 2010). Procedures raising constitutional objections against the national legislation proved successful in the Czech Republic, Germany and Romania, causing data retention laws to be annulled in these countries. Furthermore, significant differences remain between the

[34] See Article 5 of the Data Retention Directive for a full list.

Member States' laws on the exact scope of retention obligations (both with respect to the categories of information and retention periods), as well as the procedures for obtaining access to such data.[35] Thus, further harmonisation in this area may be required in the future.

In addition, the aforementioned amendment in 2009 of the ePrivacy Directive 2002/58/EC has introduced a data breach notification obligation, requiring providers of a publicly available electronic communications service to notify national supervisory bodies of any 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community' (Revised Telecommunications Regulatory Package , 2009, articles 3 (a) and 2 (h)). The provider is additionally required to notify the customer or subscriber, if the breach is likely to adversely affect the personal data or privacy of a subscriber or individual. While certain exceptions to these rules exist, they are nonetheless a useful principle for CERTs, as they provide red flag indications of when incidents have occurred, and what their impact may be.

However, the right to access this data (including by national/government CERTs) is not harmonised by these texts. Article 4 of the Data Retention Directive 2006/24/EC directly stipulates that retained data

> 'are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.'

Thus, there is more limited harmonisation on the issue of accessibility (and none at all with respect to exchange of information) than on the issue of data collection, other than the requirement to make data available only to 'competent national authorities.' Thus, once again, the mandate of CERTs will be a critical factor. Finally, it should be noted that these obligations only apply to 'providers of a publicly available electronic communications service'; thus, operators of closed or private networks will not be subject to these rules.

3.3.3 Freedom of information and public sector re-use of information legislation

There are varying interpretations and implementations of freedom of information (FoI) legislation across Europe. Freedom of information legislation governs the right or possibility of public sector authorities to make certain information available, upon request, to citizens to support accountability and transparency.

Rules with respect to Public Sector Re-use of Information (PSI) can also impact the operation of CERTs under some circumstances. In Europe, this issue is regulated by the

[35] See the April 2011 Evaluation report on the Data Retention Directive; http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf [accessed 22 August 2011]

Directive 2003/98/EC on the re-use of public sector information ('PSI Directive 2003/98/EC'). This Directive does not provide a generic right to access or re-use PSI; rather, it determines the obligations that apply when public sector bodies choose to make their PSI available, and what the rights of re-users are. For CERTs, this can be relevant when requesting permission to re-use information which is made available by public sector bodies, or inversely when they themselves are public sector bodies and make their own information available for re-use. In these circumstances, the PSI Directive provides a common framework for the rights of re-users, which could theoretically support the exchange of information. In practice, however, the impact of this framework is likely to be very limited for CERTs, primarily because the information which directly relates to security incidents that fall within their remit is unlikely to be made available for re-use.

Anecdotal evidence from interviews of those involved in incident response indicated that in regard to FoI, there was the possibility that those sending material had to mark it as 'exempt from onward FoI disclosure' in order to maximise discretion in exchanging information. Establishing how to do so legally required the support of specific legal expertise.

3.3.4 Criminal procedure

In the section above on definitions of computer and network misuse, we outlined the importance of current cyber crime legislation, and its potential impact on the activities of CERTs. However, it should be noted that other provisions of criminal law may also have an impact on the operations of CERTs.

Criminal procedural law is a key example of this, as it covers the various investigative competences and procedures in a given country, as well as the rules of procedure during criminal trials. At the European level, harmonisation of these rules is fairly limited and fragmented. The aforementioned Convention on Cybercrime contains a section on procedural law (Section 2 of the Convention), which provides a certain degree of harmonisation with respect to specific investigative measures in relation to cyber crime (specifically expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and the real-time collection of computer data). However, no comparable harmonisation initiatives exist at the EU level, meaning that rules and procedures for investigative measures may vary widely between the Member States.

This also implies that CERTs may not be able to avail themselves of the same tools to collect information, provided that these rules are even applicable to them (which will vary, depending on the status of a CERT as being a public body with law enforcement competences). Even when rules exist in all Member States, it is important to note that the harmonisation afforded by the Convention on Cybercrime is limited. For instance, it does not provide rules on the safe storage of seized information while investigations are being conducted. This implies that information which was lawfully stored by a CERT in its own country may not satisfy the legal requirements for safe storage in a different country, which could lead to the information being considered as unreliable evidence in a criminal proceeding. Such regulations with respect to the evidentiary value of information in criminal procedures remain largely a matter of national sovereignty.

It should be noted, however, that the European Union has increasingly adopted measures to improve judicial cooperation in criminal matters,[36] including specifically through the assistance request and information exchange mechanisms established by the Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (Convention on Mutual Assistance in Criminal Matters, 2000) establishing the Acts adopted under Title VI of the EU Treaty, Council Framework Decision of 30 November 2009 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (Council Framework Decision on Exercise of Jurisdiction 2009/948/JHA). Specifically with respect to cyber crime, it is worth noting that the Framework Decision on Attacks Against Information Systems, 2005/222/JHA required the establishment of 24/7 contact points in all Member States to facilitate the exchange of information. These provisions are expected to be retained and even strengthened in the anticipated Directive on attacks against information systems, which is set to replace the Framework Decision in the near future, and which will introduce an obligation for the contact points to respond to urgent information requests within eight hours (among other things). As with the procedural law rules above, however, the utility of these cooperation frameworks to CERTs depends largely on their own status, as this determines if they can directly avail themselves of the provided information exchange mechanisms.

3.3.5 Intellectual Property Rights

An ancillary body of law that may affect CERTs' ability to collect and exchange information is the domain of intellectual property rights. In the absence of a specific mandate as a law enforcement body, CERTs are not exempt from intellectual property rights, including copyrights, trademarks, patents and *sui generis* database rights as established under EU law. The scope of application of these rights can be very broad, with the line between protected and unprotected information being particularly blurred in the case of copyrights (Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society; Directive 2009/24/EC on the legal protection of computer programs; Directive 2004/48/EC on the enforcement of intellectual property rights, 29/04/2004) and *sui generis* database rights (Directive 96/9/EC on the legal protection of databases), as these do not require any prior registration. Thus, CERTs need to be aware that the duplication and dissemination of certain types of information (including many creative works and collections of data, such as log files) may be a breach of a third party's intellectual property rights. Obviously, this issue may also apply to the exchange of software that was supposedly used in a specific incident or investigation. This implies the need for access to specialised legal expertise to assess these questions, which may not be readily available to CERTs, for whom this is not likely to be considered a core competence.

3.3.6 Confidentiality obligations toward third parties

Apart from the intellectual property provisions mentioned above, the dissemination of information can also be controlled through confidentiality obligations, which can take a multitude of forms. Information may be provided to a CERT under formal or informal obligations of confidentiality. For instance, an ISP may make its voluntary cooperation with a CERT conditional on the secrecy of any incidents it reports, by establishing a non-

[36] See http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/index_en.htm [accessed 22 August 2011]

disclosure agreement, for example. Even in the absence of formal contractual obligations, information may be protected by trade secrecy rules, or it may be provided under the cover of whistle-blowing arrangements, which may serve as a legal impediment to the CERT for making the information available to other parties. These are challenges which are not formally regulated at the European level, and which may not even have a formal legal basis at the national level (e.g. non-disclosure agreements may be purely contractual in nature). Nonetheless, they can act as a strong disincentive for the exchange of information to a CERT.

3.3.7 Determining applicable law

A horizontal issue (irrespective of the qualification of an incident or the nature of the information to be exchanged) is the difficulty of determining applicable law (through rules of private international law) and of identifying competent law enforcement bodies/courts for any given incident. Since the focus of this study is on international information exchange, the main question is how applicable law and jurisdiction can be determined for incidents with cross-border aspects. In practice, it is not uncommon for multiple countries to claim jurisdiction in such cases (e.g. incidents where a criminal from country A victimises a person in country B using equipment situated in countries C, D and E). This represents a challenge to CERTs as well, since it may be difficult or even impossible for them to determine which country should claim competence and investigate, and thus who might reasonably be entitled to receive the relevant information. Under the application of the *ne bis in idem* principle (a criminal law application of the double jeopardy rule in common law systems), criminals cannot be convicted by multiple courts for the same offence; thus, in practical terms, only one country needs the information to initiate proceedings.

As an example, one might consider a fraud case initiated through a false identity profile on a social networking website, in which a CERT has obtained the IP addresses of the suspect (as assigned by his ISP) from the social network operator. It is perfectly possible for the suspect and victim to have different nationalities or residences, and for the ISP and the social network to be established in other countries (all of which may be different from the country in which the CERT operates). Law enforcement bodies from each of the countries involved could then contact the CERT to obtain this information, as they all have at least some basis for claiming jurisdiction under the rules of the aforementioned Framework Decision on attacks against information systems, as will be discussed further below. For a CERT, it will be practically impossible to determine in advance which law enforcement body (if any) will ultimately pursue a criminal case, and which body should thus get access to the information.

In practical terms, once prosecutors or investigators have decided that an incident is covered by their national laws and that they will act on the incident by requesting data from a CERT, the CERT will have little alternative but to respond to these requests, even if they would receive multiple requests from prosecutors or investigators in several countries. Formally, a CERT is not under any strict obligation to respond to information requests from other countries if it is not subject to the laws of the country of the law enforcement body (since the law enforcement body has no way to exert competence over the CERT). However, not responding could still be legally risky for a CERT: it could be sued (criminally or civilly) in the law enforcement body's country for refusing to assist in a crime investigation; or it could even be sued in its own country (again, criminally or civilly) if the refusal would be a violation of national laws. Thus, a refusal to comply with information requests from law enforcement bodies in other countries may in principle lead to the CERT's liability.

To some extent, this problem has been addressed through specific policy initiatives in the European Union. Similarly to the Convention on Cybercrime, the Framework Decision on Attacks against Information Systems 2005/222/JHA contains an explicit rule (Article 10) determining jurisdiction for incidents covered by the Decision, including rules for resolving any conflicts that occur when multiple Member States can claim jurisdiction. However, the rule is relatively vague and depends on good faith cooperation between the Member States: in case of conflicts, the Member States involved are to 'cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State'. While a few factors are provided to guide these discussions (notably the territory where the incident has occurred, the nationality of the perpetrator, and the location where (s)he was found), none of these is binding.

Thus, a margin of appreciation and negotiation exists, which is in line with broader jurisdictional principles established under EU criminal cooperation rules.[37] This provides a certain degree of flexibility to the Member States and to prosecuting bodies. However, this flexibility comes at the expense of legal predictability, which may hamper the efforts of CERTs, as they will generally not be able to determine with certainty whether their efforts will be able to result in prosecutions under their own national laws, and (more importantly) what the value of their efforts will be if cases will ultimately be brought before a court outside their own jurisdiction.

3.3.8 Mandate and competences of the CERT

As has been frequently noted, a recurring question is the issue of limitations to national or governmental CERT mandates. Not all CERTs will have a mandate to intervene in any type of computer emergency. This may result from their operating rules and frameworks depending on the legal basis of their formation (e.g. as independent entities or as part of an interior or economic affairs ministry). Their activities may be restricted to specific networks, specific geographies, specific companies or sectors, or specific types of incidents. Overstepping their bounds by exchanging information with a third party unrelated to their remit may result in evidence being tainted and/or the CERT risking its liability. The specific aspects of how the mandate and competencies of national/governmental CERTs may affect cross-border information exchange are detailed below.

We now turn to the specific considerations and implications for CERTs of different legal factors associated with cross-border information exchange.

3.4 Overarching factors relevant for CERTs

In this section we present evidence concerning some overall factors or concerns which bear upon the different legal and regulatory aspects that may become apparent. These concerns include the legal basis of the CERT to act and the experience and governance of information exchange.

[37] See notably Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/jl0021_en.htm [accessed 22 August 2011]

3.4.1 The legal basis of the CERT to act

The primary legal concern of a CERT is its mandate to act; in other words under whose authority and with what scope it should operate.[38] As this study has the main focus on national/governmental CERTs, it raises a question about the extent to which national/governmental CERTs can influence the resolution of issues relating to matters outside their jurisdiction.

Chisholm-Smith (2006) also notes that there may be a failure of duty to act if the CERT did not do something to address or alleviate a problem detected upon its networks. This might be especially pertinent with regard to the case of national/government CERTs that have a particular national security remit.

ENISA (2006c) identified the four most common legal bases for CERTs, motivated by involvement of funds, fulfilling legal requirements or for the exchange of sensitive data. These are:

1. Non Disclosure Agreement (NDA) – a legal contract between two parties which outlines confidential materials or knowledge the parties wish to share with one another but wish to restrict from general use;
2. Memorandum of Understanding (MoU) – a legal document describing a bilateral agreement between two parties expressing a convergence of will. Lacking the binding power of a contract, a MoU is a more formal alternative to a 'gentleman's agreement';
3. Contract (common in Managed Security Service Providers) – a promise or agreement, breach of which is recognised by the law and for which there are legal remedies. Legally, performance of a contract is considered as a duty;
4. Terms of Reference – a document describing the purpose and structure of a specific project (for example, to establish a CERT).

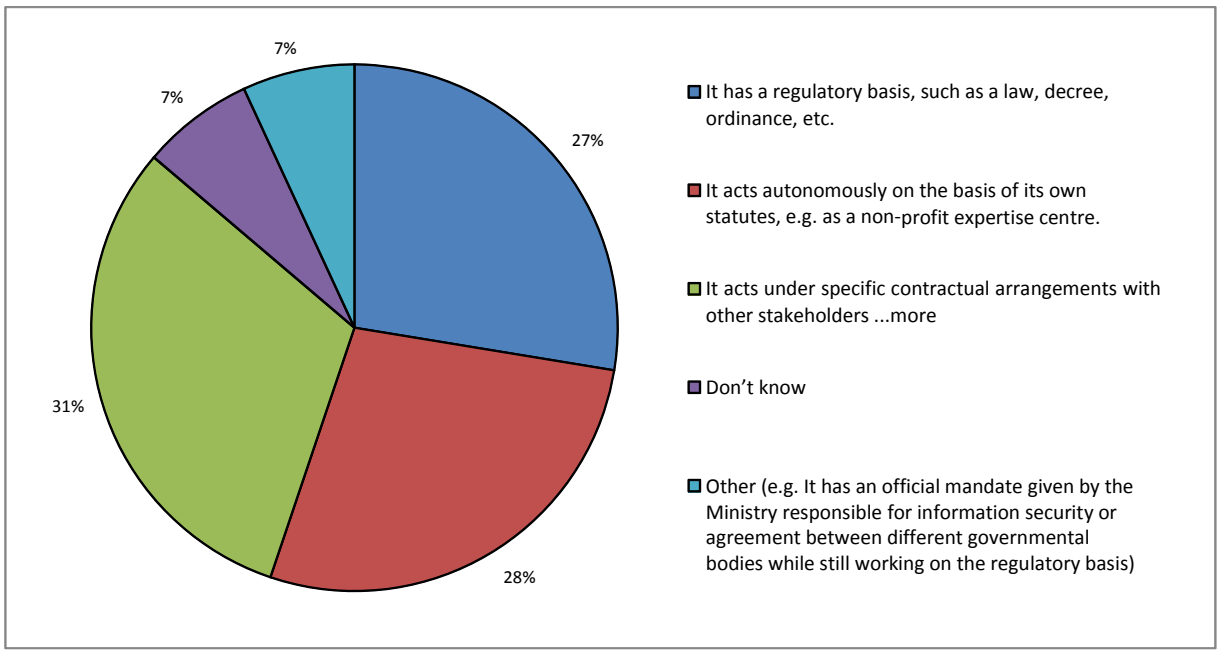
Evidence from an interviewee also indicated that sometimes certain activities associated with the work of national/governmental CERTs may be delegated to other CERTs.[39]

[38] Anonymous interviewees: 04/05/2011 and 11/07/2011

[39] Anonymous interviewee 11/05/2011

Figure 3 indicates that most of the respondents had some kind of solid basis (such as regulatory, own statutes or specific contractual arrangements).

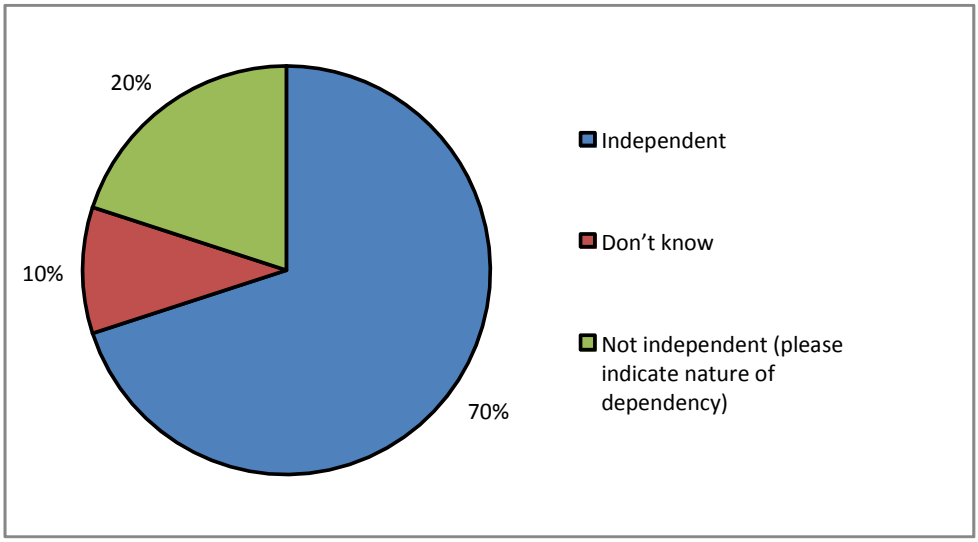
Figure 3: Established basis of CERTs



Source: RAND Europe and time.lex questionnaire (2011) n = 23

As Figure 4 indicates, of those participants responding, there is a high degree (70%) of autonomy with regard to incident response tasks; that is to say, they were independent of direction from another authority about what activities they performed.

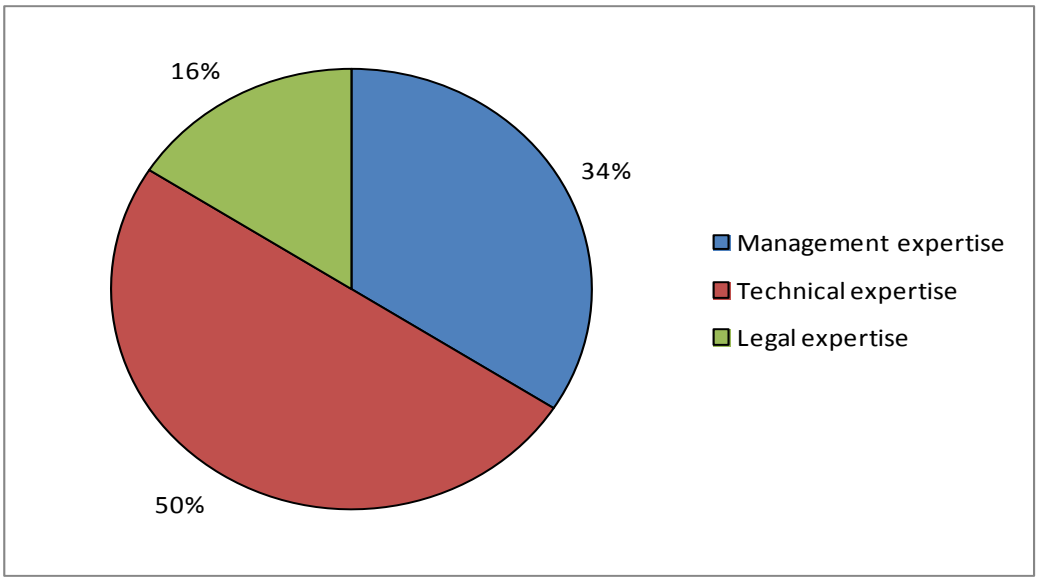
Figure 4: Autonomy of organisation when conducting incident response interventions



Source: RAND Europe and time.lex questionnaire (2011) n = 20

Within the teams, as Figure 5 illustrates, half of respondents indicated their team was composed of principally technical expertise. A minority (16%) reported having legal expertise within their team. Respondents were able to indicate they had more than one type of expertise.

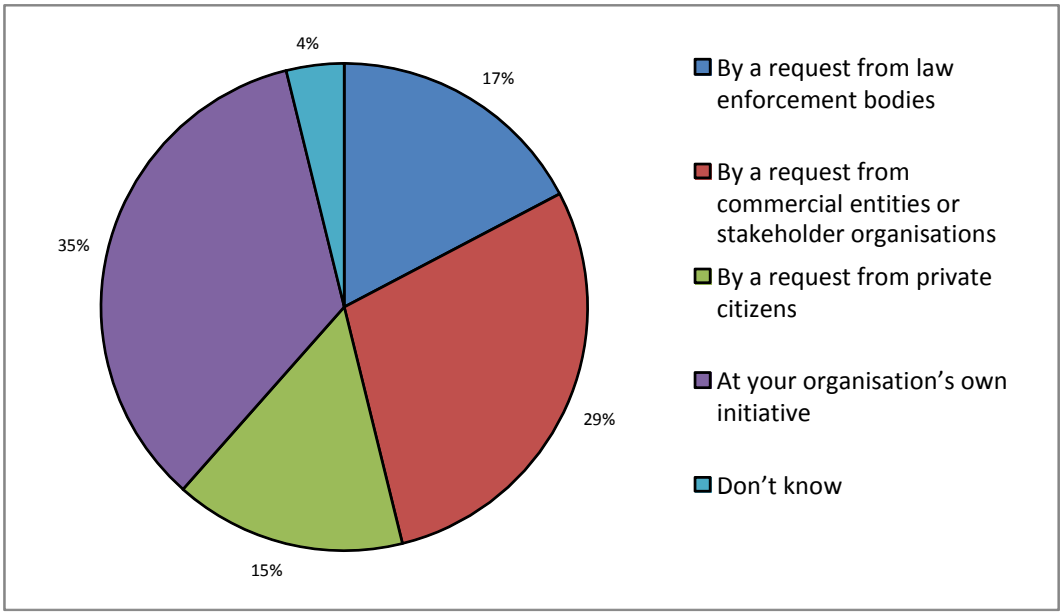
Figure 5: Composition of teams



Source: RAND Europe and time.lex questionnaire (2011) n = 23

The initiator of intervention stems from a range of sources including requests from other stakeholders, law enforcement or on the initiative of the team themselves. As can be seen in Figure 6, incident response generally comes at the behest of non-law enforcement stakeholders or on the organisation's own initiative.

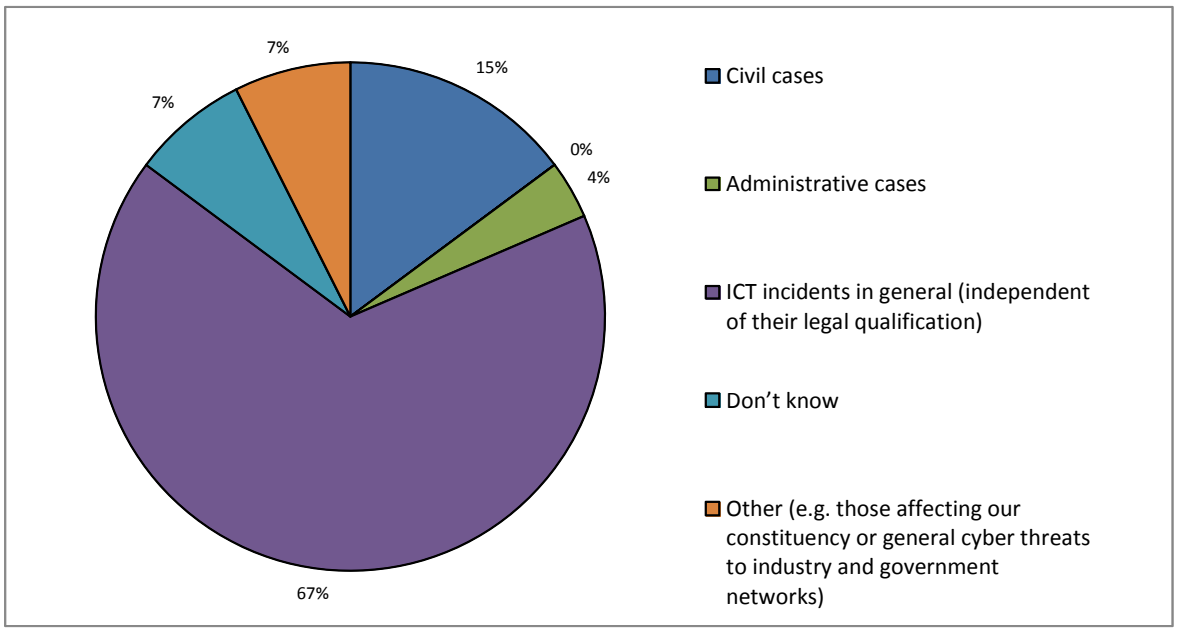
Figure 6: Sources of intervention



Source: RAND Europe and time.lex questionnaire (2011) n = 23

Moving to the types of incidents, respondents as shown in Figure 7 mainly (67%) indicated that they were involved with general ICT incidents, which perhaps reflects their 'security' role rather than crime investigation role (i.e. they were not able to make a determination whether an incident was criminal or civil in nature).

Figure 7: Types of incidents

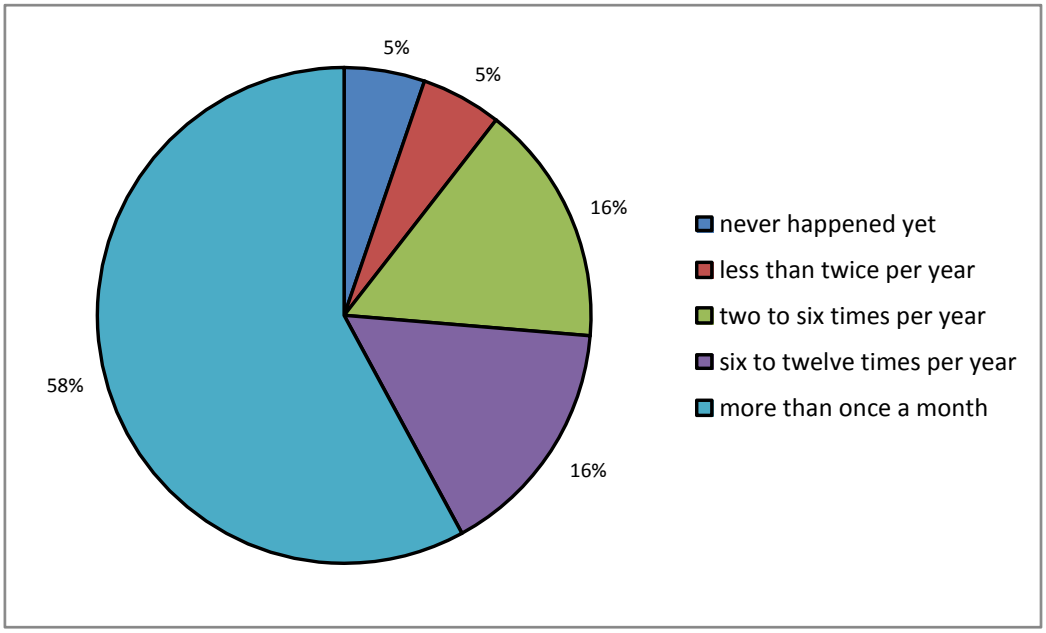


Source: RAND Europe and time.lex questionnaire (2011) n = 23

3.4.2 Experience of cross-border information exchange

Figure 8 indicates that the majority of respondents (58%) have been involved in some kind of cross-border information exchange, frequently on a very regular basis (more than once a month). Still, in 5% of CERTs no cross-border information exchange has ever occurred.

Figure 8: Experience of cross-border information exchange

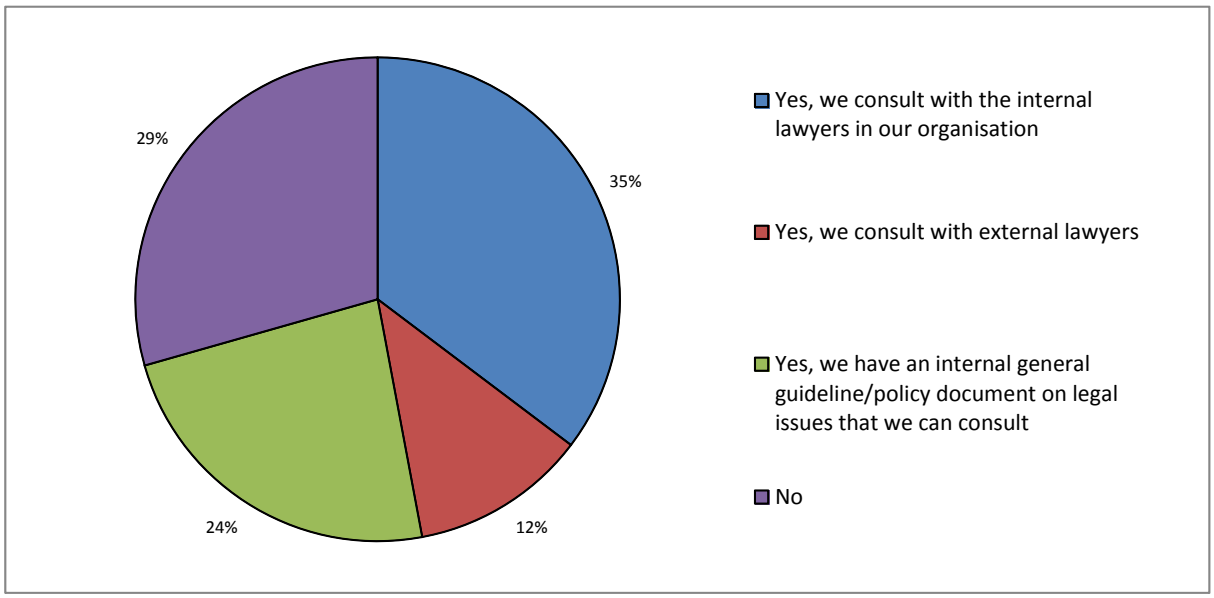


Source: RAND Europe and time.lex questionnaire (2011) n =23

3.4.3 Governance of information exchange in CERTs

Whether organisations are responding to requests for information exchange, seeking legal advice from lawyers external to the organisation is a minority practice amongst respondents (12%), as Figure 9 illustrates. More typically, they would seek advice from lawyers internal to the organisation (35%). Quite regularly, the respondents do not seek any legal advice (29%) or they consult guidelines (whether official or developed by the organisation) (24%). To some extent, this relatively low rate of legal consultation may relate to the fact that they are making repeated similar requests; in such cases, it is conceivable that legal advice is only sought for the first instance of a request, but not for later requests that are not substantially different.

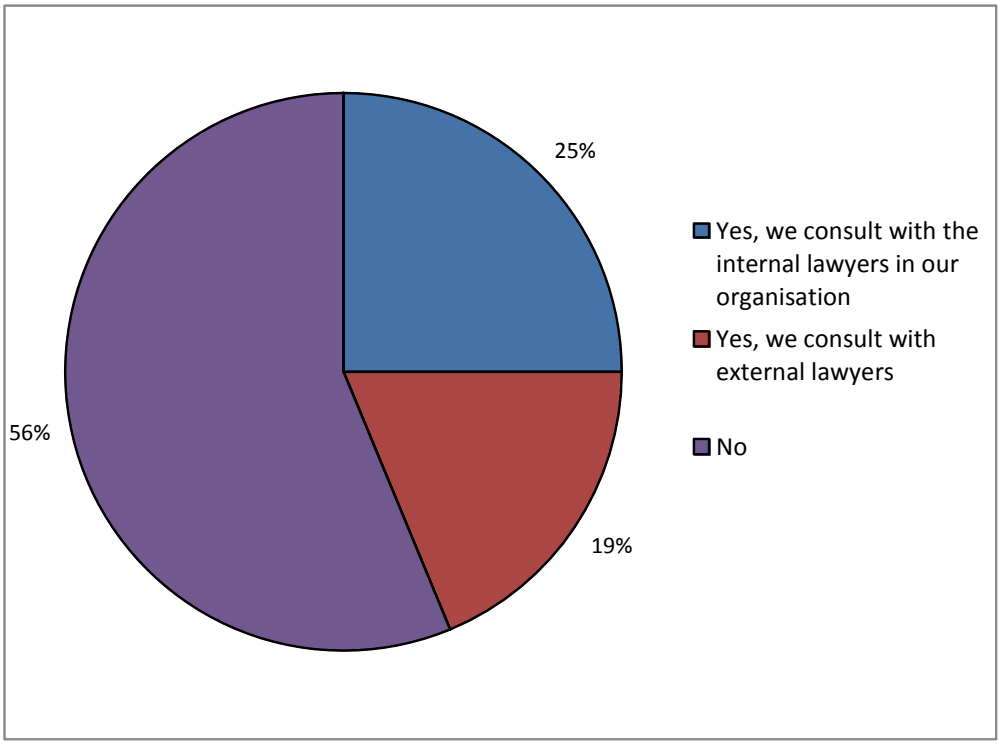
Figure 9: Use of advice or guidance when responding to information requests



Source: RAND Europe and time.lex questionnaire (2011) n = 16

While the situation is similar with regard to obtaining legal advice when issuing requests, as shown in Figure 10, respondents reported that legal advice is even less likely to be sought (56%). When it is sought, it is not through guidelines but mainly through lawyers internal (25%) or external (19%) to the organisation. No respondent indicated that they had an internal guideline or policy document on legal issues.

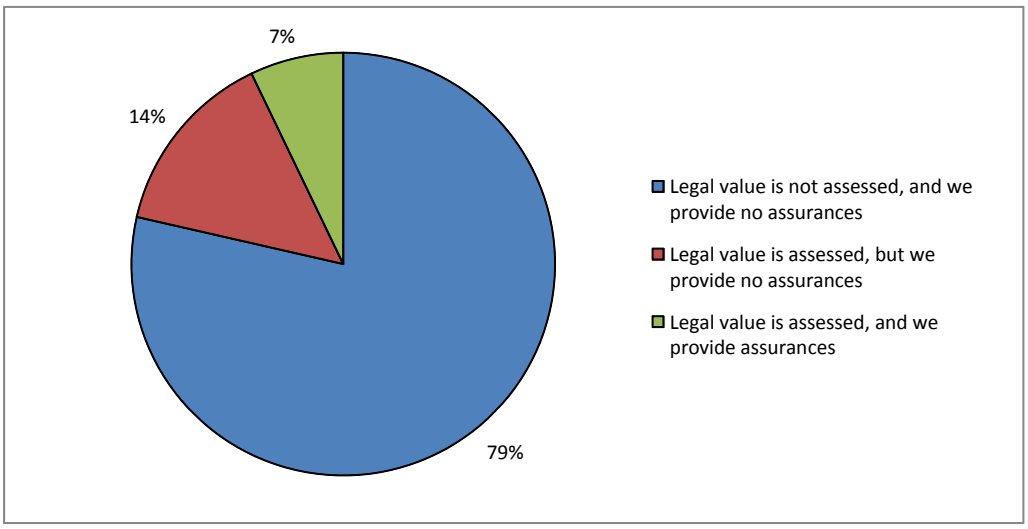
Figure 10: Legal advice when preparing requests



Source: RAND Europe and time.lex questionnaire (2011) n = 16

Even when legal advice is sought, as Figure 11 shows, the legal value of the information does not tend to be assessed (only 14% of respondents do when they are responding to requests), and is even more rarely supported by clear assurances (only 7% of respondents do).

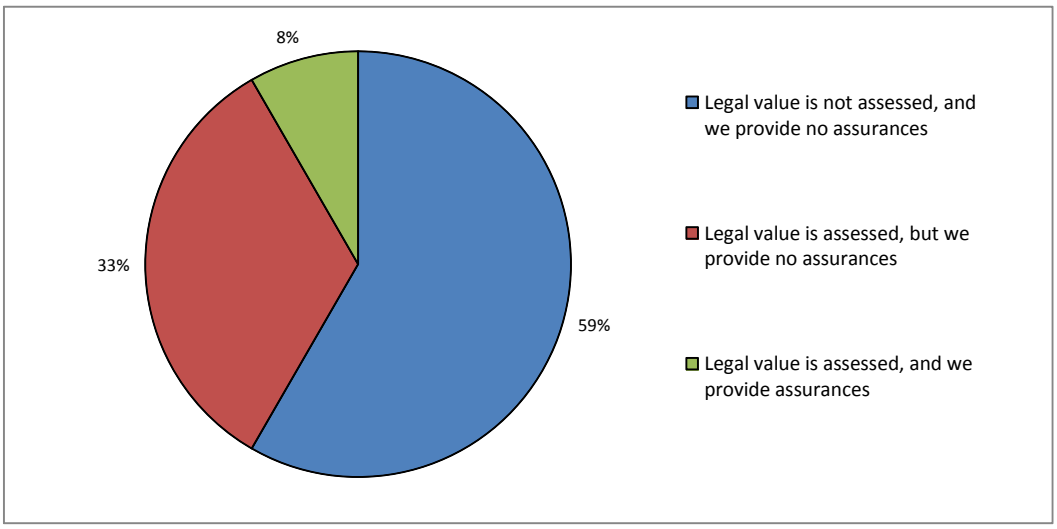
Figure 11: Assessment of legal value when responding to requests



Source: RAND Europe and time.lex questionnaire (2011) n = 16

Figure 12 shows that there was slightly more consideration given to the legal value when requests were prepared by the respondent's CERT. Here one-third of respondents indicated they undertook some form of assessment of the legal value, and a minority (8%) reported that they provide assurances.

Figure 12: Assessment of legal value when information requests are prepared



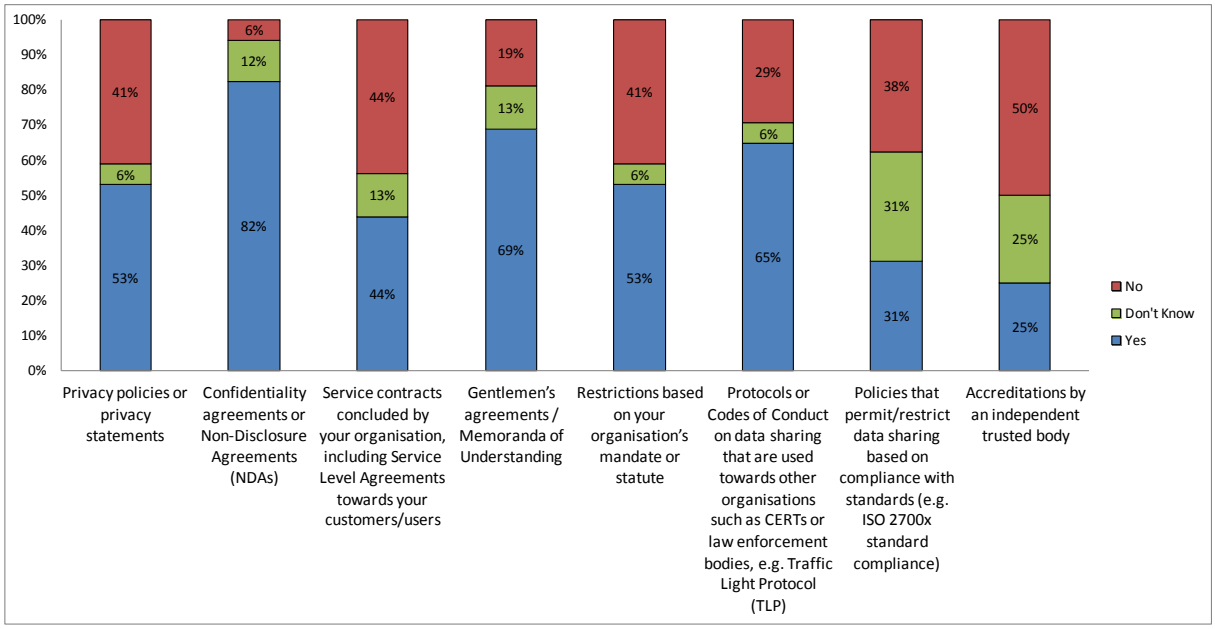
Source: RAND Europe and time.lex questionnaire (2011) n = 12

Trust was cited by a couple of respondents as being of primary importance to information sharing, implying that legal concerns are only secondary. This was supported by several of the KIIs, who noted the importance of face-to-face meetings such as TF-CSIRT to establish credibility and enhance trust. They also indicated a perception that the intervention of legal experts introduced a degree of friction in informal cooperation.

Concerns over untrustworthy peers gaining from disclosed information is borne out by evidence from elsewhere regarding the factors which may incite individuals or organisations to disclose breaches (e.g. Gal-Or and Ghose, 2004) and also the regulatory framework concerning the disclosure of breaches (e.g. Article 13a of the Revised Telecommunications Regulatory Framework 2009 and proposed inclusion of a similar breach notification requirement in the review of the European legal framework concerning privacy and data protection).

Figure 13 indicates the proportion of respondents indicating that they did, did not or did not know whether they used specific mechanisms to govern information exchange. As can be clearly seen, confidentiality agreements or non disclosure agreements are by far and away the most popular, followed by non-binding measures such as MoUs or the TLP (Stikvoort, 2009).

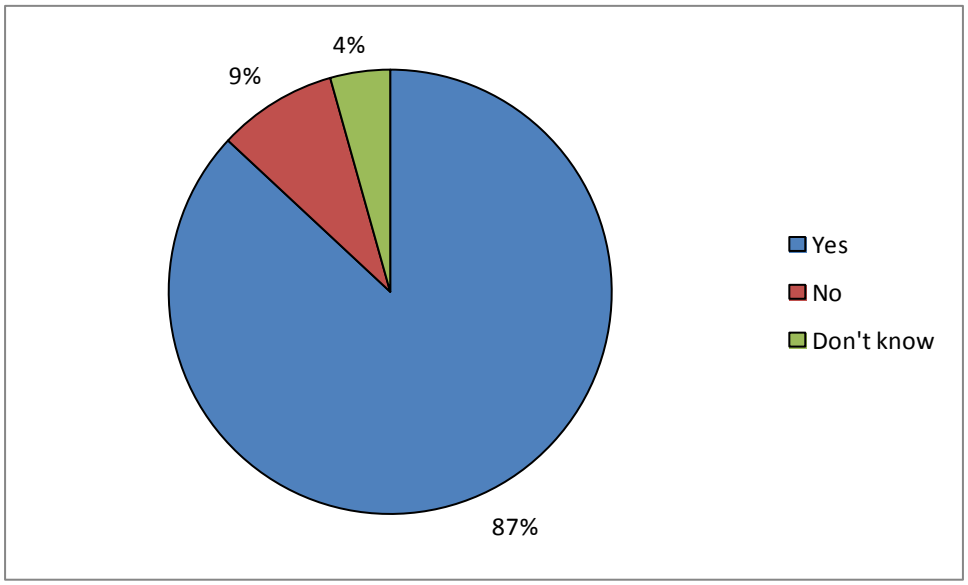
Figure 13: Mechanisms governing information exchange



Source: RAND Europe and time.lex questionnaire (2011) n = 18

Given the noted importance of international cooperation (Silicki and Maj, 2008) respondents were asked about their participation in various international initiatives or communities. Figure 14 indicates an overwhelming (87%) degree of participation in national and international networks such as EGC, TF-CSIRT and FIRST.

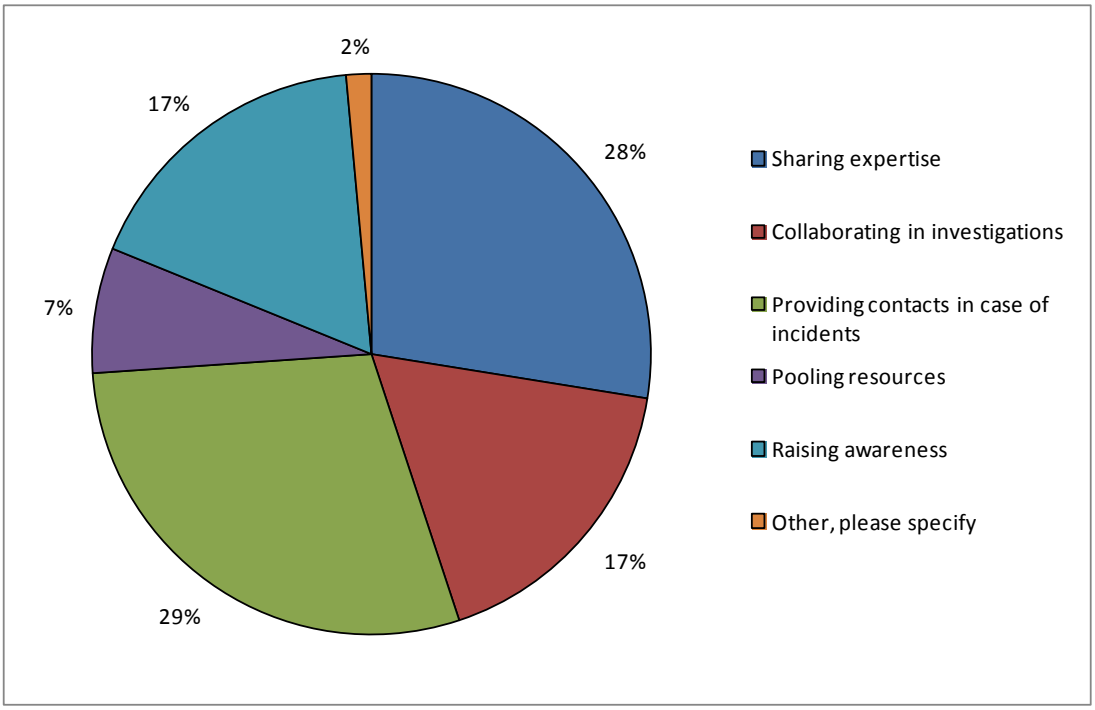
Figure 14: Participation in national or international networks



Source: RAND Europe and time.lex questionnaire (2011) n = 23

These networks were reported to have varying goals, as indicated in Figure 15.

Figure 15: Reported goals of national and international networks



Source: RAND Europe and time.lex questionnaire (2011) n = 23

3.5 Specific legal factors

There is a reported lack of familiarity with the indicated international harmonisation initiatives: fewer than a quarter of respondents ever expressed having some familiarity with specific initiatives regarded and listed of relevance in our questionnaire.

There is also a low awareness overall of the existing guidelines concerning legal factors associated with information sharing (ENISA 2010b), which is more or less evenly distributed across the various guidelines. Only around 15% of respondents report ever being aware of specific guidelines.

It is worth noting here that the questionnaire did not cover a number of national-level laws which respondents felt to be key to their field: data protection law (e.g. the Spanish LOPD (Data protection) Law[40] – which consider the IP as personal data, data breach notification law (e.g. the US Protected Critical Infrastructure Information (PCII)

[40] Organic Law 15/1999 of 13 December 1999 on the Protection of Personal Data (LOPD), (Ley Orgánica 15/99 de 13 de Diciembre 1999 de Protección de Datos de Carácter Personal (LOPD), Available from: http://www.boe.es/aeboe/consultas/bases_datos/doc.php?coleccion=iberlex&id=1999/23750 [accessed 22 August 2011]

Program[41] that protects certain information from Freedom of Information requests[42]) (DHS, 2011) and information security law (e.g. the German Act to Strengthen the Security of Federal Information Technology of 14 August 2009) (BSI, 2009)

Privacy and data protection legislation is regarded as the most important legal aspect concerning information sharing across the literature, interviews and online questionnaire. More specifically, the broad scope of the personal data concept causes real challenges in practice, as it can cover a large number of data types commonly collected and exchanged by CERTs (IP addresses, usernames/passwords, attack profiling, payment information, etc). The uneven interpretation of Article 29 Working Party guidance on IP addresses may also contribute to this perception (Graux, 2011). Other difficulties include the differences between laws in different countries, and the law profession's lack of understanding of IT and security incidents in particular.

For example, in the United States, Burnstein (2007) identifies that relevant legal provisions governing privacy of communications (the Stored Communications Act (USC, 2000)) may affect the sharing of network traffic data – necessary to provide researchers and network operators with 'much needed insight' to develop defences against highly distributed attacks (such as those perpetrated by botnets) against network infrastructure.

3.5.1 Knowledge of relevant national and international legal frameworks

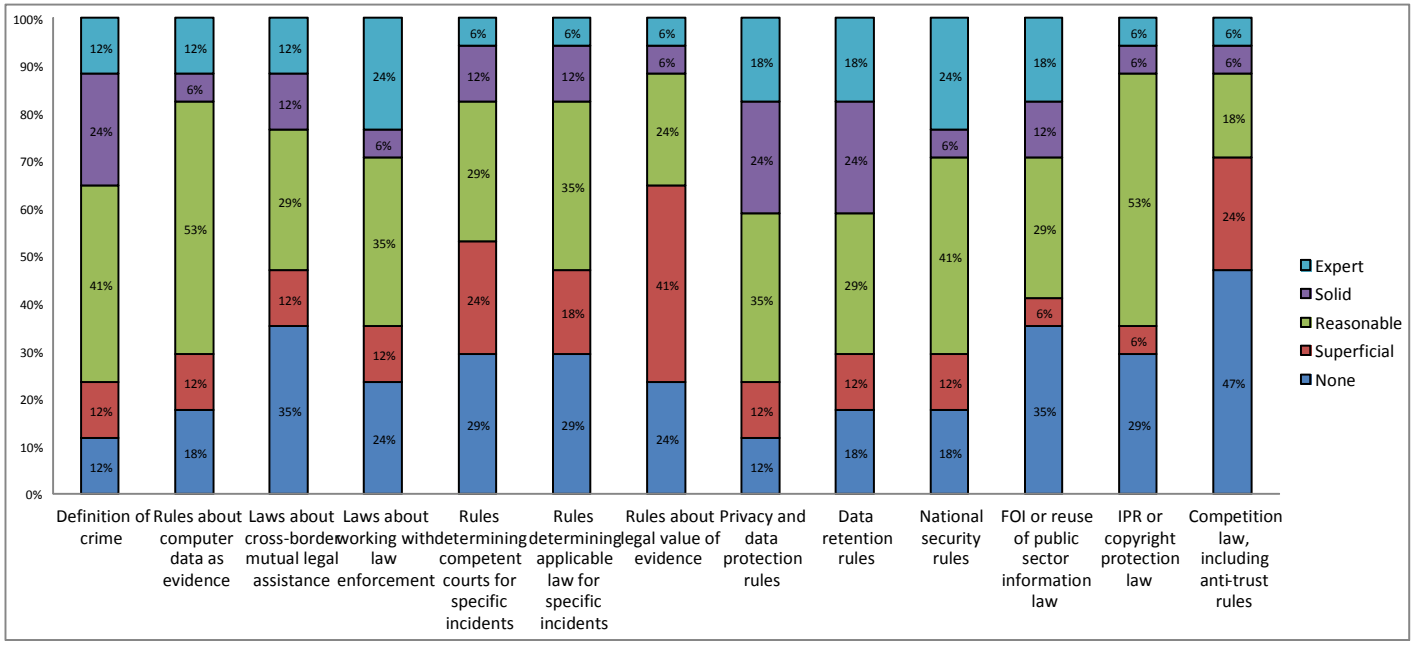
Respondents were asked to indicate their familiarity with national law regarding a number of different legal frameworks that were considered to play a role in CERT activities. As may be assumed, awareness of the definitions of computer misuse, legal obligations to work with law enforcement authorities; privacy rules; data retention rules and national security obligations ran high amongst respondents.

[41] Critical Infrastructure Information Act of 2002 Department of Homeland Security, USA. Available from: http://www.dhs.gov/xlibrary/assets/CII_Act.pdf [accessed 22 August 2011]

[42] Protected Critical Infrastructure Information (PCII) Program. Department of Homeland Security, USA. Available from: http://www.dhs.gov/files/programs/editorial_0404.shtm [accessed 22 August 2011]

Figure 16 indicates the respective degree of familiarity with relevant national law reported by respondents to the questionnaire.

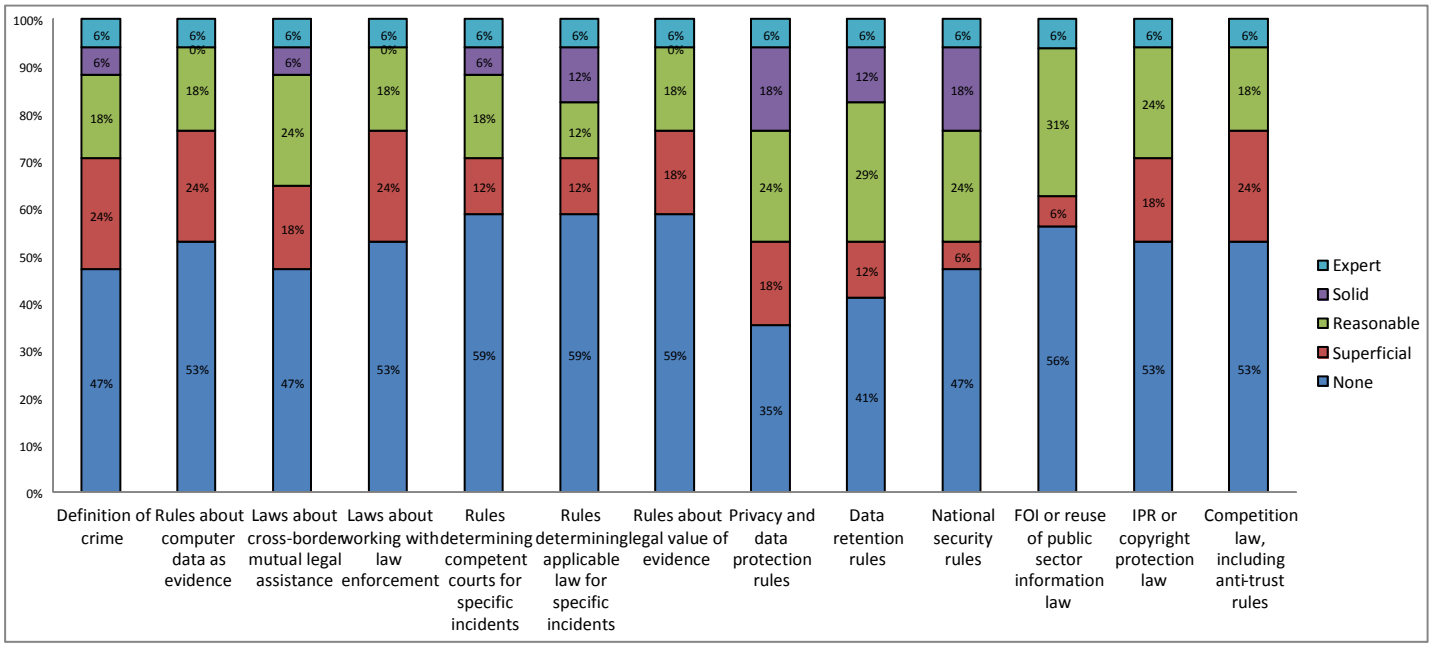
Figure 16: Familiarity with pertinent national laws



Source: RAND Europe and time.lex questionnaire (2011) n = 18

Respondents were also asked about familiarity with international harmonisation initiatives, across the same legal frameworks as shown in Figure 17. Examples include the Convention on Cybercrime and the legal framework governing privacy and data protection (including the Data Protection Directive, 95/46/EC). The purpose of this was to see the extent to which harmonisation (or lack thereof) played a role – if the level of awareness between national and international initiatives for the same legal domains was the same, this would suggest a high degree of harmonisation. As it turned out, there would appear to be more uncertainty concerning international harmonisation initiatives. Except for definitions of computer misuse, the legal framework governing privacy and data protection and data retention regimes, at least 50% of respondents indicated no familiarity with the remainder of international initiatives.

Figure 17: Familiarity with international harmonisation initiatives

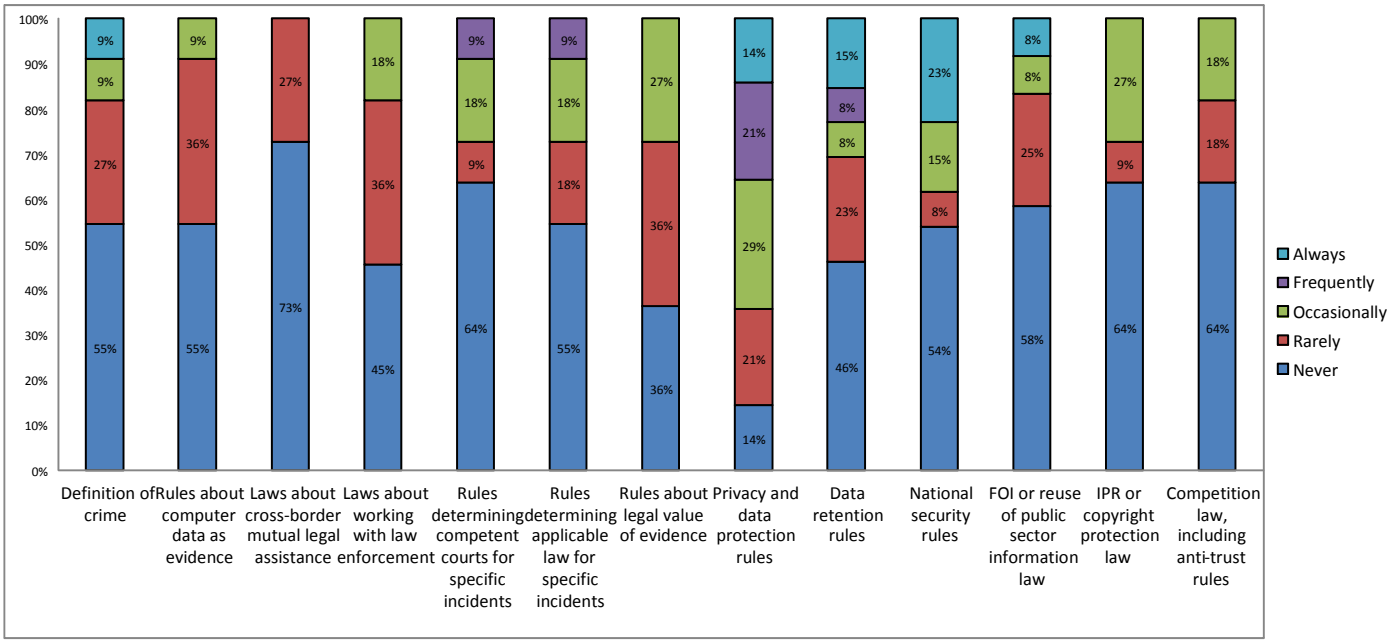


Source: RAND Europe and time.lex questionnaire (2011) n = 17

3.6 Transmitting and responding to information sharing requests

As can be seen from Figure 18, there are different legal frameworks that appear to be a concern when issuing requests to other peers. This gives a clear indication that privacy and data protection rules are more often than not cited by the respondents as a reason to decline requests for information. Furthermore, other legal frameworks pertinent to the activity of national/governmental CERTs (such as national security rules, or data retention, which governs serious and organised crime) are also more often than not cited as a reason to decline requests from peer CERTs.

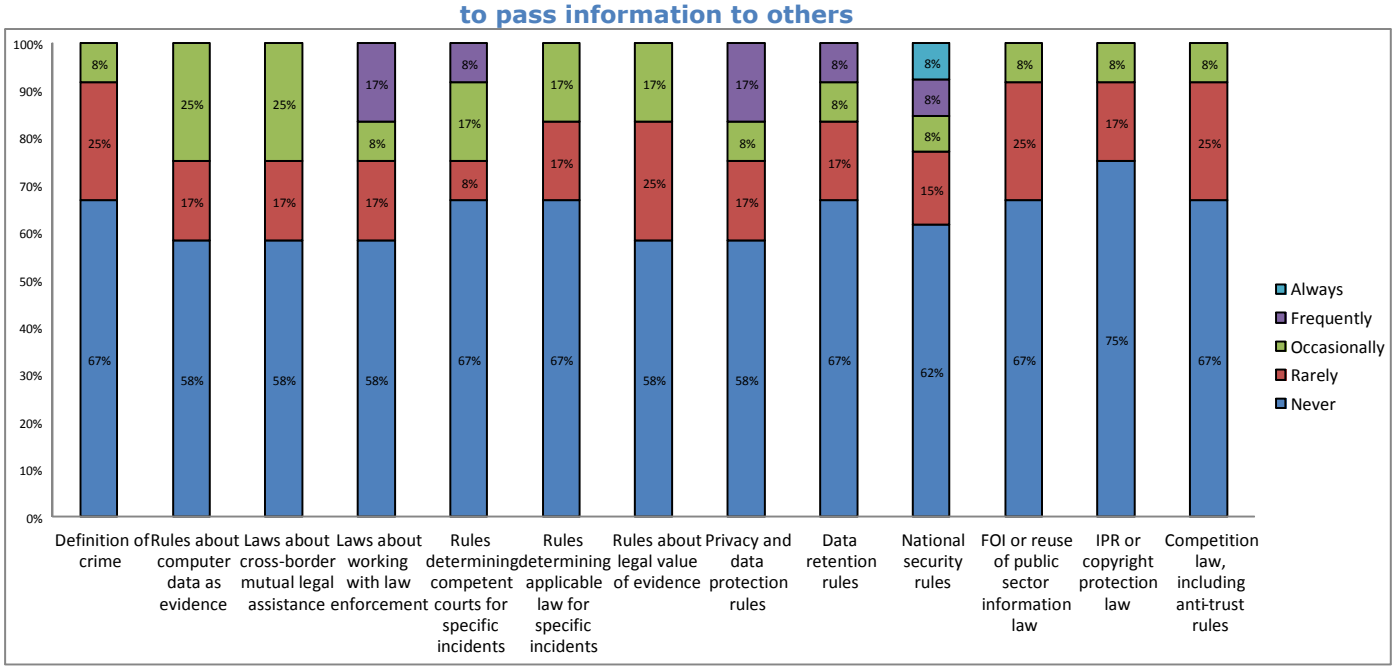
Figure 18: Prevalence of different legal frameworks cited as a factor when receiving requests from peers



Source: RAND Europe and time.lex questionnaire (2011) n = 14

We now turn to the question of those legal aspects cited when the organisation is preparing its own requests to send on to others. Figure 19 indicates that there was less inconsistency between different legal frameworks cited as reasons not to transmit information from the CERT (i.e. where the CERT had obtained or been given legal advice prior to the transmission of information to a peer). This finding in particular is important: it shows that in general, from the CERTs responding to this questionnaire, there is a difference in the extent of legal understanding prior to the onward transmission of data (otherwise this would be similar to the previous figure concerning the extent to which different legal frameworks are assigned as justification by peers). Although it may be seen that the preparation of a request is less risky from a legal perspective (since the originator of the request may not be held liable for simply asking) nonetheless, it may illustrate the potential for difficulties in the cross-border exchange of data.

Figure 19: Prevalence of different legal frameworks cited as a factor when preparing requests to pass information to others



Source: RAND Europe and time.lex questionnaire (2011) n = 13

As Figure 19 illustrates, there is more consistency about legal frameworks in the transmission of information to peers. This means that the different legal frameworks identified earlier as relevant are, more often than not, cited less as a barrier to preparing requests for peers. It is clear from this data that, when legal concerns are invoked, national security rules, rules regarding working with law enforcement and data protection considerations are by far the most important.

Nonetheless, both sides of the coin regarding cross-border information sharing (the transmission and response to requests) seem to converge on a few key legal factors, which are obvious when we consider the overall constituency and stakeholders for this study:

- Law enforcement
- National security
- Data protection & privacy
- Data retention regime.

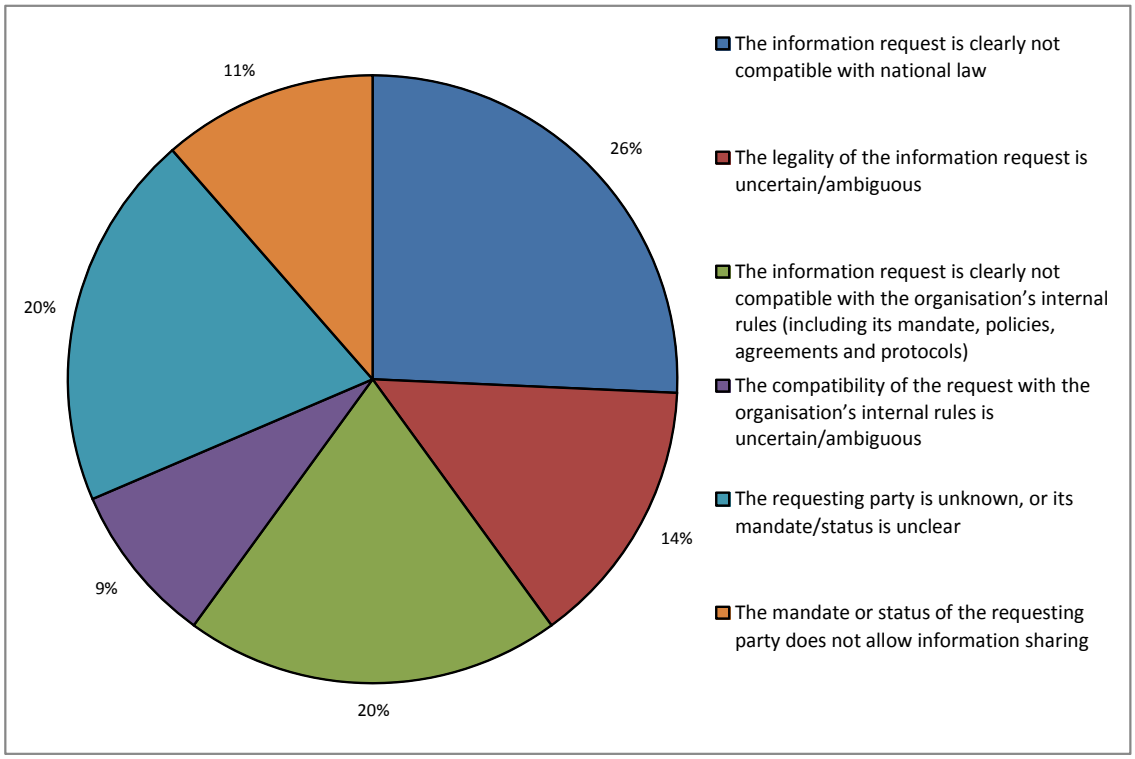
The asymmetry of findings between the two sets of responses to the questions above (Figure 18 and Figure 19) highlights some interesting further questions about the operational realities of information sharing. These data would appear to show that respondents considered their own organisation to be on the whole more flexible when it comes to complying with information requests, despite legal issues, than when they try to request information from their peers. There may be a number of possible interrelated reasons for this:

- Self-selection bias – respondents may have been representative of the most active and cooperative teams;

- Respondents may simply not have been aware of instances where their organisation had declined an information request. However, this may lead to a more serious implication since the majority of respondents were heads or team leaders, raising questions about the oversight of information exchange within a team;
- Cognitive – respondents were more likely to recall instances where they were denied information requests (since it prevented them from achieving certain goals) rather than when they had denied the transmission of an information request to other teams because of a perceived legal problem;
- Psychological / sociological – those working in CERTs naturally consider that they are the most flexible and adaptable team and others are always more reluctant to share, thus putting barriers in the way of the requesting team achieving its objective.
-

Figure 20 describes the reasons given for why the respondent's own organisation could not meet information requests. As can be seen, the question of compatibility with national law comes up as a significant factor. Less importantly, the legality of the information and the compatibility of the request with the organisation's own internal rules are also given as a justification for declining an information request from a third party.

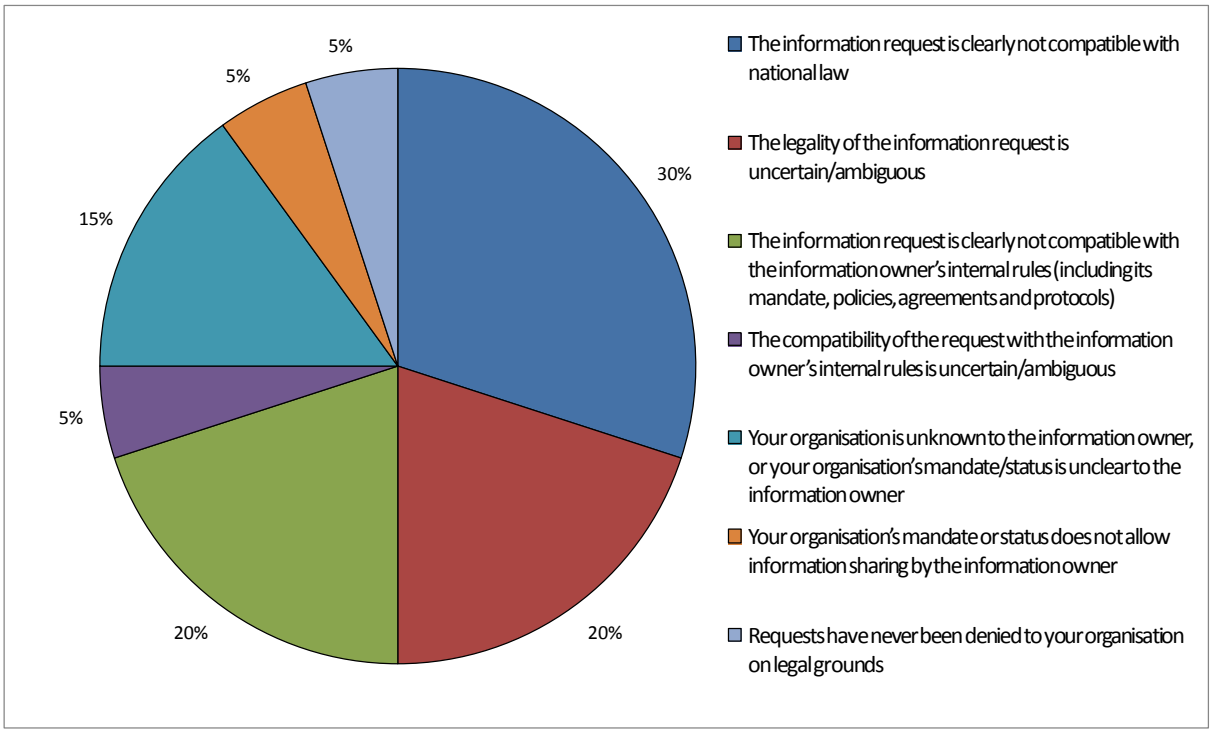
Figure 20: Justification given by the respondent's organisation to decline information requests from third parties



Source: RAND Europe and time.lex questionnaire (2011) n = 16

Turning to those instances where a request from the respondent's own organisation has been declined by a peer the picture is broadly similar, with a variety of reasons being provided. Compatibility with national laws accounts for around one-third of all respondent's perspectives, as shown by Figure 21.

Figure 21: Justification given to the respondent's organisation by a third party when declining an information request



Source: RAND Europe and time.lex questionnaire (2011) n = 13

Data from questions relating to reasons given and received by the respondents indicate that around three-quarters of responses concern just three reasons – incompatibility with national law, uncertain legality of information request and incompatibility with internal rules. It would appear worthwhile to consider how these justifications could be addressed or at least mitigated.

3.7 Conclusions

This chapter has provided evidence from the desktop research, interviews and online questionnaire about the different types of legal issues that may enable or prohibit cross-border information sharing between CERTs. The CERTs that responded to our online questionnaire had some experience of cross-border information requests, but had little legal expertise within teams. We have seen that CERTs report a focus on issues surrounding data protection and privacy law, data retention and laws and rules concerning working with law enforcement, commensurate with their specific status. We have also observed differences between the perception of legal issues being referenced as a reason not to provide information by peers, compared to the citation of such justification when the CERT itself is responding to requests from its peers.

Finally, we observed that compatibility of national legal frameworks was one of the major specific justifications given as to why certain data could not be shared.

However, it is important to note that with particular regard to the responses to our questionnaire, they are a very small, self-selecting sample of the entire relevant CERT community. Therefore, care must be taken in interpreting these results as categorically having broader applicability to the whole CERT community. Nonetheless, despite this the depth of the questionnaire has allowed us the opportunity to explore in detail some of these concerns amongst those participating. Noting these findings and associated caveats, we now turn to proposing recommendations that might help to address the concerns identified from the evidence derived at each phase of the study.

4. Recommendations

This chapter presents recommendations based on the data gathered from the desk research, key informant interviews and online questionnaire.

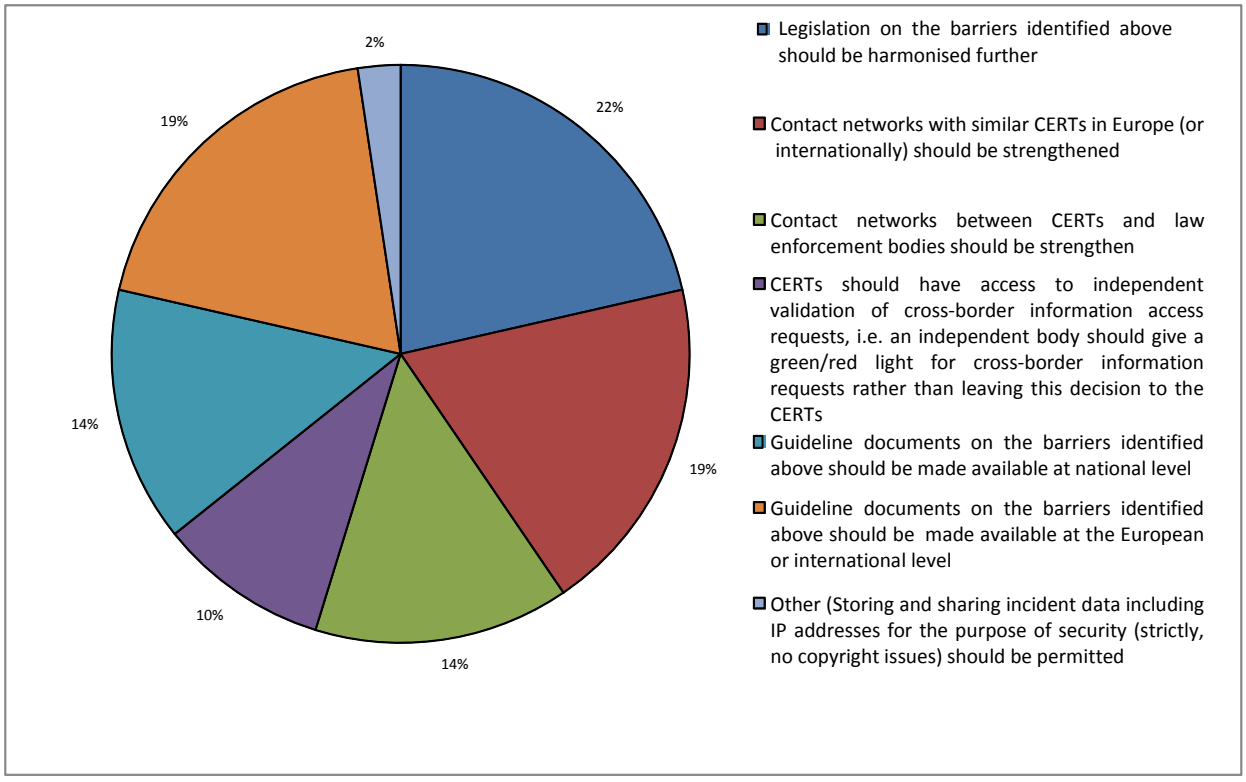
The relevant stakeholder through which the recommendation could be best addressed is also indicated by underlining.

4.1 Appetite for particular recommendations from respondents

Figure 22 presents data on the level of interest in some suggested recommendations proposed in the questionnaire (with respondents being allowed to endorse multiple recommendations). This question was asked in order to observe if and what clear preferences were exhibited by respondents concerning some generic approaches. In the end, no single option was suggested as a clear preference – something that might change given further observations from the community.

The parties responsible for the implementation of these recommendations vary: Member State governments and lawmakers, along with the EU-level policy-makers, have the mandate to address some recommendations. A role for ENISA and previously mentioned groups such as FIRST and TF-CSIRT may be foreseen in other areas; for example, supporting operational coordination and disseminating best practice.

Figure 22: Recommendations from respondents



Source: RAND Europe and time.lex questionnaire (2011) n = 17

4.2 Recommendations in detail

Based on the desk research, key informant interviews and responses to the online questionnaire, we identify the following recommendations around three themes (broadly in order from short- to longer-term):

1) direct support to operational aspects of cross-border incident response;
2) addressing the policy and legal issues; and
3) other recommendations; in particular via interaction with a much broader set of stakeholders (e.g. the research community).

Short-term refers to activities that can be conducted within a year whereas longer-term refers to activities requiring more coordination and political complexity and thus within a longer time span.

Operational recommendations

In the short term, there are three recommendations we envisage concerning improving implementation and operational coordination.

A.1 Establish direct approaches to support cooperation between CERTs A practical way to address the legal uncertainty, as well as a potential gap regarding the provision of legal advice in the CERT (not every CERT has access to its own in-house legal counsel) would be via the establishment of a centralised 'legal hotline' or some other kind of 'one stop shop' service available to CERTs, to answer questions or provide limited advice on the applicability and aspects of those relevant frameworks identified above. An example may be found with the European Judicial Network (EJN), which is hosted by Eurojust. Currently, the EJN provides such a function in respect of public prosecutors throughout Europe across a variety of criminal justice domains. Such a hotline or one stop shop would not replace specific legal advice but might serve as a useful aid to formulating an efficient response. Nonetheless, there would be practical challenges since such a facility would cost money to set up and would no doubt require the collection of data or linking of information requests (concerning legal uncertainty) from the CERT to sources of expertise (either online or, more definitively, to in-country human experts). The Global Prosecutors of e-Crime Network (GPEN) might be one such resource to tap into in this regard (GPEN, 2011). Progressing or hosting such a facility might be a useful role for ENISA. Member States might also support such platforms through greater cooperation with Data Protection Authorities and Privacy Commissioners. Whilst by no means authoritative legal advice, further effort from ENISA and Member States might be useful in generating flexible but concise checklists of legal questions each team could ask, in regard to those legal frameworks considered to appear most often in cross-border information exchange. An example regarding data protection and privacy is provided in Appendix A: Example legal checklist for privacy and data protection.

A.2 Disseminate Declared Level of Service templates The online questionnaire as well as sources from the desk research (Silicki and Maj, 2008) illustrates that strict SLAs could be too burdensome a measure to enable CERT cooperation. Formulating non-binding 'Declared Level of Service' templates for CERTs might be a more suitable alternative, representing a best effort set of measures which the CERT would try to achieve. SLAs might have an adverse effect due to the possibility of legal action following non-compliance, which might chill information exchange. IETF RFC 2350 (Brownlee and Guttman, 1998) already covers much of this but consideration might be given to expanding it to include criteria specific to cross-border information sharing concerns,

such as estimated response time for cross-border information requests and pertinent aspects of the relevant legal frameworks that the CERT operates under. Such templates might be prepared and disseminated by Member States and national/governmental CERTs. Declared Level of Service templates could be a useful alternative because they would help to set expectations between CERTs; for example, what pertinent legal frameworks or conditions the CERT is obligated to operate under. In addition, these documents could conceivably be aligned with relevant clauses from the existing Model Contracts for the transfer of personal data to third countries.[43] This would have the added benefit of facilitating compliance with data protection regulations, including at the international level (i.e. for exchanges to/from entities outside the EU), where these Model Contracts are one of the crucial instruments for enabling exchanges of personal data to countries that do not have equivalent data protection laws.

A.3 Investigative measures to encourage cross-border information exchange

This recommendation concerns exploring possibilities of different tools to further strengthen sharing. We identify three examples: a) organisational models of sanitised sharing b) non-binding confidentiality charters and c) national-level legal frameworks to limit liability.

> a) Reference to models of sanitised infomation sharing might be useful to identify other policy domains where information sharing is also characterised by this problem to see what solutions have been used. For example, in the intelligence community, 'tear-line' or 'tear-sheets' have been a creative solution deployed by the US military to permit the sharing of intelligence information to coalition partners (Willis et al, 2009). Documents are literally 'torn in half' and the information (but not source) is passed on. Although there are clear differences in how this model might be applied to cyber security (since very often the 'source' – e.g. an IP address – is intrinsic to the intelligence that would need to be shared), perhaps this points to a more graduated possibility of information sharing, which would minimise the data protection impact and therefore more easily comply with European legal requirements in this respect. Member States and ENISA could work together to develop criteria to identify what could and could not be 'torn-off'.
> b) Another such organisational model might be a confidentiality charter such as the example published by the UK's (now defunct) National High Tech Crime Unit (NHTCU)[44] used to stimulate cooperation between law enforcement and the private sector. Given the wide variety of sources of input a CERT may rely upon, such a charter would be a useful tool in creating a common expectation amongst the different types of CERTs, within a national jurisdiction, that might be stakeholders. This would be particularly pertinent with regard to the private sector, which, as has been illustrated in other areas, may be reticient to participate for perceived fear of liability (ENISA, 2010b). Member States might suggest such models which ENISA could collate and share as examples of best practice.

---

[43] See http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm [accessed 22 August 2011]

[44] See: http://www.sourceuk.net/article/2/2476/confidentiality_charter__the_nhtcu_working_with_business.html [accessed August 22 2011]

c) As has been shown, there is a perception from the limited evidence that measures to limit liability (for subsequent regulatory enforcement action that may be taken on the basis of information provided) may help both those organisations that may supply information to CERTs and CERTs themselves. For example, an ISP may not be willing to share certain data due to a perception that it would be in breach of its licence obligations or security and integrity requirements under Article 13a of the Revised Telecom Regulatory Framework 2009. This model might also be applied at the CERT level. Anecdotal evidence from reviews of the handling of Code Red/Nimda suggests that applying certain disclaimers or caveats on material (prior to transmission) regarding applicability of Freedom of Information / Public Sector re-use of Information obligations could provide greater clarity (since it would make it clearer under what circumstances the receiving party could act on such data). However, it should be recognised that CERTs (or other information providers) cannot mitigate their liability autonomously by adding disclaimers to their communications if this would run contrary to national liability rules. An example of a possible approach can be found in the Danish June 2011 Act on Processing of Personal Data when Operating the Governmental Warning Service for Internet Threats (Folketinget, 1/6/2011).[45] As the name suggests, this Act provides a clear legal framework for the processing of personal data by the Danish GovCERT and the permissible conditions for the processing of such data. It also specifies the Danish GovCERT's mandate and competences. In this way, the lawfulness of its activities can be more easily assessed by measuring its activities against a set of clear legal requirements which allows the CERT to avoid actions that might result in liability. Further discussion on the applicability of limitations of liability with respect to information sharing can be found in ENISA (2011). Regulatory intervention is likely to be required to clarify this point. This recommendation would therefore need to be taken forward by the Member States and the European Commission.

Policy recommendations

Over the medium to longer term, more extensive recommendations concern policy intervention on the legal framework for CERT activities.

B.1 Address legal uncertainty concerning requests Regarding the finding concerning the reasons for most justifications for denial of both transmitted and received information requests
Figure 20) (namely the uncertain legality of information request) – further clarification of the differences between relevant national laws could help. This might decrease the complexities of international collaboration. Specifically with regard to data protection law, it would appear from the interviews and the evidence from the online questionnaire that the concern here is less about what the legislation does and does not say, but rather about uncertainty and uneven or different interpretations as a result of ambiguities and margins of national appreciation left by European regulations. Providing there is a clear, consistent interpretation then CERTs could recognise a 'level playing field' and devise common rules and approaches. This falls to the Member States and the European

[45] See the unofficial English translation at https://www.govcert.dk/gcdata/uk_version_l197.pdf [accessed 22 August 2011]

Commission, and additionally with respect to data protection and privacy law, to other players (e.g. the European Data Protection Supervisor and the Article 29 Working Party).

B.2 Designate national/governmental CERTs on a specific regulatory footing (alongside other Member State-level bodies charged with implementing national security-related objectives) represents a broader recommendation aimed at the Member States and European Commission with the support of ENISA. This recommendation stems from consideration of a broader issue that this study of the legal and regulatory aspects has revealed – the uncertain mandate of national/governmental CERTs, especially when contrasted with CERTs that operate as private entities without a public sector mandate. Although the meaning definition of national or governmental CERTs has been identified and described, at least informally (ENISA, 2009b, 2010a), the legal confusion arises from uncertainty about which legal framework concerning data protection would apply, as this is strongly dependent on the status and mandate of the CERT. Either Directive on Data Protection 95/46/EC would apply (with respect to private CERTs that lack any formal mandate), or specific legal frameworks concerning national security-related matters would apply for governmental or national CERTs (e.g. in the former third pillar as illustrated by the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters). If the operations of a national/governmental CERT were taking place according to a specific legal basis then it would permit a clearer evaluation of competing legal frameworks. From a simplistic perspective, what would need to be indicated is whether or not a CERT is operating as a 'national or governmental CERT' as defined by the relevant EU law or instrument. The revision of the ECI Directive would provide just such an opportunity to progress this recommendation, for example by providing the framework to designate national/governmental CERTs and potentially to streamline their competences.

The creation of such a well-defined community would also support the trusted sharing of information, as shown by Goode and Lacey (2005), who indicate that based on ancedotal evidence from a case study of a large telecommunications provider in the Asia Pacific region, social embeddedness plays a role in supporting information sharing; if an organisation can control which groups it shares information with, then it is more inclined to share information. Nonetheless, although such a framework would bring greater clarity to the numerous issues that arise between national/governmental CERTs meeting their security objectives and the relevant legal frameworks, care must be taken not to create more bureaucratic overheads for participants in preparing and managing their role as a 'national/governmental CERT'.

However, it should be recognised that this approach does not resolve any challenges resulting from the distinction between such national/governmental CERTs and other types of CERTs. As discussed in earlier sections, an example of such a challenge relates to data protection compliance: national/governmental CERTs can more easily justify the processing of personal data under the national implementation of Article 7 (e) of the Data Protection Directive, which allows processing of personal data if this 'is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed'. Obviously, this option is not readily available to private CERTs without such a mandate. Indeed, the establishment of a specific regulatory footing as recommended here would make it easier to make this distinction, which could result in the differences in competences being more easily recognisable, thus making communications with private

CERTs harder in cases where communication would not be compliant with existing laws (including data protection laws). However, this is an inherent consequence of the policy choice of entrusting certain investigative competences only to entities with a specific mandate: national/governmental CERTs generally have more far-reaching competences because their activities are a legal extension of national sovereignty (e.g. the legal right to impinge on privacy for the purpose of supporting law enforcement activities). This right is not available to private entities without an official mandate, irrespective of the reality that their activities and goals may not be so different from those of national/governmental CERTs. To mitigate this distinction between two groups of CERTs, wide-reaching regulatory reform would be needed to increase the flexibility of any regulations with respect to the competences of private entities to conduct incident investigations. Such wider-reaching regulatory reform might become a reality as a part of the revision of the Data Protection Directive 95/46/EC, linked to the disappearance of the former pillar policy distinction, which could give rise to a more harmonised data protection regime that could apply to all CERTs. This could facilitate the exchange of personal data between CERTs at the cross-border European level, by specifying more clearly under which circumstances CERTs may legitimately process personal data (including by exchanging it), and what their corresponding obligations are.

B.3 Ensure EU-level legislation takes account of scope of national/governmental CERTs A further possible improvement would be to assign explicit recognition for the requirements for national/governmental CERTs to process personal data that might conflict with requirements of the legal framework governing privacy and data protection. Given that national/governmental CERTs are intended to address incidents of national, European or regional importance, such recognition would need to be based on justification of national security (or at least serious and organised crime) perhaps via reference to the proposed Framework Directive on Attacks Against Information Systems (COM (2010) 516). In this way, it would be possible to specify that in those cases of national, regional or European-level incident response which require the sharing of personal data between national/governmental CERTs, a specific set of legal considerations concerning personal data would apply (as was the case in criminal justice instruments with the former third pillar of EU policy). It would also need to include a reaffirmation of the high-level contact group principles (Wright et al, 2011) concerning the use of personal data in the fight against international terrorism and serious and organised crime:

1. Purpose specification of limitation
2. Integrity and data quality
3. Proportionality
4. Information security
5. Special categories of personal information
6. Accountability
7. Independent and effective oversight
8. Individual access and rectification
9. Transparency and notice
10. Redress – debated scope
11. Automated individual decisions
12. Restrictions on onward transfers to third countries

Action on this improvement would need to be very rapid, however, as a proposed new strategic European legal framework regarding privacy and data protection is already

mature. This recommendation would require joint action from a number of EU policy-makers and Member States.

B.4 Specify threshold for incidents requiring national/governmental CERT response & sharing The question of legal uncertainty would also be aided by clearer legal specification of exactly what level of magnitude of incidents national/governmental CERTs should be dealing with. This might be facilitated by progressing understanding of what type and scale of incidents ought to justify a response by a national/governmental CERT (for example, specific types of incidents which have the potential for national or EU-wide impacts). This might be implemented via appropriate stakeholders exchanging information. Allied to the recommendation above, a clearer specification of the types of incidents that national/governmental CERTs are empowered to address, manage and respond to (implying sharing of data) would help in clarifying parameters for subsequent discussion on what the relevant legal frameworks are, and just what can and cannot be done under those frameworks. This recommendation would also need to be taken forward by the Member States, the European Commission and ENISA.

B.5 Articulate why CERTs need to process personal data to Article 29 Working Party Following on from this, another suggested measure would be via representation to the Article 29 Working Party outlining the obligations and security-related objectives of CERTs and how the existing uncertainty concerning the European legal framework regarding privacy and data protection presents challenges for them to collaborate effectively (specifically through the trusted and proportional exchange of personal data). The European Commission would be best placed to take forward this recommendation with the Article 29 Working Party, possibly by seeking an opinion from the Article 29 Working Party on the conditions for legitimacy of data exchange activities with respect to cross-border information exchange. ENISA may be able to lend its support as appropriate.

Longer-term recommendations

Finally, three long-term recommendations concern research initiatives or projects:

C.1 Incorporate information on the legal basis for an information request Measures to provide clarity regarding the legal basis for an information request (and its originator) may help to increase cooperation by creating more transparency about why information may not be shared. This might build upon and tie into a number of initiatives to establish common message structures or formats for incident response and information exchange. An example might be a field in the request form to allow the inclusion of information pertaining to the relevant law providing the conditions for the sharing of such data (such as: 'pursuant to Article x of Law y, this information request is being sent to you'). In this way the recipient would be able to gain an immediate and clear indication of the legal basis for a request or provided information. In the absence of harmonisation in the different domains of relevant law (e.g. data protection and privacy) across the EU, this would help reduce the uncertainty that CERTs are confronted with concerning the legitimacy of requests from peers, and inform considerations of applicable law raised in the interviews and questionnaire. Progressing this recommendation might be included in the efforts of those currently working on such structured messaging

projects (e.g. International Telecommunications Union-Telecommunications[46] (ITU-T) group, the Internet Engineering Task Force[47] (IETF), etc.). ENISA would certainly be able to lend its voice to such activities.

C.2 Further foster R&D into privacy enhancing Security Event & Incident Monitoring (SEIM) There is further opportunity to support technology research efforts which would help CERTs in meeting their legal obligations whilst achieving their goals relating to Security Event and Incident Monitoring (SEIM). Two notable examples include the SCRUB anonymisation infrastructure (Yurcik and Woolam et al, 2007) and passive Domain Name System (Lendl, 2011), both of which offer the potential for the sharing of IP address data whilst respecting the fundamental right to privacy. Such technical measures would go hand-in-hand with organisational efforts as described above. Member States and the European Commission would be in a prime position to fund such research through national cyber security programmes or programmes such as the Framework Programme in Directorate General Research Technology Development (DG RTD).

C.3 Conduct further empirical research into cross-border CERT cooperation activities The limited evidence from this exercise (albeit across a difficult-to-reach community) has illustrated potential issues which warrant further exploration. In particular, identifying via in-depth case studies the process and operational considerations of information exchange might shed further light on the practical implications of addressing concerns highlighted in the interviews and questionnaire; for example, national practice concerning common interpretations of relevant laws or detailed examples of the process by which teams manage requests and which other stakeholders they interact with.

[46] See http://www.itu.int/ITU-T/ [accessed 22 August 2011]

[47] See http://www.ietf.org/ [accessed 22 August 2011]

References

Reports

Almenoff, J.S., Pattishall, E.N., Gibbs, T.G., DuMouchel, W., Evans S. J. W. and Yuen N., (2007) 'Novel statistical tools for monitoring the safety of marketed drugs', *Clinical Pharmacology & Therapeutics*: 82, 157-166.

ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information (2011) « Défense et sécurité des systèmes d'information: Stratégie de la France ». Available from: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf [accessed 16 August 2011]

Bessant, C. (ed.) (2009) *Information Sharing Handbook*, The Law Society, London.

Bhaskar, R. (2006) 'State and Local Law Enforcement is not Ready for a Cyber Katrina', *Communications of the ACM* 49(2): 81–83.

Biggs, S., Vidalis, S. (2009) *Cloud Computing: The Impact on Digital Forensics*, Information Operations Research Group, University of Wales.

Broucek, V., Turner P. (2005) *'Riding Furiously in All Directions' – Implications of Uncoordinated Technical, Organisational and Legal Responses to Illegal or Inappropriate On-Line Behaviours*, EICAR 2005 Conference Best Paper Proceedings, 30 April – 3 May 2005, Saint Julians, Malta, pp. 190–203.

Brown, I. (2010) 'Communications Data Retention in an Evolving Internet', *International Journal of Law and Information Technology* 19(2): 95–109.

Brownlee, N., Guttman, E. (1998) 'Expectations for Computer Security Incident Response', IETF Request for Comments (RFC 2350); Available from: http://www.ietf.org/rfc/rfc2350.txt [accessed 17 August 2011]

Bunn, M. (2005) 'Incentives for Nuclear Security', Institute for Nuclear Materials Management 46th Annual Meeting, Phoenix, Arizona.

Burnstein, A.J. (2007) 'An Uneasy Relationship: Cyber Security Information Sharing, Communications Privacy, and the Boundaries of the Firm', Archive, NY University.

Cabinet Office (2009) 'Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space', Available from: Command Paper 0906 Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space [accessed 16 August 2011.

CEFIC (2009) Cefic model SIEF Agreement: benefits and practical aspects.

Chapelle, B. d. l., Kleinwächter, W. et al (2010) *International and multi-stakeholder co-operation on cross-border Internet*, Council of Europe, Directorate-General of Human Rights and Legal Affairs.

Chisholm-Smith, G. (2006) 'Identification of liability-related impediments to sharing chapter 409 safety data among transportation agencies and a synthesis of best practices', National Cooperative Highway Research Program Research Results Digest 306.

Christiansson, H., Fischer, G. (2005) *CIIP: A Swedish Perspective*. Stockholm, FOI.

Collins, H.E., et al (1986) 'Information exchange and mutual emergency assistance: The framework for accident response and notification', *IAEA Bulletin*, Autumn 1986. Available from: http://www.iaea.org/Publications/Magazines/Bulletin/Bull283/28302741617.pdf [Accessed 19 August 2011]

Computer Security Incidents_Internet2 (CSI2) Working Group (2006) 'Computer Security Incident Internet 2'.

Computer Security Incidents_Internet2 (CSI2) Working Group (2009) 'Security Incident Management Essentials'.

Cormack, A.N. (2011) 'Incident Response and Data Protection'; Available from http://www.terena.org/activities/tf-csirt/publications/data-protection-v2.pdf

Dependability Development Support Initiative (2002) 'Roadmap: Warning and Information Sharing', DDSI IST-2000-29202; Available from: http://www.ddsi.org/htdocs/Documents/final%20docs/DDSI_D4_WIS_roadmap_f.pdf [accessed 16 August 2011].

ENISA (2009b) 'Baseline capabilities for national/governmental CERTs (Part 1 Operational Aspects)'; Available from: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs [accessed 16 August 2011].

ENISA (2006/2007) EISAS – European Information Sharing and Alert System. A feasibility study 2006/2007.

ENISA (2006a) 'CERT cooperation and its further facilitation by relevant stakeholder. Deliverable WP2006/5.1 (CERT-D3)'; Available from: http://www.enisa.europa.eu/act/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders [accessed 16 August 2011]

ENISA (2006b) 'ENISA *ad hoc* Working Group on CERT cooperation and support'; Available from: http://www.enisa.europa.eu/act/cert/other-work/files/20060227_chair_wg_cert_report.pdf [accessed 16 August 2011]

ENISA (2009) 'Good Practice Guide'; Available from: http://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/good-practice-guide [accessed 16 August 2011]

ENISA (2010a) 'Baseline Capabilities of National/Governmental CERTs (Part 2 Policy Recommendations)'; Available from: http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations [accessed 16 August 2011]

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

ENISA (2011) 'Cyber Security Strategy of the Czech Republic for the 2011–2015 Period'; Available from: http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF [accessed 16 August 2011]

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.

Federal Ministry of the Interior, Germany (2008) 'Early detection and Mitigation of IT Crises'; Available at: http://www.bmi.bund.de/cae/servlet/contentblob/560094/publicationFile/27813/kritis_2_eng.pdf [accessed 16 August 2011]

Federal Ministry of the Interior, Germany (2011) 'Cyber Security Strategy for Germany': Available at: http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile [accessed 30 November 2011]

Fullerton, P.J. (2008) 'Removing barriers to sharing data between national institutions and reducing response burdens'; Available from: http://epp.eurostat.ec.europa.eu/portal/page/portal/conferences/documents/94th_dgins_conference/P%20I-4%20UK%20-%20DATA%20SHARING.PDF

Gal-Or, E., Ghose, A. (2004) *The Economic Consequences of Sharing Security Information. Economics of Information Security* (L.J. Camp and S. Lewis), New York, Kluwer Academic Publishers.

Gole, J. (2006) 'Telecoms Service Provider Network Resiliency Measures: A Survey', ENISA.

Goode, S., Lacey, D. (2005) 'Social Embeddedness and Sharing Security Information: Bridging the Cost Benefit Gap', 20th Australasian Conference on Information Systems 2–4 Dec 2009, Melbourne

Gordon, L.A., Loeb, M.P., et al (2003) 'Sharing information on computer systems security: An economic analysis', *Journal of Accounting and Public Policy* 22: 461–485.

GPEN (2011) 'Website of Global Prosecutors of e-Crime Network'; Available at: http://www.gpen.info/index.php [Accessed 17 August 2011]

Graux, H. (2011) 'Study of case law on the circumstances in which IP addresses are considered personal data: SMART 2010/2012 – D3. Final report'; Available from: http://timelex2011.svn.be/frontend/files/userfiles/files/publications/2011/IP_addresses_report_-_Final.pdf [accessed 16 August 2011]

Grewe, B.A. (2004) 'Legal Barriers to Information-Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations', Commission on Terrorist Attacks Upon the United States.

Gritzalis, S., Yannacopoulos, A.N., et al (2007) 'A Probabilistic Model for Optimal Insurance Contracts against Security Risks and Privacy in IT Outsourcing Environments', *International Journal of Information Security* 6: 197–211.

Grobauer, B., Schreck, T. (2010) 'Towards Incident Handling in the Cloud: Challenges and Approaches',2010 ACM workshop on Cloud computing security workshop, New York.

ISAC Council (2004) 'Vetting and Trust for Communication among ISACs and Government Entities', W. Paper.

Kenneally, E.E., Claffy, K. (2010) 'Dialing Privacy and Utility: A Proposed Data-Sharing Framework to Advance Internet Research', San Diego, Cooperative Association for Internet Data Analysis (CAIDA), University of California.

Killcrece, G., Kossakowski, K.-P., et al (2003a) 'State of the Practice of Computer Incidence Response Teams (CSIRTs)', Carnegie Mellon Software Engineering Institute.

Killcrece, G., Kossakowski, K.-P., et al (2003b) 'Organizational Models for Computer Security Incident Response Teams (CSIRTs)', Carnegie Mellon Software Engineering Institute.

Kossakowski, K.-P., Sander, J., et al (2006) 'A German Early Warning Information System – Challenges and Approaches', 18th Annual FIRST Conference. CarmentiS. Baltimore, MD.

Ksherti, N. (2009) 'Positive Externality, Increasing Returns, and the Rise in Cybercrimes', *Communications of the ACM* 52(12): 141–144.

Lendl (2011) 'Passive DNS System Update', Presented at the 32nd TF-CSIRT Meeting, Barcelona, Spain; Available at: http://www.terena.org/activities/tf-csirt/meeting32/lendl-dns.pdf [accessed 17 August 2011]

Madnick, S., Li, X., et al (2009) 'Experiences and Challenges with Using CERT Data to Analyze International Cyber Security', Working Paper Series. Massachusetts Institute of Technology Engineering Systems Division.

Makedon, F., Sudborough, C., et al (2008) 'A Safe Information Sharing Framework for E-Government Communication'.

Mandel, J.R. (1992) 'Data sharing to the defense (sharing information to resolve liability issues)', Association Management.

Messenger, M. (2005) 'Why would I tell you? Perceived influences for disclosure decisions by senior professionals in inter organisation sharing forums', Unpublished Masters dissertation, University of London Birkbeck School of Management and Organisational Psychology.

Miller, P. (2005) *How can we Improve Information Sharing among Local Law Enforcement Agencies?*, Monterey, California, Naval Postgraduate School.

Ministry of Justice (2010) 'Addressing the Drivers of Crime. Background Paper: Improving information-sharing, inter-agency co-ordination and case management to address the drivers of crime', Ministry of Justice.

Ministry of Security and Justice (2011) 'The National Cyber Security Strategy (NCSS): Strength through cooperation'; Available at: http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/actueel/nieuws/nationale-cyber-security-strategie-gepresenteerd/nationale-cyber-security-strategie-gepresenteerd/govcert%3AdocumentResource%5B3%5D/govcert%3Aresource [accessed 16 August 2011]

National Infrastructure Security Co-ordination Centre (2009) *Sharing Culture Assessment Workbook*.

Onsrud, H.J. (1995) 'Role of Law in Impeding and Facilitating the Sharing of Geographic Information', in *Sharing Geographic Information* (H.J. Onsrud and G. Rushton), Rutgers, CUPR Press, pp. 292–306.

OECD (Organisation for Economic Cooperation and Development) (2011) The Future of the Internet Economy: A Statistical Profile – June 2011 update; OECD, Paris http://www.oecd.org/dataoecd/24/5/48255770.pdf [accessed 29 September 2011]

Pirmohamed, M., and Darbyshire, J. (2004) 'Collecting and sharing information about harms: Appropriate strategies to communicate this information are essential', *British Medical Journal*, vol. 329, Iss. 3 (July): 6-7.

Privacy International (2009) 'Sharing the Misery: The UK's Strategy to Circumvent Data Privacy Protections', Balck Zone Report Series.

Robinson, N., Valeri, L., Cave, J., et al (2011) *The Cloud: Understanding the Security, Privacy and Trust Challenges*, Santa Monica, CA, RAND Corporation, 2011.

Schmidt, A., Pasic, A., et al (2008) 'Position Paper on Security Challenges in Future Internet', Plenary Workshop of Working Groups. Paris, Think-Trust.

Schonlau, M., Fricker, R.D., Elliott, M.N. (2002) *Conducting Research Surveys via E-Mail and the Web*, Santa Monica, CA, RAND Corporation.

Schwartz, P.M., Janger, E.J. (2007. 'Notification of Data Security Breaches', *Michigan Law Review* 105(5): 913–984.

Sclafane, S. (2010) 'Insurers Respond As Privacy Attacks Soar', National Underwriter Property and Casualty.

Sherman, S.E.E.B. (2004) 'I Object … It's Hearsay': Hearsay and Evidence in the Computer Emergency Response Team (CERT). InfoSec. S. Institute.

Silicki, K., Maj, M. (2008) 'Barriers to CSIRTs cooperation. Challenge in practice – the CLOSER Project', 20th FIRST Annual Conference, Vancouver, Canada.

Slagell, A., Yurcik, W. (2005) 'Sharing Computer Network Logs for Security and Privacy: A Motivation for New Methodologies of Anonymization. Security and Privacy for Emerging Areas in Communication Networks', Workshop of the 1st International Conference.

Sommer, P.M. (2009) *Directors' and Corporate Advisors' Guide to Digital Investigations and Evidence* (2nd edn), Swindon, UK: Information Assurance Advisory Council.

Stikvoort, D. (2009) by courtesy of NISCC (UK); Trusted Introducer Information Sharing Traffic Light Protocol (ISTLP) https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf [accessed 16 August 2011]

Symantec LIRIC Ltd (2009) Messaging Standards for Sharing Security Information (MS3i) European Commission, DG Justice, Freedom and Security.

Thomas, R., Walport, M. (2008) Data Sharing Review Report. Available from: http://www.justice.gov.uk/reviews/docs/data-sharing-review-report.pdf [accessed 30 November 2011]

Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A-M., Vihul L. (2008) 'Cyber Attacks Against Georgia: Legal Lessons Identified', Tallinn, ET: Cooperative Cyber Defence Centre of Excellence.

United States General Accounting Office (2000) 'Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination', Statement of Jack L. Brock, Jr.

United States General Accounting Office (2000) 'The Challenge of Data Sharing: Results of a GEO-Sponsored Symposium on Benefit and Loan program', Report to the Committee on Governmental Affairs, US Senate.

United States Government Accountability Office (2007) 'Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats'. USGA Office.

Valeri, L., Robinson, N., et al (2005) *Handbook of Legal Procedures of Computer and Network Misuse in EU Countries*, Tr-337-EC, RAND Corporation, Santa Monica, CA, USA.

Vermeulen, G., De Bondt, W. (2009) 'EULOCS. The EU Level Offence Classification System. A Bench-mark for Enhanced Internal Coherence of the EU's Criminal Policy', *IRCP series* Vol. 35, Maklu Publishers, Brussels, Belgium.

WANO, http://www.wano.info [accessed 19 August 2011]

Wiik, J., Gonzalez, Jose J., Davidsen, P.I., Kossakowski, K-P. (2009) Chronic workload problems in CSIRTs. Paper read at 27th International Conference of the System Dynamics Society July, Albuquerque, NM, USA.

Willis, H., Lester, G., Treverton, G. (2009) Information Sharing for Infrastructure Risk Management: Barriers and Solutions. *Intelligence and National Security*, 24(3):339–365(27)

Wright, D., Hert, P.D., Gutworth, S. (2011) 'Are the OECD Guidelines at 30 Showing Their Age?', *Communications of the ACM* 54(2).

Yurcik, W., Woolam, C., et al (2007) 'SCRUB-tcpdump: A Multi-Level Packet Anonymizer Demonstrating Privacy/Analysis Tradeoffs.'

Legislative texts and official documents

Article 29 Working Party 'Opinion 2/2010 on online behavioural advertising'; Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf [accessed 16 August 2011]

Article 29 Working Party 'Opinion 4/2007 on the concept of personal data'; Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf [accessed 16 August 2011]

Bundestag (14/8/2009) 'Act to Strengthen the Security of Federal Information Technology'; Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile [accessed 16 August 2011]

Parlament České republiky (2011) Resolution No. 564 approving the Czech Cyber Security Strategy for the Period 2011–2015 (20 July 2011)

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: 'A strategy for a Secure Information Society: Dialogue, partnership and empowerment', COM(2006) 251 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 'A Digital Agenda for Europe', COM(2010) 245.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on' Critical Information Infrastructure Protection: Achievements and next steps: towards global cyber-security, COM(2011) 163 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM(2009) 149 final.

Communication on the Internal Security Strategy (22/11/2010) 'Communication from the Commission to the European Parliament and the Council: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe', COM(2010) 673 final.

Convention on Cybercrime (23/11/2011) 'Convention on Cybercrime, Budapest, 23.XI.2001'. Council of Europe; Available at: http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm [accessed 16 August 2011]

Convention on Mutual Assistance (29/5/2000) 'Council Act establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union', *Official Journal of the European Communities* C 197/1.

Directive 2002/22/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, *Official Journal of the European Union* L337/11.

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L 201*, pp. 37–47.

Directive 2003/98/EC on the re-use of public sector information, *Official Journal of the European Union* L 345/90.

Directive 2004/48/EC on the enforcement of intellectual property rights, *Official Journal of the European Union* L 195/16.

Directive 2006/54/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of publication communications networks and amending Directive 2002/58/EC, *Official Journal of the European Union* L 105/54.

Directive 2009/24/EC on the legal protection of computer programs, *Official Journal of the European Union* L111/16.

Directive 2011/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal of the European Communities* L 167/10.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281*, pp. 31-50.

Directive on the harmonisation of certain aspects of copyright and related rights in the information society, *Official Journal of the European Communities* L 167/10.

ECI Directive, (8/12/2008) 'Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection', *Official Journal of the European Union* L 345/75.

European Commission (30/9/2010a) 'Proposal for a directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA', COM (2010) 516 final.

European Commission (30/9/2010b) 'Proposal for a Regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA)', COM (2010) 521 final.

European Parliament and Council of the European Union (11/3/1996) 'Directive 96/9/EC on the legal protection of databases', *Official Journal of the European Union* L 077.

Folketinget (1/6/2011) 'Act on Processing of Personal Data when Operating the Governmental Warning Service for Internet Threats etc.'; Available at: https://www.govcert.dk/gcdata/uk_version_l197.pdf [accessed 16 August 2011]

Framework Decision on Attacks against Information Systems (2005) 'Attacks against information systems', Council Framework Decision 2005/222/JHA.

Framework Decision on EJ, (30/11/2009) Acts adopted under Title VI of the EU Treaty, Council Framework Decision of 30 November 2009 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, *Official Journal of the European Union L 328/42.*

Revised Telecommunications Regulatory Framework (25/11/2009) 'Directive 2009/140/EC amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associate facilities, and 2002/20/EC on the authorisation of electronic communications networks and services', *Official Journal of the European Union* L 337/37.

Swedish Initiative (18/12/2006) 'Simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union', Council Framework Decision 2006/960/JHA.

United States Congress (1986) 'Electronic Communications Privacy Act of 1986 (ECPA)'; Available at: http://it.ojp.gov/default.aspx?area=privacy&page=1285 [accessed 16 August 2011]

USC (2000) 'Stored communications act. 18 U.S.C. §§ 2701-2712', United States Congress; Available at: http://www.cybercrime.gov/ssmanual/03ssma.pdf [accessed 18 August 2011]

Appendix A: Example legal checklist for privacy and data protection

From a practical perspective, CERTs that are looking to share or request information should at the very least evaluate the following questions with respect to data protection:

- Is the information legally considered to be personal data, and therefore subject to data protection rules?
- If so, have you obtained the personal data legitimately, i.e. in accordance with nationally applicable data protection laws? The CERT will need to evaluate in particular:

  o Whether there was a legitimate basis for the collection of the personal data. This question should be evaluated keeping into account the original source of the data (e.g. an ISP or service provider), the specific mandate of the CERT and any legal basis for its work (including possible specific laws or legal exemptions);

  o Whether there are specific national legal restrictions that apply to the data, e.g. protection of judicial data, professional secrecy or telecommunications secrecy;

  o Whether the collected data observes the principles of the nationally applicable data protection laws, including specifically with respect to data quality and proportionality. The use of anonymisation and encryption techniques should be considered whenever viable.

  o Whether data subject rights are appropriately respected, again taking into account any specific laws that may apply to the CERT.

- Before requesting personal data from a third party or examining whether or not to share personal data with a third party, the CERT should:

  o If this is not the case, it should examine whether an alternative basis for legitimacy exists, on the basis of the national transposition of Article 7 of the Data Protection Directive. For this question, the specific mandate of the CERT and any legal basis for its work is crucial, as is the identity, mandate and legal basis for the third party's operations;

  o Evaluate whether data will be transferred to a recipient outside of the European Union, and if so, whether this transfer is legitimate on the basis of the national transposition of Article 25 of the Data Protection Directive;

  o Verify whether the planned data exchange observes the principles of the nationally applicable data protection laws, including specifically with respect to data quality and proportionality. The use of anonymisation and encryption techniques should be considered whenever viable;

  o Obtain assurances that the recipient of the shared data will only process it in accordance with applicable data protection law.

If no legal expertise is available in-house, the CERT should consult appropriate third parties such as lawyers or data protection bodies before processing personal data.

Appendix B: List of acronyms

ACM – Association for Computing Machinery

ANSSI – Agence nationale de la sécurité des systèms d'information

ARF – Abuse Report Format

Art 29 WP – Article 29 Working Party (of the Data Protection Directive 95/46/EC)

ASFJ – Area of Freedom, Safety and Justice

BSI – Bundeamt für Sicherheit in der Informationstechnik

CAA – Civil Aviation Authority

CERT – Computer Emergency Response Team

CII – Critical Information Infrastructure

CIIP – Critical Information Infrastructure Protection

CIP – Critical Infrastructure Protection

CPNI – Centre for the Protection of the National Infrastructure

CSIRT – Computer Security Incident Response Team

DDoS – Distributed Denial of Service

DHS – Department of Homeland Security

DNA – Deoxyribonucleic acid

DNS – Domain Name System

DPA – Data Protection Authority

DRD – Data Retention Directive

ECCP – European Cybercrime Platform

ECHR – European Charter of Human Rights

ECI – European Critical Infrastructure

ECRIS – European Criminal Records Information System

EEA – European Economic Area

EGC – European Government CERT Grouping

EJN – European Judicial Network

ENISA – European Network and Information Security Agency

EP3R – European Public Private Partnership for Resilience

EU – European Union

FIRST – Forum of Incident Response & Security Teams

FoI – Freedom of Information

G8 – Group of 8 industrialised nations

GPEN – Global Prosecutors of e-Crime Network

ICRP – International Cancer Research Portfolio

ICT – Information Communications Technology

IETF – Internet Engineering Task Force

IP – Internet Protocol

ISP – Internet Service Provider

ITU – International Telecommunications Union

ITU-T – International Telecommuncations Union-Telecommunications group

JHA – Justice and Home Affairs Council

KII – Key Informant Interview

LECC-SIG – Law Enforcement / CSIRT Cooperation Special Interest Group

LOAC – Law of Armed Conflict

LOPD – Data Protection Law (Spain)

MMR – Measles, Mumps and Rubella vaccine

MoU – Memorandum of Understanding

MS – Member States

MS3i – Messaging Standard for Secure Information Exchange

NDA – Non Disclosure Agreement

NHTCU – National Hi-Tech Crime Unit

OECD – Organisation for Economic Co-operation and Development

PCII – Protected Critical Information Infrastructure

PSI – Public Sector Re-use of Information

R&D – Research and Development

RFC – Request for Comments

SEIM – Security Event and Incident Monitoring

SIS – Schengen Information System

SLA –Service Level Agreement

SOE – Special Operating Events

TERENA – Trans-European Research and Education Networking Association

TF-CSIRT – Task Force on Computer Security Incident Response Team

TLP – Traffic Light Protocol

ToR – Term of Reference

TRIPS – Trade Related Aspects of Intellectual Property Rights

WANO – World Association of Nuclear Operators

WTO – World Trade Organisation

ENISA – European Network and Information Security Agency
PO Box 1309, 71001 Heraklion, Greece
Tel: +30 2810 391 280
Fax: +30 2810 391 410

www.enisa.europa.eu