CERT cooperation and its further facilitation by relevant stakeholders

Deliverable WP2006/5.1(CERT-D3)

1 Management Summary

The document at hand is dedicated to the cooperation among CERTs and similar entities. It is the first document of its kind, and not only tells the story of cooperation in Europe and beyond, but that also tries to summarise the lessons learned and give recommendations to the involved stakeholders on how cooperation can be improved.

This document is aimed at management, policy makers, teams and other stakeholders that, in one way or another, are involved in CERT cooperation. It should also provide an interesting read for everybody else who wants to learn about the rich culture of cooperation among European and international teams over the last two decades.

The document *Cert cooperation and its further facilitation by the relevant stakeholders* implements the deliverable WP2006/5.1 (**CERT-D3**) as laid down in ENISA Working Programme 2006, Paragraph 5.1.

2 Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of the-art and it might be updated from time to time.

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

This publication is intended for educational and information purposes only. 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.

3 Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special “Thank You” goes to the following contributors:

- Przemysław Jaroszewski, Krzysztof Silicki, and Mirosław Maj from NASK/CERT Polska, who produced the first version of this document as consultants
- The countless people who reviewed this document

4 Terms and Definitions

In this section we give a basic description of elementary terms and definitions which are frequently used in this document.

4.1 CERTs (CSIRTs, IRTs, other kinds of the CERT teams)

CERT stands for Computer Emergency Response Team. There exist various abbreviations for the same sort of teams:

- CERT or CERT/CC (Computer Emergency Response Team / Coordination Centre)
- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

The first major outbreak of a worm in the global IT infrastructure occurred in the late 1980s. The worm was named Morris[1] and it spread swiftly, effectively infecting a great number of IT systems around the world.

This incident acted as a wake-up call: suddenly people got aware of a strong need for cooperation and coordination between system administrators and IT managers in order to deal with cases like this. Due to the fact that time was a critical factor, a more organised and structural approach on handling IT security incidents had to be established. And so a few days after the "Morris-incident" the Defence Advanced Research Projects Agency (DARPA) established the first CSIRT: the CERT Coordination Centre (CERT/CC[2]), located at the Carnegie Mellon University in Pittsburgh (Pennsylvania).

This model was soon adopted within Europe, and 1992 the Dutch Academic provider SURFnet launched the first CSIRT in Europe, named SURFnet-CERT[3]. Many teams followed and at present ENISAs *Inventory of CERT activities in Europe*[4] lists more than 100 known teams located in Europe.

Over the years CERTs extended their capacities from being a mere reaction force to a complete security service provider, including preventative services such as alerts, security advisories, training and security management services. The term "CERT" was soon considered insufficient. As a result, the new term "CSIRT" was established at the end of the1990s. At the moment both terms (CERT and CSIRT) are used synonymously, with CSIRT being the more precise term.

For the purpose of this document the term CERT will be used!

---

[1] More info about the Morris Worm http://en.wikipedia.org/wiki/Morris_worm

[2] CERT-CC, http://www.cert.org

[3] SURFnet-CERT: http://cert.surfnet.nl/

[4] ENISA Inventory: http://www.enisa.europa.eu/cert_inventory

4.2 The term Constituency

From now on the (in the CERT communities) well established term 'constituency' will be used to refer to the customer base or the served group of users of a CERT. A single customer will be addressed as 'constituent', a group as 'constituents'.

4.3 CERT Services as basis for cooperation

To understand the role of cooperation among CERT/CSIRT teams in the process of enhancing effectiveness of combating threats, vulnerabilities and security incidents it is necessary to discuss benefits of such a cooperation as an important factor in improving services offered by CERTs, as well as barriers that can slow down this process. Further on, there is a question: Who are (or can be) the relevant stakeholders that facilitate (or can facilitate) the CERT cooperation? In this chapter the status quo analysis of benefits and barriers of CERT cooperation is performed and also some models of trust between parties are discussed. Several types of relevant stakeholders facilitating this cooperation have been described, as well. At the end of this chapter evaluation of the most important cooperation initiatives has been done, taking into the consideration two main aspects: what has been achieved and what future opportunities are available for those initiatives

A good way to acquire information about CERT activities is to find a list of services they provide. Below there is a list developed by the CERT/CC team. The list of services is important from the cooperation point of view. A modified list of services was used to present chapter *7.2 Influence of cooperation on CERTs services improvement*.

<table>
<tr><th>Reactive Services</th><th>Proactive Services</th><th>Artifact Handling</th></tr>
<tr><td rowspan="3">Alerts and Warnings
Incident Handling
Incident analysis
Incident response support
Incident response coordination
Incident response on site
Vulnerability Handling
Vulnerability analysis
Vulnerability response
Vulnerability response coordination</td><td rowspan="3">Announcements
Technology Watch
Security Audits or Assessments
Configuration and Maintenance of Security
Development of Security Tools
Intrusion Detection Services
Security-Related Information Dissemination</td><td>Artifact analysis
Artifact response
Artifact response coordination</td></tr>
<tr><td>Security Quality Management</td></tr>
<tr><td>Risk Analysis
Business Continuity and Disaster Recovery
Security Consulting
Awareness Building
Education/Training
Product Evaluation or Certification</td></tr>
</table>

Fig. 1. CSIRT Services list from CERT/CC[5]

A second well known document that deals with CERT services is RFC 2350 “Expectations for Computer Security Incident Response”[6].

And finally the standard ISO/IEC 17799 mentions incident response capabilities (in chapter 6.3 Responding to security incidents and malfunctions).

Sectors of CERT operation

Usually CERTs are distinguished by the sector they provide their services to. The *ENISA CSIRT Setting up Guide*[7] defines the following sectors: The following different kinds of teams can be identified:

- Academic Sector
- Commercial
- CIP/CIIP Sector
- Governmental Sector
- Internal

[5] CSIRT Services list from CERT/CC: http://www.cert.org/csirts/services.html

[6] RFC 2350 "Expectations for Computer Emergency Response Teams": http://www.ietf.org/rfc/rfc2350.txt

[7] A Step-by-step approach on ho to set up a CSIRT: http://www.enisa.europa.eu/cert_guide/index_guide.htm

- Military Sector
- National
- Small & Medium Enterprises (SME) Sector
- Vendor Teams

A special kind of CERT is the national CERT, who operates on the national level. National CERTs usually do not have a constituency by themselves but rather act as security point of contact (PoC) for a country. In most cases this role is fulfilled by the governmental CERT, which serves government and governmental related agencies. An example might be US-CERT[8] that acts as a PoC for the United States and is supported by the CERT/CC in delivering its services.

4.4 WARPs

WARPs (Warning, Advice and Reporting Points) are part of NISCC's (National Infrastructure Security Co-ordination Centre in the United Kingdom) information sharing strategy to protect the UK's Critical National Infrastructure from electronic attack. WARPs have been shown to be effective in improving information security by stimulating better communication of alerts and warnings, improving awareness and education, and encouraging incident reporting.

WARP members agree to work together in a community and share information to reduce the risk of their information systems being compromised and therefore reduce the risk to their organisation. This sharing community could be based on a business sector, geographic location, technology standards, risk grouping or whatever makes business sense[9]. See also chapter *8.6.2*.

4.5 Other security teams

4.5.1 Abuse Teams

Abuse Teams are very similar to CERTs and usually operate within the structure of an Internet Service Provider (ISP). The character of tasks differs, but often a CERT also acts as an Abuse Team for their constituents. The mainly accepted characteristics of Abuse Teams are:

- Dealing with a large number of the same kinds of incidents (like spam, phishing etc.)
- Being responsible for the customers (end-users) of a particular ISP in contacts with other network organisations and individuals
- Dealing with relatively "simple" and well-documented incidents only
- Increased necessity of taking into consideration commercial aspects of operation (for example when it comes to sanctions against “misbehaving” hosts within the their network)

---

[8] US-CERT: http://www.us-cert.gov/

[9] WARPs: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

4.5.2 System Administrators with incident response responsibility

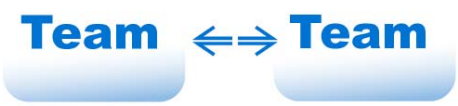
Quite often, especially in smaller organisations, no dedicated CERT is appointed, even though that organisation possesses capabilities to respond to incidents. Such capabilities usually are provided by the IT staff responsible for the operation of the network.

5 Models and Legal Basis of Cooperation

There exist different models of possible cooperation. The models we present in this chapter do not exhaust all possible models, but are aimed to cover the most common models that are characteristic to the "CERT world". Generally models of cooperation are not unique to CERTs, but do follow similar models of cooperation used by other kinds of organisations.

5.1 Models of cooperation

Bilateral team-team cooperation



This is a model of a bilateral cooperation between two teams only. It is based on the trust between particular teams and their members, usually built over years, for example through joined participation in security projects. This kind of cooperation is often stimulated by common goals for future development and similar team missions. It can lead to cooperation between more than one team, but it is commonly seen that for cooperation between multiple teams a more formal approach is necessary (see chapter 5.2 Legal basis). But also in case of bilateral cooperation teams often chose to formalise their relationship with a written agreement. The team-team model is quite effective, because teams usually focus on jointly formulated goals, which can be very concrete and simple to determinate. The team-team model is relatively easy to manage as there are fewer issues to coordinate, for example the calendar of joint events. Naturally, because of the nature of this kind of cooperation, its overall effect is limited and the beneficiaries are mostly only the collaborating teams. Even though the results (like a new tool, a new standard or something else) of the cooperation can be used by other teams also, these results only reflect needs of the participating teams. Especially in development of new standards (for example data formats for information exchange) another model of cooperation should be chosen that allows including more opinions from the CERT communities.

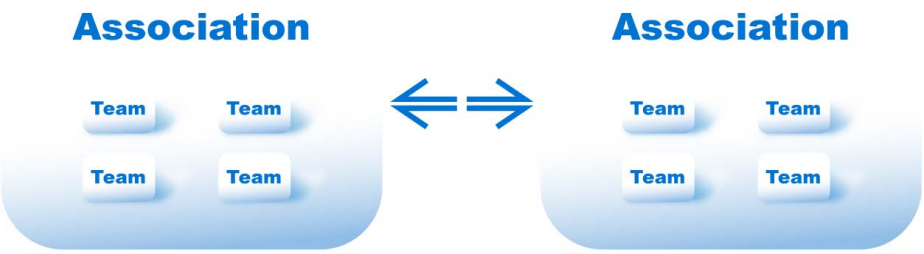
Association

The association is a model of cooperation between many teams which have common interests and goals. The framework for this kind of cooperation might be set by a common geographical area (like in the national cooperation activities), common sets of services, similar constituencies (like in the European Government CERT group[10]), sector of operations etc. The association model comes with different names: forum, task-force, group, coalition, alliance etc. An association is often a

[10] EGC: http://www.enisa.europa.eu/cert_inventory/pages/04_01_01.htm#04

launching platform for team-team cooperation, as it usually provides a framework to network with other teams and helps to discover common interests. It gives probably the best opportunity for long term cooperation between interested parties, and accommodates a dynamic process of change (joining, opting out) of an association. A long term existence of an association is beneficial for trust building (see chapter *5.3 Models of trust*), for example like in the Trusted Introducer initiative[11]. Best known examples for the association model are FIRST, TERENAs TF-CSIRT and APCERT, see chapter 6). It is worth to add that effective development of associated cooperation requires some organisational tools and formal bodies like steering groups, association chairing and secretariat support. Also facilitating cooperation by providing mailing list capability and regular meetings is very important.

Cooperation between associations



This model depicts cooperation among two or more associations. It is usually based on the common goals of both organisations and shared benefits. This kind of cooperation is very often realised by exchanging experiences (for example delegates on the organisation's meetings) and formulation of common goals and rules of cooperation (for example Memorandum of Understanding, see chapter *5.2 Legal basis for cooperation*). Cooperation between associations may concern overall activity of both sides as well as particular aspects of activity, for example technical projects. The best known example of association-association cooperation is the cooperation between TERENAs TF-CSIRT[12] and APCERT[13]. Both organisations signed a memorandum of understanding (see the document in *Annex I*).

5.2 Legal basis for cooperation

Cooperation between CERTs may assume different legal bases. Cooperation between teams (especially in the team-team model) can obviously be informal in many cases. If there is a need to formalise the cooperation, it can assume different legal forms that we list in this chapter. The motivation for formalising cooperation may be the involvement of funds, fulfilling legal requirements or the exchange of sensitive data.

Non-disclosure agreement

A non-disclosure agreement (NDA), sometimes also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement, is a legal contract between at least two parties which outlines confidential materials or knowledge the parties wish to share with one

[11] Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[12] TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

[13] APCERT: http://www.enisa.europa.eu/cert_inventory/pages/05_01.htm

another for certain purposes, but wish to restrict from generalised use. In other words, it is a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of trade secret. As such, an NDA can protect non-public business information[14].

Memorandum of Understanding

A Memorandum of Understanding (MOU) is a legal document describing a bilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action, rather than a legal commitment. It is a more formal alternative to a gentlemen's agreement, but generally lacks the binding power of a contract[15].

As an example of a MoU see *Annex I*.

Contract

A contract is a "promise" or an "agreement" made of a set of promises. Breach of this contract is recognised by the law and legal remedies can be provided. In civil law, contracts are considered to be part of the general law of obligations. The law generally sees performance of a contract as a duty[16].

Terms of Reference

A Terms of Reference (ToR) is a document which describes the purpose and structure of a project. Otherwise known as a *TOR* or a *Project Charter*, the Terms of Reference is created during the initiation phase of a project management life cycle[17].

Creating a detailed Terms of Reference is critical to the success of an association, as it defines its purpose of existence:

- Vision, objectives, scope and deliverables (i.e. what has to be achieved)
- Stakeholders, roles and responsibilities (i.e. who will take part in it)
- Resource, financial and quality plans (i.e. how it will be achieved)
- Work breakdown structure and schedule (i.e. when it will be achieved)

For an example ToR see *Annex II*.

[14] NDA in Wikipedia: http://en.wikipedia.org/wiki/Memorandum_of_understanding

[15] MoU in Wikipedia: http://en.wikipedia.org/wiki/Non-disclosure_agreement

[16] Contract in Wikipedia: http://en.wikipedia.org/wiki/Contract

[17] ToR in Wikipedia: http://en.wikipedia.org/wiki/Terms_of_reference

5.3 Models of Trust

Development of trust plays a very important role in cooperation between CERTs. In many cases, operational data may be considered private or otherwise sensitive. On the other hand, sharing of sanitised data often causes additional workload or prevents the receiving party from effectively acting altogether.

Bilateral and multilateral agreements

The most straightforward way to establish trust between several parties is to sign a legal document defining the scope of cooperation and data sharing. These kinds of documents are presented in chapter *5.2 Legal basis for cooperation*. Note that contracts and non-disclosure agreements are usually legally binding, thus the signing parties can be assured that possible breaches of the agreement would result in legal repercussions.

Note also that this model of trust does not scale very well. Any written document, especially when legally binding, has to be agreed by all parties, which in case of CERT cooperation usually means legal departments of companies that operate a CERT team. In practice, documents such as a memorandum of understanding or contracts will usually not involve more than two parties.

Another, more "relaxed" possibility is using a Code of Conduct (CoC), which is not a legally binding document. A CoC usually contains a set of rules and guidelines for a specific behaviour and decisions of the cooperating parties. Even though it is usually not legally binding, signing a code of conduct is a clear sign of good will to respect the rules and behave in certain ethical ways. In closed communities it may be obligatory to sign a code of conduct in order to become a member (for example European Governmental Cooperation, see chapter *6.2 Regional cooperation*). At the same time a breaching of the CoC can be a clear reason to ban or expel a participant from the community.

How does a Code of Conduct work?

In 2005 one of the existing CERT teams applied to join the Trusted Introducer (TI) forum. The problem was that this team had quite "liberal" approach to the vulnerability handling process. It had been publishing exploits for known vulnerabilities as "proof of concept". The question arose: should this team be allowed to join the TI framework? For achieving a decision one of the statements from the TI CoC was applied. According to the statement "*a team should not publish materials which could be used as tools to abuse somebody else's resources (computers, networks)*". So the team was refused to join the initiative.

Sponsorship

Another well known model of building trust is the model of sponsorship. In the CERT world this model was introduced and popularised by the FIRST community (see *chapter 6.3 International cooperation*). It is based on the closer relationship between a team, which can manifest its respected level of trust, and a new team, which wants to reach some level of trust. A trusted team becomes a sponsor for the new team. It conducts a new team through a process of fulfilling various requirements, which should serve as a guarantee for the other teams of that community, that the new member would add value and give benefit to them.

In the case of FIRST the most important issues connected to sponsorship are:

- Teach the new member about the organisation it is about to join
- Make a site-visit to learn more about the applicants working environment (and by this support the evaluation of the worthiness of the applicant)
- Introduce the new team to the community, and further foster it (by being its first point of contact for problems, questions, etc.)
- Represent the new team in the community during the application process

Limitations to trust-building

An interesting case study is the problem of building a trust relationship between two significantly different sectors, for example between a CERT with roots in the industrial sector and a CERT operating within law enforcement. The latter operates in very specific environment and very often is legally obliged to undertake restrictive steps when it becomes aware of information about breaches, crimes, etc. So the information exchange in such model would cause very concrete results like undertaking legal steps which could have a negative impact on the industrial CERT, as it would then be obliged to take an active part in the investigation. So the information exchange among these two teams would be limited to specific and restricted types of information.

This shows that all the models and bases discussed in this document can not be generically applied to all possible scenarios of cooperation, but (at least in some cases) need further examination.

Open community

In many cases a group is fairly open and anyone who claims (or in some cases proves) to have a valid interest in the matters discussed by the forum can participate. A very common example is the open security mailing lists everybody can join.

Building up trust in these open communities is not an easy thing. The open community approach generally resembles a situation when one starts with a reasonably high level of trust for other individuals (unless he has reasons otherwise) and keeps this state unless the trust is abused. This model is usually adopted by special interest groups and working groups. Although this model encourages participation and communication, most sensitive data cannot be shared among participants of open communities without violating laws. Also, the model generally works well with smaller communities – up to 30-40 people. For larger communities, a tendency to form smaller groups of interest is observed. This is a case in TERENA TF-CSIRT where the number of participants has grown over 100.

The more serious or productive the cooperation in an open group evolves, the more restrictive the rules for this group get. Usually there are a couple of very active members (also called “regulars”) that see the need of restrict the access to overall enhance the trust and productivity.

Measures usually used in that case (among others) are limitation to active users only (and exclusion of the inactive ones), election (or appointment) of an official moderator/chairperson or abandonment of the existing forum and setting up a new one with restricted access.

Accreditation

When needed, a community can use a process of accreditation to establish level of trust for its members. This process should probably be performed by an external authority – a trusted third party. It can be performed once, for example when a team or an individual applies for membership in the community, or it can be repeated periodically to ensure competence and quality of services necessary to grant a certain level of trust. This model of trust can also be beneficial for communities with large number of participants allowing for the creation of subgroups of higher trust levels, which is the case in TERENA TF-CSIRT and teams accredited by the Trusted Introducer.

The Trusted Introducer service (TI)

The Trusted Introducer (TI) is a trust broker for European CERTs. The "web-of-trust" is built by introducing three levels:

- **Listed** – any team identified within the scope of TI
- **Accreditation Candidate** – a team which received and accepted invitation for accreditation process
- **Accredited** – a team which successfully completed accreditation / verification process

An invitation to start the accreditation process can be sent to a "Listed" team upon its request or e.g. by recommendation of an already "Accredited" CERT. The process of accreditation requires the team to declare its support for a number of criteria and provide a standardized set of information about itself. This data is then kept and maintained by the TI to ensure it is correct and up to date. Gaining the "Accredited" level results in access to numerous services, e.g. a database of in-depth operational contacts of all accredited teams, the TI mailing lists open to accredited CERTs only, PGP key signing, etc.

The services of the TI are provided by an independent contractor appointed by TERENA and supervised by TI Review Board consisting of 5 members: a TERENA representative, three members elected by accredited teams and the chair of TERENA TF-CSIRT *ex officio*.

5.4 Overview of existing cooperation initiatives

Below is a list of many known organisations and initiatives. These examples are a fundamental material for further research on cooperation, cooperation evaluation and ideas for future facilitation and improvement. In this chapter we will shortly introduce the name and scope of the known activities, and elaborate more about them in following chapters.

There are some known examples of cooperation between CERT teams operating in the same country. The detailed description of them is presented in chapter *6.1 National cooperation*.

CIRCA (Austria) – Austrian national forum of cooperation, also known as CIRCA (Computer Incident Response Coordination)

CERT-Verbund (Germany) – the German CERT-Verbund initiative associates German security and incident response teams from various sectors

O-IRT-o (The Netherlands) – the Dutch o-IRT-o initiative associates CERT teams listed on the www.cert.nl website. The website is a starting point for contacting an appropriate CERT team in The Netherlands

Polish Abuse Forum (Poland) – the Polish Abuse Forum assembles a group of CERTs and security teams of Polish ISP (Internet Service Providers) and ICP (Incident Content Providers)

UKCERTS (United Kingdom) – the British UKCERTs alliance is an informal forum of CERTs from different sectors.

The next level of cooperation is international cooperation. It is usually based on geographical criteria facilitating closer contacts and cooperation in a certain region. This level of cooperation is referred to as regional and/or international cooperation in this document. Sometimes there is another distinguishing feature besides the geographical region, for example, a particular sector that is common to the teams inside a cooperation activity.

APCERT – a coalition of CERTs established to ensure network security, especially by incident response activities, in the Asia Pacific Region. APCERT associates teams from 13 economies across Asian Pacific region.

CEENet - Central and Eastern European Networking Association (CEENet) is an association comprised of 23 national research and education networks from: Albania, Armenia, Austria, Azerbaijan, Bulgaria, Croatia, Czech Republic, Estonia, Georgia, Greece, Hungary, Latvia, Lithuania, Macedonia, Moldova, Poland, Romania, Russia, Serbia and Montenegro, Slovenia, Slovakia, Turkey and Uzbekistan. The primary mission of CEENet is to co-ordinate the international aspects of the academic, research and education networks in Central and Eastern Europe and in adjacent countries. On this basis exchange of knowledge about security aspects of computer networks exploitation between member countries is conducted. Thus, naturally, building up new CERTs and cooperation among them is becoming more and more important for CEENet.

EGC – European Governmental CERTs group is a group of CERTs with governmental constituencies and national responsibilities in their countries. They cooperate in tasks specifically related to the operational work of governmental CERTs.

NORDUnet CERT – this group assembles Scandinavian CERTs within the NORDUnet network. NORDUnet is a cooperation of Nordic national research networks (NREN).

FIRST – the oldest (founded 1990) and the biggest international forum of CERTs and other security teams. FIRST brings together more than 200 members from around the world. Within the forum there are many formal and informal initiatives usually built on the common areas of interest, constituencies or provided services. The formal cooperation is built within the confines of SIGs (Special Interest Groups).

TERENA TF-CSIRT – a task force organised under the auspices of the TERENA[18] (Trans European Research and Education Networking Association). The task force is an informal platform for cooperation for European CERTs that facilitates closer collaboration between particular teams or group of teams (common projects, common initiatives). Within the task force the Trusted Introducer initiative was built.

[18] TERENA is the Trans-European Research and Academic Network, a not-for-profit association of European NRENs (National Research and Education Networks). It was formed in October 1994 through the merger of RARE (Réseaux Associés pour la Recherche Européenne) and EARN (European Academic and Research Network), and is incorporated in Amsterdam, The Netherlands. The objectives of TERENA are to promote and develop high-quality international network infrastructures to support European research and education; see: http://www.terena.nl/

6 Past and Present of Cooperation

This chapter describes the past and the present of cooperation among CERTs. The examples are divided into groups based on the different factors that were a prime reason for the creation of cooperation initiative, like geographical regions or business sector. These factors form a kind of framework (or borders) for building cooperation structures. At the end of this chapter, also some “border crossing” examples are presented.

The list of cooperation activities in this chapter is not intended to be complete, but we think that we present the most significant examples.

6.1 National Cooperation

The first presented kind of cooperation is the national cooperation. This kind of cooperation gathers CERTs from the same country. The same nationality, language, common knowledge about political, economic and technical issues is probably the main reasons behind such cooperation. National cooperation initiatives can act as a national point of contact (PoC) for the particular country if there is no recognised national CERT present. Usually these national groups gather teams from various sectors, including sensitive ones like government or banking sector. Such a mixture of different interests usually needs a clear statement of commitment (like a code of conduct) and a mission statement that is clearly presented to the outside world. The rest of this section lists the well known national cooperation initiatives.

Austrian national Cooperation (CIRCA.AT)

Circa is a confidential and protected electronic communication network ("Web of Trust") between network- and safety officers of Internet Service Providers (ISPs) and other carriers of IP-networks, from the private as well as from the public sector (Private Public Partnership). The electronic communication network of the private sector (ISPs and carrier of IP networks) is lead by ISPA (Internet Service Providers Austria), while in the public sector the responsibility lies within the BKA (Bundeskanzleramt und Krisenmanagement - Federal Chancellery and Crisis Management).

The goal of this Austrian security network is a nationwide early warning system for worms, viruses, so called DDoS-attacks (Distributed Denial of Service) and other scenarios which threaten the ISP-infrastructure as well as IP-networks and customers. This will be achieved through proactive measures (daily warnings, information, risk assessment, information about possible countermeasures, international correlation, etc.) as well as reactive measures (detection of intrusion attempts, coordination of countermeasures, quick information sharing and alerting).[19]

[19] CIRCA.AT: http://www.enisa.europa.eu/cert_inventory/pages/04_01.htm#02

British national cooperation (UKCERTS)

UKCERTS is an informal forum of UK CERT teams with participants from the government, academic, corporate and commercial CERTs. The forum has quarterly meetings of up to 25 members, with presentations provided by team members and invited information security experts. The forum is designed to encourage cooperation and information sharing between the participants. UK WARP teams also recently attended the meetings, enhancing the relationship between the UK CERT and WARP communities.[20]

Dutch national cooperation (o-IRT-o)

o-IRT-o stands for the Dutch name 'operationeel Incident Response Team overleg' (operational Incident Response Team meeting). This forum is initiated by GOVCERT.NL in 2002. At the moment 31 organisations are participating in o-IRT-o.

o-IRT-o is a group of incident handlers from the public and private sector in the Netherlands. Participants from the private sector are handlers at ISP's, banks, multi-national or industrial companies. From the public sector GOVCERT.NL is participating but also universities, employees from the national police force and the High-Tech Crime Center.

GOVCERT.NL facilitates this forum to stimulate the exchange of knowledge about various security- and incident-related topics like incidents, security-threat trends and best practices. Also, we would like to stimulate that incident handlers in the Netherlands know each other and that they can co-operate together during serious incidents.

Participants of o-IRT-o have signed a non-disclosure agreement. This agreement is signed on behalf of the person, not on behalf of the organisation where the participant works for.

[20] UKCERTS: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#08

German national cooperation (CERT-Verbund)

The German national CERT-Verbund is an alliance of German security and emergency response teams. The CERT-Verbund provides the German teams with a framework for cooperation and information sharing. Besides this, all the single teams stay autonomous in their responsibility for their respective constituency.

The CERT-Verbund has the following overall goals:

- Protection of the national IT-networks
- Immediate joint reaction to security incidents[21]

Polish national cooperation (Polish Abuse Forum)

Cooperation between Polish Security and Incident Response Teams known also as "Abuse-Forum" is an informal cooperation between security teams in Poland. The forum was initialised by the Research and Academic Computer Network in Poland (NASK[22]) and operating within NASKs CERT Polska[23] team. The forum meets quarterly and regularly more then 10 of the members are present. The main topics of discussion and activities are:

- Cooperation between forum teams and Law Enforcement Agencies (LEAs) in Poland
- Exchanging of experiences between the teams, especially related to the operation of a team within their company organisational structure and methods of contacting and cooperating with the teams' constituencies.
- The undertaking of technical actions in the teams' networks, with the goal of improving the security of the teams' parental organisations, as well as their customers.

[21] CERT-VERBUND: http://www.enisa.europa.eu/cert_inventory/pages/04_01.htm#01

[22] NASK: http://www.nask.pl

[23] CERT POLSKA: http://www.enisa.europa.eu/cert_inventory/pages/03_pl.htm

6.2 Regional Cooperation

CERT cooperation proved to be most effective within regions. This can be easily explained, as short travel times and overall relatively low costs stimulate more frequent personal meetings. Another important role plays the similarity of the cultural backgrounds of the participating teams which makes social networking easier and facilitates common projects. The longest standing and most mature regional cooperation initiatives are developed in Europe, but the Asia-Pacific region has progressed enormously since the establishment of APCERT in 2003. Lately, an initiative for regional cooperation has also emerged in South America.

6.2.1 Asia

As an initiative of JPCERT/CC, the leading CERTs from economies in the Asia Pacific region were invited to attend the first Asia-Pacific Security Incident Response Coordination (APSIRC) meeting in Japan in March 2002 to discuss improved working relationships between CERT neighbours across national borders.

A key outcome from this APSIRC meeting was the decision to form APCERT as the vehicle for regional cross border cooperation and information sharing. A working group was formed which used a consultative process to forge an agreement for the 15 CERT teams from the 12 Asia Pacific economies that agreed to establish APCERT.

In February 2003, the APCERT agreement was accepted by the attendees of the APSIRC meeting and elections were held for the positions of the steering committee, chairperson and secretariat. During the annual grand meeting (AGM) in Kyoto in February 2005, the position of the deputy chairperson was created and assigned.

Many of the goals and objectives of APSIRC firmly established and became the legacy upon which APCERT is built.

APCERT gave itself the following goals:

- maintain a trusted contact network of computer security experts in the Asia Pacific region to improve the region's awareness and competency in relation to computer security incidents through:
- enhance Asia Pacific regional and international cooperation on information security
- jointly develop measures to deal with large-scale or regional network security incidents
- facilitate information sharing and technology exchange, including information security, computer virus and malicious code among its members
- promote collaborative research and development on subjects of interest to its members

- assist other CERTs in the region to conduct efficient and effective computer emergency response
- provide input and/or recommendations to help address legal issues related to information security and emergency response across regional boundaries[24]

6.2.2 Europe

The history of European cooperation will be discussed later in a more detailed form. The understanding of how various initiatives developed, which ideas proved successful , which didn't and what lessons were learned gives a very good picture of the problems identified and solutions proposed in the next chapters.

The early days (1992-1995)

The very first CERT in Europe was established by the French Space Physics Analysis Network (SPAN) in 1990. Since SPAN was part of the NASA networks, the needs for IT and network security were recognised very early. Around 1992, along with the rising number of Internet-connected hosts, various European research networks also started to look at the CERT concept more closely. A working group organised by the Association of European Research Networks (RARE) had agreed that it would be beneficial to stimulate CERT development in the national research networks in each European country. As a result, some networks started individual projects to establish CERT teams for their constituencies. The first operational team was SURFnet CERT (formerly known as CERT NL), established by SURFnet – the Dutch research network, which became active already in 1992 and was shortly followed by DFN-CERT (the CERT for the German Research Network), which started operations in the beginning of 1993.

The RARE research on CERT co-ordination in Europe

In the years of 1993-1994 a research project was performed by the freshly built Réseaux Associés pour la Recherche Européene (RARE) CERT Task Force on needs for having a centralised European team to coordinate the efforts of individual CERTs. The final report from the project recommended, that coordinated incident response via a top-down approach. should be provided However, the report was rather unpopular and did not have much influence, among other things because the establishment of a centralised CERT for Europe would require additional funding and would possibly be seen as competition for individual teams in the countries.

During this time, most of the existing teams did establish with CERT/CC and with FIRST, but rarely cooperated with each other. In 1993, FIRST counted already seven members from Europe:

- Micro-Bit Virus Centre – a vendor team from Germany
- CCTA[25] from the United Kingdom

[24] APCERT: http://www.enisa.europa.eu/cert_inventory/pages/05_01.htm

[25] Central Computer and Telecommunications Agency: The British government centre for information services. As from 1st April 2001, CCTA became an integral part of the Office of Government Commerce.

- NORDUnet from Scandinavia
- CERT-NL (see above)
- DFN-CERT – a team of German National Research and Educational Network
- RARE CERT Task Force (see textbox above)
- RENATER – a team of French National Research and Educational Network

During the "Workshop for Security Incident Handling" in St. Louis (an event that later should evolve into the FIRST AGM), several European FIRST members agreed on the need of more cooperation and regular relationships between European teams, including non-FIRST members. In the late 1993 14 representatives of 10 European CERTs met in Amsterdam - for the first time outside of the United States. Two more meetings took place in 1994 in Hamburg and 1995 in Karlsruhe, attracting more and more teams (16 and 33 organisations were represented in 1994 and 1995 respectively).

EuroCERT

One of the conclusions of the meetings of European CERTs was a clear need for a European Coordination Centre for CERTs. In 1995, TERENA created a task force *CERTs in Europe* that analyzed the existing situation and constructed a coordination model to overcome its shortcomings. Following the recommendations of the task force, TERENA prepared a call for proposals to establish *Security Incident Response Coordination for Europe* (SIRCE). The contract was won by DANTE[26] and UKERNA[27] and the pilot was started in May 1997 under the name *EuroCERT* with very ambitious goals like providing a 24/7 incident coordination for participating teams, collecting and distributing information within a defined response time, providing real-time connection channels for CERTs and peer relationships with law enforcement agencies or teams from outside of Europe. EuroCERT was not aimed to be an incident response team itself, and the actual handling of security incidents would be done by each participating team individually, implying the hierarchical coordination environment.

[26] DANTE (Delivery of Advanced Network Technology to Europe) plans, builds and operates advanced networks for research and education. It is owned by European NRENs (national research and education networks), and works in partnership with them and in cooperation with the European Commission.; see: http://www.dante.net/

[27] UKERNA (United Kingdom Education and Research Networking Association) manages the operation and development of JANET (the network dedicated to the needs of education and research in the UK) on behalf of JISC (Joint Information Systems Committee) for the UK Further and Higher Education Funding Councils (http://www.ja.net/)

A brief history of EuroCERT

The EuroCERT was funded by TERENA with money collected from voluntaries wishing to participate and contribute to the project. Since TERENA was established for research and academic networks, all participants came from this area. It was expected however that commercial ISPs would join by the end of the pilot. The pilot did not work as well as expected. One of the problems was that with different set of services delivered by each team, it was very hard to define the scope of work for EuroCERT that would satisfy the needs of all sponsors without overlapping with work that others are already doing for their own constituencies. Other problems were caused by the need of acceptance of submission to an external authority, e.g. giving up direct personal links. The fact that Europe if a multinational and multicultural structure and that work of a CERT team within national research network would be coordinated with international EuroCERT which was an international entity did not make things any easier.

The EuroCERT services, and thus the project SIRCE itself ended in September 1999, two months before the scheduled date, due to lack of interest and funding.

(We would like to hereby acknowledge and appreciate comments received from people directly involved in the works of EuroCERT, namely: Andrew Cormack, Klaus-Peter Kossakowski, Damir Rajnovic and Don Stikvoort.)

Fig. 2. A (very) brief history of EuroCERT

At that time, European teams chose to take the path of cooperation and collaboration rather than coordination.

Cert-coord and TERENAs TF-CSIRT

After SIRCE ended prematurely in 1999, 27 individuals from 18 organisations in 15 countries involved in CERT co-ordination met in Amsterdam to discuss possible options to follow up the pilot phase. The group did not yet constitute any formal task force or working group; to identify this initiative, we will use the term *cert-coord*, coming from the name of the mailing list, which persisted even after a formal task force was established.

The following organisations (listed in alphabetical order) attended the first *cert-coord* meeting in Amsterdam:

- ARNES, Slovenia
- BELNET, Belgium
- CERN, Switzerland
- CERT-RENATER, France
- DANTE, United Kingdom
- ESCERT, Spain

- FCCN, Portugal
- FUNET-CERT, Finland
- GARR-CERT, Italy
- GRNET-CERT, Greece
- IRIS-CERT, Spain
- POL-34, Poland
- Secunet, Germany
- Stelvio, The Netherlands
- SURFnet (former CERT-NL), The Netherlands
- Telia Internet, Sweden
- TeliaCERT CC, Sweden
- TERENA, The Netherlands
- UKERNA, United Kingdom
- UNINETT, Norway

The results from the EuroCERT project made clear that it would not be possible to establish a permanent operational European CERT co-ordination service in the next couple of years, due to different interests and needs of various networks in Europe and their CERT teams. The group therefore decided to give up fields of mostly operational nature, such as co-ordination of incident handling and emergency back-up for CERTs. However, certain areas were identified to be in common interest and yield an area for further cooperation and development[28]:

- **Sharing of statistics** - As most teams would not be able to share full incident data (mainly due to data protection provisions) it was agreed that it would be beneficial to share statistical data like the numbers of incidents in different classes. With this data put together it would be possible to observe current trends. This task would require development and implementation of common classification scheme between different teams.
- **Development of an accreditation scheme** – The group looked for an authority to delegate trust brokerage. Different ideas were raised, including the building of a European accreditation scheme within FIRST.
- **Education and training** – For the time being everyone was encouraged to gather and produce educational material and make it available to other teams.
- **Assistance to new teams** – This task was considered crucial for successful IT and network security. Experienced teams should provide guidance and disseminate best practice to new teams in forms including site visits, tutorials and identifying expert able to fulfil the needs of new teams.
- **Providing a clearinghouse for tools and software**
- **Add security contact information** to the RIPE NCC database

There were another two cert-coord meetings in the following year, the last one was held in Vienna in May, 2000, where the group decided to continue its activities as a task force of TERENA: the hour of birth for TF-CSIRT!..

[28] The minutes from the 1st *Meeting to Discuss Future Collaborative Activities between CERTs in Europe* can be found at http://www.terena.nl/activities/tf-csirt/pre-meeting1/minutes.pdf

The first TF-CSIRT meeting was held in Paris and was attended by 40 people. Since then, the group has met every three months in various European locations[29]. From the beginning the TF-CSIRT is a group of individuals not organisations with very loose membership restrictions. The task force clearly defines its goals within the terms of reference which are renewed every two years. Working groups are called as needed to carry out work for individual goals.

The examples given below describe how TF-CSIRT has addressed the goals defined by cert-coord:

[29] The 19th meeting in Espoo, Finland (September 2006) attracted 84 people.

Development of an European accreditation scheme	**The** Trusted Introducer (TI) **service was piloted and, after the pilot-phase, successfully established. Since then the number of accredited teams grows steadily.**[30]
Education and training	TRANSITS **– a major European project was carried out by TERENA and several task force members to promote the establishment of CERTs and the enhancement of existing CERTs by addressing the problem of the shortage of skilled CERT staff. This goal has been addressed by providing specialist training courses to train staff of (new) CERTs in the organisational, operational, technical, market and legal issues involved in providing CERT services. The lifetime of the TRANSITS project was from 1 July 2002 until 30 September 2005, during which 7 workshops were organised and over 150 current or future CERT employees were trained. TERENA and FIRST have joined forces to organise further training workshops in Europe after the end of the project. Since march 2006 the courses in Europe are sponsored by ENISA. Also, the training materials produced during the project are available to anyone who wishes to organise training provided certain conditions are met**[31]**.**
Information and assistance for new teams	Best practice **documents have been gathered in a starter kit**[32]**. Task force members are also willing to help any team that is seeking guidelines on ad hoc basis (mentoring**[33]**).**
Clearinghouse for tools and software	**A Clearing House for Incident Handling Tools** (CHIHT) **was established based on input from teams that recommended software they use in their everyday work**[34]**.**
Security information in the RIPE NCC database	**A new type of object (IRT object**[35]**) was introduced in RIPE NCC database to hold information about CERTs thanks to works carried out by members of the TF-CSIRT. Also, Trusted Introducer is carrying out the process of record creation for accredited teams.**

Fig. 3. Goals achieved by TF-CSIRT

[30] Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[31] TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11

[32] CSIRT Starter Kit: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#06

[33] CSIRT Mentoring Scheme: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#05

[34] CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[35] IRT Object: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

From within TF-CSIRT a couple of other cooperation activities out of various reasons with various goals have been started and carried out by TF-CSIRT members. The following paragraphs shortly describe the most important ones.

IODEF

Many members of the TF-CSIRT were involved in the creation of a standardised format to exchange incident information. The proposed XML-based format called IODEF (Incident Object Description and Exchange Format) has not yet been widely adopted, mostly due to lack of tools and different set of information used across teams. Alas, the eCSIRT.net project (see next paragraph) made an effort to transfer IODEF into a usable standard.[36]

ECSIRT.NET

The eighteen month EU funded project eCSIRT.net was carried out between July 2002 to December 2003 with the main goals to research a possibility of common incident handling and information sharing between teams in Europe. It was conducted by a consortium of nine partners: JANET CERT (UK), CERT Polska (PL), CERT Renater (FR), IRIS-CERT (ES), DFN-CERT (DE), GARR-CERT (IT), CERT-DK (DK), Stelvio (NL) and PRE-Secure (DE) and two liaisons: CERT-NL (NL) and JP-CERT (JP). Various aspects of cooperation were investigated:

- For the purpose of incident data exchange, the use of IODEF was investigated but was discarded due to reasons given above
- To create common set of statistics, certain numerical data on a very general level (such as number of handled incidents) was shared among the teams. The biggest problem identified was that different teams use different taxonomies and classification schemes. To address this issue, a common classification scheme was proposed, but it was not widely adopted.
- A network of IDS sensors was built with a central server, allowing teams to correlate alerts generated for their networks with information from others.
- To facilitate communication between teams and allow for secure and reliable channels for the distribution of alerts, a couple of dedicated services were established. These services included a web form and an encrypted mail server as well as a voice mailbox for out-of-band communication. After the project has finished, the services are now provided to accredited teams by the TI service[37].

[36] IODEF: http://www.enisa.europa.eu/cert_inventory/pages/04_03_01.htm#04

[37] Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

Request Tracker for Incident Response (RTIR)

Several teams represented in the task force have decided to work cooperatively on the development of an incident handling tool[38]. On behalf of those teams, TERENA has signed a two-year contract to fund this software with a commercial software developer. Teams who participate in the cost have specified the requirements for the software and commit their time to test and verify delivered functionalities[39].

NORDUnet CERT

One of the regional CERT initiatives that aims at better co-ordination of incident handling and cooperation among Northern European countries is NORDUnet CERT. NORDUnet CERT performs security incident handling in cooperation with the Nordic national research networks. As NORDUnet (http://www.nordu.net/) is the Nordic Internet highway to research and education networks in Denmark, Finland, Iceland, Norway and Sweden, NORDUnet CERT fulfils the co-ordination role for:

- DK-CERT, (Denmark)
- RHnet CERT, (Iceland)
- FUNET CERT, (Finland)
- Uninett CERT, (Norway)
- SUNET CERT, (Sweden)

The constituency of NORDUnet CERT is therefore the members of the Nordic academic networks.

NORDUnet CERT stresses in their presentations[40] that when dealing with network security incidents cooperation with other parties is a necessary success criterion.

[38] Following teams are contributing to development of RTIR: Janet CERT (UK), ACOnet-CERT (AT), LITNET CERT (LT), CERT Polska (PL), SWITCH-CERT (CH), IRIS-CERT (ES), FCCN/CERT.PT (PT), SUNet CERT (SE), GOVCERT.NL (NL)

[39] RTIR: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#09

[40] NORDUnet presentation: http://www.nordunet2002.dk/powerpoint/a_per_arne_anstad.pdf

As key elements for successful cooperation, NORDUnet CERT perceives:

- Co-ordination
- Trust
- Organisation

Each of the CERTs listed above operates in its own country and is independent in operation and can be a member of international organisations (TERENA TF-CSIRT, FIRST). Nevertheless, those teams have established a network of peers which is also a "web of trust". Thus the trust model in this case is based on a strong cooperation between all Nordic networks (under of an umbrella of NORDUNET). Organisation of a NORDUnet CERT consists of one single point of contact and procedures for information handover based on web of trust mentioned before. NORDUnet CERT plays also a role in international contacts since it is a member of FIRST and TF-CSIRT[41].

6.2.3 South America

The development of cooperation among CERTs in the region of South America and the Caribbean took a path similar to that in European. CLARA (Cooperation of Advanced Networks in Latin America[42]) has established a working group to address security issues. The group is focusing on two main areas:

- The protection of the critical infrastructure of REDClara – the network connecting Latin America NRENs with each other and Europe
- The creation of security working groups in the NRENs

The second field is currently addressed with TRANSITS trainings and security workshops co-organised by FIRST.

Like TERENAs TF-CSIRT, the CLARA WG-CSIRT has well-defined goals:

- To establish a work framework, in terms of security, for each NREN
- To promote the development of new working groups dealing with security in Latin America and the region through training programs aimed at working group members
- To establish discussion fora to exchange ideas, knowledge and experiences within the field of computer security, attention to incidents, etc.

[41] NORDUNET: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#05

[42] RedCLARA: http://www.redclara.net/

- To promote the exchange of data and information on related problems, incident management, etc.
- To promote coordinated and prompt reactions for security incidents occurring on REDClaras infrastructure and that of each NREN.
- To create documents of best practices focused on academic environments
- To build a data base of contact points responsible for security in each NREN
- To cooperate with similar initiatives, such as TF-CSIRT and APCERT

6.2.4 North America

In the United States, the nation with the biggest number of existing CERTs, US-CERT (United States Computer Emergency Readiness Team), with the support of the CERT/CC team, has organised several meetings that were called *North American CSIRT Meeting*. These meetings brought together CSIRTs from product vendors, security vendors, service providers, industry, academia, and government. It was limited to CERTs in the United States. This group is informal and there is no charter or formal structure.

The United States government has also worked with the sector information sharing and analysis centres (ISACs), and hosted a couple of meetings. These meetings are limited to organisations dealing with the protection of critical national infrastructure (electricity, transportation, telecommunications, etc.).

The Information Technology Information Sharing and Analysis Centre (IT-ISAC) is a trusted community of security specialists from companies across the Information Technology industry dedicated to protecting the Information Technology infrastructure that propels today's global economy by identifying threats and vulnerabilities to the infrastructure, and sharing best practices on how to quickly and properly address them. The IT-ISAC also communicates with other sector specific ISACs, enabling members to understand physical threats, in addition to cyber threats. Taken together, these services provide members a current and coherent picture of the security of the IT infrastructure.

The mission of IT-ISAC is to:

- Report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures,
- Establish a mechanism for systematic and protected exchange and coordination of such information; and

- Provide thought leadership to policymakers on cyber security and information sharing issues[43].

6.3 International cooperation

Successful cooperation among CERT/CSIRT or Abuse Teams located in different countries in many regions is a key factor for successful incident handling due to the global character of the Internet and security threat propagation. But also many other CERT services are strongly dependent on collaboration with other teams from different parts of the world. In this chapter the history and role of the Forum of Incident Response and Security Teams (FIRST) in building the international community of CERTs is presented (with a look at Special Interests Groups within this forum), as well as some examples of sector cooperation (for example among governmental CERTs) and cooperation initiatives among Abuse Teams. Since it appears that an increasingly important element of international collaboration is cross-regional cooperation, two examples are presented below: region to region cooperation (for example Europe – Asia Pacific) and cooperation among member states from two different regions in the same organisation.

6.3.1 FIRST (Forum of Incident Response and Security Teams)

In August 1989 an invitational workshop was organised by the CERT/CC to discuss not only what was learned during the first year of operation but also what the next steps were in coordinating relationships between the existing teams. This became the first event drawing practitioners from the field.

In October 1989 a worm called WANK attacked the Internet, at that time consisting of approximately 170,000 hosts. Three teams coordinated their activities to provide response to this worm: the Department of Energy's Computer Incident Advisory Capability (CIAC), the NASA Space Physics Analysis Network and the CERT/CC. Various warnings were released from both CIAC and CERT/CC that were helpful to the Internet community, even though many administrators did not heed the warnings and were infected by a variant of the WANK worm called OILZ released two weeks later.

After this example of successful collaboration between teams, more discussions ensued on how to set up a response team network. During a 1990 workshop by NIST and CERT/CC, a panel session presented and discussed the ideas for such a network. The discussions established goals for future collaboration. These goals were to share information among CERTs and, if needed, to aid one another during incidents and network-wide attacks. The CERT community is still pursuing these goals today.

After the workshop, further discussion brought 11 founding members (including one from France) together in November 1990 to establish a forum for CERTs and security teams, which is now known as the Forum of Incident Response and Security Teams (FIRST). At this time, the Internet had approximately 340,000 hosts.

[43] IT-ISAC: http://www.it-isac.org/

Initial members

Below a list of founding FIRST members in alphabetical order:

- Air Force Computer Emergency Response Team (AFCERT)
- CERT Coordination Center
- Defense Communication Agency/Defense Data Network
- Department of the Army Response Team
- Department of Energy's Computer Incident Advisory Capability
- (CIAC), Lawrence Livermore National Laboratory
- Goddard Space Flight Center
- NASA Ames Research Center Computer Network Security Response
- Team (NASA ARC CNSRT)
- NASA Space Physics Analysis Network (SPAN CERT)
- Naval Computer Incident Response Team (NAVCIRT)
- National Institute of Standards and Technology Computer Security
- Resource and Response Center (CSRC)
- SPAN-France

Status quo

The current mission statement of FIRST is:

- FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.
- FIRST members develop and share technical information, tools, methodologies, processes and best practices
- FIRST encourages and promotes the development of quality security products, policies & services
- FIRST develops and promulgates best computer security practices
- FIRST promotes the creation and expansion of Incident Response teams and membership from organisations from around the world
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment.

Each year FIRST has continued to grow, and now (November 2006) 184 organisations are participating members.

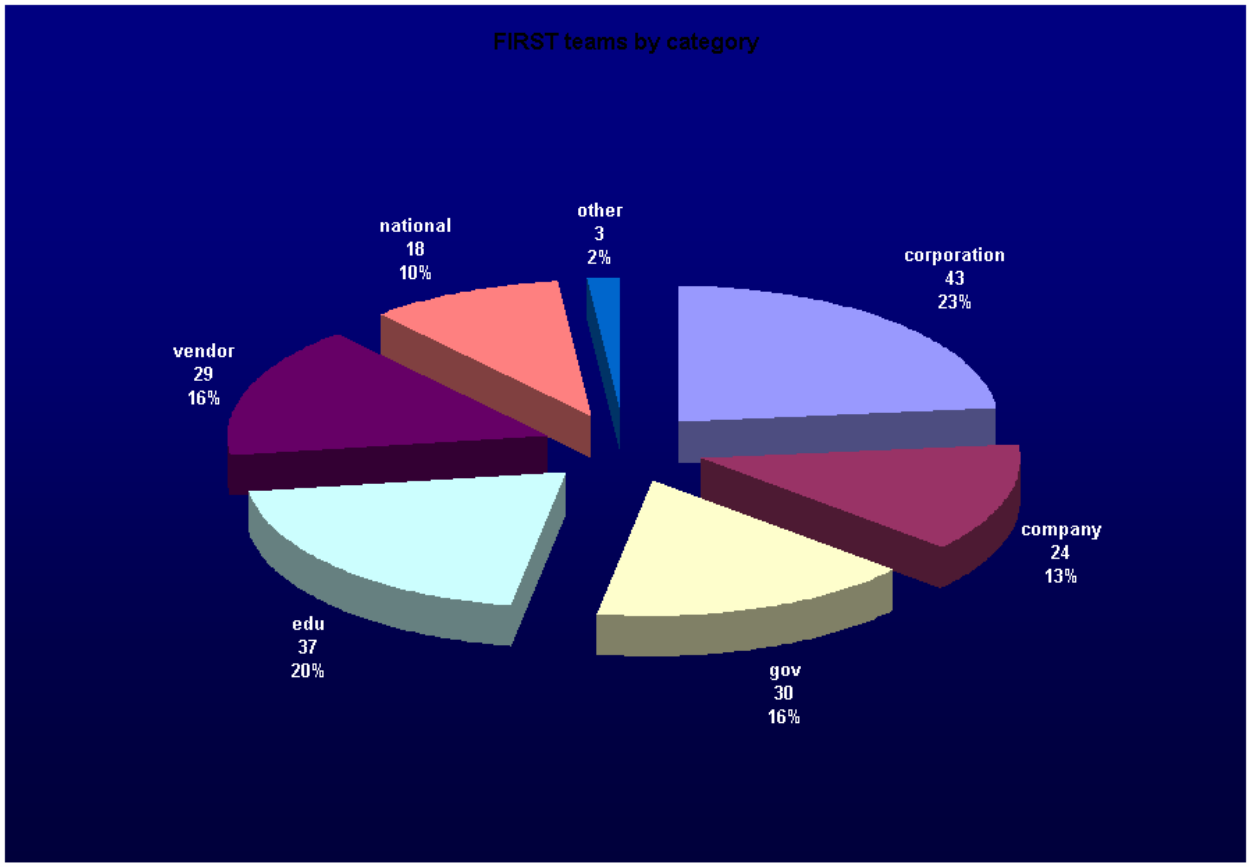


Fig. 4. FIRST teams by category (November 2006)

Bodies

The steering committee, designated committees, and the secretariat provide the general coordination of FIRST activities. The steering committee may establish an advisory board to seek strategic guidance and advice. The steering committee is responsible for general operating policy, procedures, and related matters affecting the FIRST as a whole.

The initial steering committee consisted of one representative of each of the initial CERTs listed above. Five of those original steering committee members were chosen at random to serve until the second general meeting; the remaining members served until the first general meeting. After the first general meeting, the steering committee comprised ten individuals serving on two-year terms.

The individuals for the one-half of the steering committee positions are elected at each annual general meeting. A candidate must be nominated by petition of at least six FIRST members. A FIRST member may vote for no more than the number of open positions. The five candidates receiving the most votes become members of the steering committee.

The steering committee elects from its membership a chair to serve a term of one year. A person may not serve as chair for more than two consecutive terms.

The FIRST steering committee establishes standing (permanent) and ad-hoc (temporary) committees in order to better achieve FIRST goals. The steering committee appoints the membership and chair of such committees and shall determine their operating procedures.

Currently there are two permanent committees and two temporary committees. The permanent committees are membership committee and editorial committee. The membership committee was established in 2003 to review current policies, standards, and procedures for the acceptance, review and approval of membership applications, for the suspension and removal of existing members. It reports its recommendations to the Steering Committee. The editorial committee, also established in 2003, has the main goal to issue FIRST newsletter.

The first one of the temporary committees, the education committee, was established in June 2004. The mission of the education committee is to ensure that high-quality, affordable education and training is available to those who wish to create or operate incident response teams that further support the goals and objectives of FIRST. This mission derives directly from the FIRST mission statement. This committee makes use of results of other examples of cooperation. It collaborates with regional initiatives and uses the TRANSITS project materials. The last committee, the program committee, has the goal to prepare the program of the annual FIRST conference.

It is worth to note some significant points describing the operation of FIRST:

- The Annual FIRST conference together with the Annual General Meeting have become the main organisation's event
- FIRST Technical Colloquies (TC) have become the primary meeting points for team members and other technical specialists. They provide a discussion forum to share information about vulnerabilities, incidents, tools and all other issues that affect the operation of incident response and security teams
- The liaison membership formula turned out to be useful. Every year the number of individuals, who are FIRST members increases[44]. It is a good solution for those who have terminated their membership in teams that are FIRST members
- FIRST is recognised as a world level partner for discussion about security and safety of information society. For example a FIRST representative was invited to participate in the world summit on the information society in Tunis in 2005
- For the last couple of years the organisation is very active in the field of security awareness. The main tool of this activity is the website based newsroom[45].
- FIRST has become actively involved in security trainings. Trainings mainly focus on the establishment of new CERT teams. To achieve the best results, the "Train the trainers" formula was developed
- FIRST tries to develop its activity by introducing new programs. On the technical and operational field the SIG idea was developed (see chapter *6.3.2 Sector cooperation*). On the executive level the Corporate Executive Programme (CEP) was developed. The aim

[44] FIRST liaison members: http://www.first.org/members/liaisons/

[45] FIRST newsroom: https://members.first.org/newsroom/index.html

of the CEP is to bring together cross-functional senior executives who are responsible for decision-making in their organisations[46].

- For better coordination and to give members a chance to participate more often in the organisation's meetings, a closer coordination with regional forums was established. For example the collocation of FIRST TCs and TF-CSIRT meetings proved to be very successful.

6.3.2 Sector Cooperation

Another incentive to cooperate is the similarity of the sectors a CERT operates in. A sector (as explained in *chapter 4*) is mainly defined by the type of constituency, but also by the responsibility a specific CERT has. Some teams associate and start closer cooperation because of their common area of interest, such as work in the same or similar type of environment. This kind of cooperation exists in the public as well as in the private sector.

European Government CERT group (EGC)

The European Government CSIRTs group (EGC) is an informal group of governmental CERTs that is developing effective cooperation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CERTs in Europe.

To achieve this goal, the ECG group members will:

- Jointly develop measures to deal with large-scale or regional network security incidents
- Facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities
- Identify areas of specialist knowledge and expertise that could be shared within the group
- Identify areas of collaborative research and development on subjects of mutual interest
- Encourage formation of government CERTs in European countries
- Communicate common views with other initiatives and organisations.

Current members of the European Government CSIRTs group:

- CERTA – France
- CERT-Bund – Germany
- CERT-FI – Finland

[46] FIRST CEP programme: http://www.first.org/global/cep/

- GOVCERT.NL – The Netherlands
- SITIC – Sweden
- UNIRAS – United Kingom
- NorCERT – Norway
- SWITCH CERT - Switzerland[47]

FIRST Special Interest Groups (SIGs)

FIRST SIGs are a very good example of a tighter form of cooperation within an existing cooperation forum. This tightening is built on the common area of interest, e.g network monitoring, vulnerability handling, artifact analysis etc.

The SIGs exist to provide a forum where FIRST Members can discuss topics of common interest to the incident response community. A SIG is a group of individuals composed of FIRST Members and invited parties, typically coming together to explore an area of interest or specific technology area, with a goal of collaborating and sharing expertise and experiences to address common challenges.

SIGs define their own missions and goals, and serve as a forum for its members to discuss technologies, challenges and solutions in specific areas of mutual interest, including hearing relevant presentations from SIG participants and invited guests. SIGs are free to build their own meeting schedule but are also encouraged to co-locate meetings with FIRST Conferences, Technical Colloquia or other events.[48]

Abuse Handling SIG (AH-SIG)

The mission of this SIG is to improve abuse handling on the Internet, by bringing together abuse teams worldwide, encouraging the exchange of experiences and developing of best practices.

Abuse is considered to be any undesired use of the Internet, such as viruses, spam, phishing or botnets (the list of topics is not restricted to messaging). The focus of the efforts will be large scale, where often dedicated abuse teams work independent of CERT teams.

Artifact Analysis SIG (AA-SIG)

The mission of this SIG is to improve artifact analysis capability within the FIRST community. Its members want to:

- Foster the adoption and development of artifact analysis capabilities within the FIRST community.
- Encourage developing and evolving policies related to artifact collection, handling, analysis, and sharing.

---

[47] EGC: http://www.enisa.europa.eu/cert_inventory/pages/04_01_01.htm#04

[48] FIRST SIGs: http://www.first.org/global/sigs/

- Encourage understanding of the international legal environment relating to artifact analysis.
- Encourage technical exchange of artifact analysis methodologies and practices.
- Encourage to develop of the best practices for the artifact analysis.

Artifacts in this case are leftovers from computer security incidents. Find a more comprehensive explanation of artifact analysis in the CSIRT handbook from the CERT/CC[49].

Common Vulnerability Scoring System SIG (CVSS SIG)

The mission of this SIG is the promotion of the CVSS standard. It is the result of the fact that FIRST was chosen to be the custodian of the Common Vulnerability Scoring System (CVSS). The objectives of this SIG are the following:

- Promote and educate the information technology community on the benefits of using a common scoring system framework to describe the severity of computer security vulnerabilities replacing vendor-specific severity rating systems
- Foster cooperation among information technology constituents in the effective implementation and testing of the Common Vulnerability Scoring System framework
- Provide a means for the communication of the CVSS Vendor Base and/or Temporal scoring information on published vulnerabilities
- Support the actions and activities of FIRSTs CVSS Committee including research, software development and operational activities
- Facilitate the sharing of CVSS-related information, tools, and techniques.[50]

FIRST Internet Infrastructure Vendors SIG (Vendor SIG)

The goal of this SIG is to provide a forum for Internet infrastructure vendors. In this context Internet infrastructure is considered to be operating systems, computer hardware, networking equipment and and other critical applications (this list is by no means exhaustive nor comprehensive).

In order to become member an applicant must be recognised by at least, two existing members. Forum moderators have a final word in all matters regarding this SIG. Membership in FIRST is not required to become a member of SIGIIV.

FIRST Law Enforcement / CSIRT Cooperation SIG (LECC SIG)

The mission of this SIG is to facilitate further cooperation between incident response and law enforcement agencies, by the development of better understanding of organisational missions and specific requirements and producing practical trust and information-sharing protocols.

---

[49] CSIRT handbook: http://www.cert.org/archive/pdf/csirt-handbook.pdf

[50] CVSS: http://www.first.org/cvss/intro/

Network Monitoring SIG (NM-SIG)

The mission of this SIG is to advocate, develop and promote knowledge and techniques for collection and analysis of network sensor and monitoring data to build the capabilities of CERTs to quantify and measure malicious activity on networks in order to create more secure systems.

6.3.3 Cooperation among Abuse Teams

Abuse teams handle large numbers of incidents of similar nature, for example spam, zombie networks or copyright infringements. Most of these incidents are limited in scope to customers of an ISP, which the abuse team is a part of. As a consequence, it seems that abuse teams would not have much need of coordination or operational cooperation. There is however a lot of benefit from cooperation in sharing of knowledge and experience as many abuse teams encounter similar obstacles. The most disputed subjects between abuse teams are:

- fighting unwanted mass messages
- blacklisting
- cleaning and preventing zombie infections
- cooperation with government and Law Enforcement Authorities

Many CERT-teams also handle abuse cases, but most of them do not do it on the large scale that for example the telco-company ISPs have to do. The latter also usually have both abuse-teams *and* CERT-teams, who operate independently.

MAAWG

The Messaging Anti-Abuse Working Group is a global organisation focusing on preserving electronic messaging from online exploits and abuse with the goal of enhancing user trust and confidence, while ensuring the deliverability of legitimate messages. With a broad base of Internet Service Providers (ISPs) and network operators representing over 600 million mailboxes, key technology providers and senders, MAAWG works to address messaging abuse by focusing on technology, industry collaboration and public policy initiatives. The purpose of MAAWG is to bring the messaging industry together to work collaboratively and successfully address forms of messaging abuse such as messaging spam, virus attacks, denial-of-service attacks, and other forms of abuse. To accomplish this, MAAWG is developing initiatives in the three areas needed to resolve the messaging abuse problem: Collaboration, Technology, and Public Policy. Goals of MAAWG include:

- development of an ISP code of conduct
- development and sharing of industry best practices
- developing a trusted inter-carrier network for messaging
- defining a reference architecture and network standards for combating messaging abuse
- building effective interfaces to key standards and legislative bodies

Currently MAAWG has over 80 members representing many areas of telecommunication industry, for example security solutions vendors, ISPs, e-mail service providers[51].

The purpose of MAAWG is to bring the messaging industry together to work collaboratively and successfully address forms of messaging abuse such as messaging spam, virus attacks, denial-of-service attacks, and other forms of abuse. To accomplish this, MAAWG is developing initiatives in the three areas needed to resolve the messaging abuse problem: Collaboration, Technology, and Public Policy.

E-CoAT

E-CoAT (European Cooperation of Abuse Teams) is intended for all those who professionally handle (or have a legitimate and significant interest in) "Internet-abuse" reports or complaints, with a team of people, on a relatively large scale. By that we really mean what is usually referred to as "abuse-teams" or CERT-teams of ISPs that also deal with "Internet abuse" on a large scale. E-CoAT concentrates its efforts on Europe, for pragmatical reasons.

E-CoAT cooperates closely with TF-CSIRT. It liaises with FIRST, with MAAWG (a global messaging abuse forum), and with other fora. Thus far E-CoAT has organised 4 workshops, between January 2004 and now[52].

6.3.4 Cross-regional cooperation

There are examples of cross-regional cooperation between different teams and organisations. Usually such cooperation is based on the exchanging of knowledge and experience at meetings. Representatives from different regional forums are asked to present their ideas of cooperation to the members of different forums.

TERENA TF-CSIRT – APCERT Memorandum of Understanding

There is one example of closer continuous cooperation between two regional forums. On the 28th of June 2005 in Singapore (during the FIRST conference) representatives of APCERT and TF-CSIRT signed a “Memorandum of Understanding” between the two associations. The document says that both sides recognise each other as regional expert bodies, are interested in establishing a channel of information exchange and constant usage of it, and that they are going to establish a framework for joint projects, especially with a wider global scope, and establish direct operational contact points. Of course both forums retain their full independence. For the text of the MoU between TF-CSIRT and APCERT see Annex I).

Collaboration of CERTs with National Responsibility

Another example of cross-regional cooperation is based on a proposal by the CERT Coordination Centre, to form an interest group consisting of CERTs from different countries around the world operating on national level or with national responsibilities. This cooperation is based on the fact that such teams face unique issues and it is valuable to exchange knowledge

[51] Full list of MAAWG members is available at http://www.maawg.org/about/roster/

[52] E-COAT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_01.htm#03

and experiences. 37 different CERTs were identified as CERTs with national responsibility[53] 17 of them participated in the first meeting organised by the CERT CC in Pittsburgh in July 2006. Besides an opportunity to learn a lot about the experiences of others, such cooperation is probably (it is too early to fully assess) a very good platform for establishing and building peer-to-peer relations or small cooperation groups between teams with common interests[54].

CEENET Central Eastern and European Network Association

The Central and Eastern European Networking Association (CEENet) is an association of national organisations, which focus on academic, research and educational networking. CEENet membership comprises of 23 national research and education networks from the following countries: Albania, Armenia, Austria, Azerbaijan, Bulgaria, Croatia, Czech Republic, Estonia, Georgia, Greece, Hungary, Latvia, Lithuania, Macedonia, Moldova, Poland, Romania, Russia, Serbia and Montenegro, Slovenia, Slovakia, Turkey and Uzbekistan. As one can see even though the name suggests only inter-European cooperation there are some adjacent members from Asia region: CEENet in practise acts as a cross-regional initiative.

The primary mission of CEENet is to co-ordinate the international aspects of the academic, research and education networks in Central and Eastern Europe and in adjacent countries. This co-ordination has lately spread to the computer network security area. Since there are substantial differences in ICT development among members of this organisation, sharing of information between those countries is a key element to achieve acceptable average level of ICT security across the whole region. The CEENet community is planning to establish a network of cooperation between CERTs once CERTs in CEENet countries are established[55].

[53] CSIRTs with national responsibility: http://www.cert.org/csirts/national/contact.html

[54] National CSIRTs initiative: http://www.cert.org/csirts/national/

[55] CEENET: http://www.ceenet.org/

7 Analysis and evaluation of the status quo

To understand the role of cooperation among CERT/CSIRT teams in the process of enhancing effectiveness of combating threats, vulnerabilities and security incidents it is necessary to first discuss the benefits of such a cooperation as an important factor in improving services offered by CERTs, and after that the barriers that can slow down this process. Further on, there is a question to be answered: Who are (or could be) the relevant stakeholders of CERT cooperation that potentially can facilitate it? In this chapter a short analysis of the status quo in order to assess benefits and barriers of CERT cooperation is performed and also some models of trust between involved parties are discussed. Several types of relevant stakeholders facilitating this cooperation have been identified and are listed as well. At the end of this chapter a (very brief) evaluation of the most important cooperation initiatives has been done taking into account two main aspects: what has already been achieve and what chances for the future appear for those initiatives.

7.1 Benefits of cooperation

A statement that cooperation is a benefit for all sides is a truism. Thus, specific kinds of cooperation, in close relation to the CERT operation, should be analyzed.

For the purpose of this document, four main areas of benefits were identified:

- **Incident handling**
- **Project conducting**
- **Resource- and information sharing**
- **(Social) networking**

7.1.1 Benefits related to common incident handling

The number of years of cooperation between CERTs has shown that probably one of the most important benefits resulting from CERT cooperation is the enhancement of incident handling. Since incidents reported to CERTs are international – there is practically no chance for effective incident handling without good cooperation between all involved sides. The information exchanged during the incident handling process is in most cases of very sensitive nature. Incident reports contain data about activities of internet underground groups, successfully attacked organisations, plans of internet criminals, detailed analysis of malicious code, electronic evidence etc. Exchanging this data in a secure way and the promptness of reaction and quality of the provided information are very important during the incident handling process. If we agree on the mentioned correlation then we understand the benefit of the cooperation. Long term and effective exchanging of incident data can result in the setting up a regular exchange of incidents related to the constituencies of cooperating CERTs. This can lead to a big improvement of the quality of the incident handling process and significant reduction of workload of CERTs, especially if a common set of rules for incident handling can be established.

7.1.2 Benefits related to common project conducting

Incident handling is the core daily work of CERTs. Another example of positive result of cooperation is the conduction of joint projects. Experience shows that cooperation between CERTs gives them the capability to better recognise their common areas of interest, their competence, their goals and also a chance of building trust. Based on this recognition some teams embarked on closer cooperation. This cooperation might be a part of an already established, ongoing project or it might be a completely new project. A good example of closer cooperation is the eCSIRT.net project[56]. The seven European CERT teams, which were members of the project consortium, were also members of the same cooperation forum (TERENA TF-CSIRT), all reached a higher level of a trust (all are Accredited Teams within Trusted Introducer Initiative) and all operate in similar sectors.

There are also examples of smaller and not strictly formalised cooperation. Teams work together on similar problems related to their projects. They exchange ideas, solutions or even source code.

7.1.3 Benefits related to resource- and information sharing

It is worth to relate information sharing to the particular kind of resources and services provided by CERTs.

Below are listed different kinds of resources that can be shared by CERTs and the related benefits. The term “information sharing” was treated very widely to show different kinds of activities that it can be applied to.

Knowledge and experience sharing – regular, formal or informal, exchange of information about issues related to IT security. It can be provided on request or by regular delivery of information (for example daily report from team’s observations and technology watch). Usually such sharing bases on team-team and association cooperation models or within an existing forum. It gives teams a chance to compare their knowledge and make a use of better experience and knowledge of other teams in the areas, which they want to operate in, but can not (for example due to lack of resources) develop their own procedures.

Staff exchange – a method of exchanging information and experience by exchange of personnel. This method is also used for mentoring new teams of organisations that just started with the process of establishing a CERT. Short site visits (for example during the sponsorship process for new teams that want to join FIRST) also fall into this category. Even though this method is not often applied in practice, the potential benefits it provides are very valuable. Through such exchange team staff can learn in detail about methods of daily work, procedures and techniques used to provide CERT services. By this they also get a feeling for coherences that are difficult to explain and therefore do not find their way into manuals and handbooks.

Technology sharing – by technology sharing CERTs give each other an opportunity of direct usage of concrete technical solutions which can significantly improve the quality of the services which a particular team provides. A good example of such sharing is the process of making available information about techniques and software used by teams, including the actual

[56] eCSIRT.net: http://www.ecsirt.net

software itself (for example Request Tracker for Incident Response as the enhanced version of Request Tracker, made available by JANET CERT to other CERT teams, or the CHIHT – Clearing House for Incident Handling Tools – where different teams share their knowledge and software which they use daily[57] or the joint development of new tools like the RTIR group within TF-CSIRT does[58]. Benefits of technology sharing include: access to well developed and verified incident handling and security tools, support in the resolving of a technology related problems and support in technical analysis of incidents (especially malicious code analysis).

7.1.4 Benefits related to (social) networking

Social networking is a crucial factor for building trusted relationships between CERTs. Besides the planned and well organised meetings, workshops, conferences, regular exchange of information (for example via mailing lists), there is a great benefit resulting from the simple fact that people gather in one place and have an opportunity to talk to each other and to get to know each other better. In effect, they learn about their business more and more and they find areas of common interest in the most convenient and effective way. Very often this is a first step to a closer and more formal cooperation between teams.

7.2 Influence of cooperation on CERTs services improvement

The matrix below presents the relation between a set of CERT services and the influence of cooperation on performance increase and improvement of those services. The list of services is based on the list provided by CERT Coordination Centre[59] We shortened this list by merging some categories and representing them by one that relates to the cooperation issues the most (like *Technology Watch* that here represents also *Announcements* and *Security-related information dissemination*). The statements made in this matrix are estimations based on the expertise of the authors of this document and are aimed to initiate and foster further discussion.

[57] CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[58] RTIR: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#09

[59] CSIRT services: http://www.cert.org./csirts/services.html

Services / influence of cooperation	Low	Medium	High
Alerts and Warnings	▲		▲
Incident Handling		▲	▲
Vulnerability Handling	▲	▲	
Artifact Handling	▲	▲	
Technology Watch[60]			▲▲
Configuration and Maintenance of Security Tools	▲▲		
Development of Security Tools		▲▲	
Intrusion Detection Services[61]	▲	▲	
Risk Analysis	▲▲		
Awareness Building		▲▲	
Education/Training		▲▲	
Product Evaluation and Certification		▲▲	

Fig. 5. Matrix of estimated relations between cooperation and quality of CERT services

▲ Potential position with well-developed cooperation

▲ Current position

Many services can benefit a lot more from cooperation than in the current status quo. For example, alerting and warning could be much more effective with a common format of advisories used by different vendors and common standards of threat assessment. The latter is already addressed by CVSS which is slowly getting accepted and is put in use by vendors[62]. On the other hand, various initiatives to deploy a common advisory format (the DAF (German advisory format) Format[63], CAIF[64] and VEDEF[65] to name only a few) have failed so far to be widely accepted. Same goes for IODEF, a standard which was designed to improve communication and facilitate incident handling did not manage to reach a "critical mass" of adopters sufficient to actually influence ways of handling incidents. All these standards were publicly promoted before

[60] Including observation of trends and phenomena

[61] Including early warning services

[62] CVSS: http://www.first.org/cvss/intro/

[63] DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

[64] CAIF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#01

[65] VEDEF/SECDEF: http://www.enisa.europa.eu/cert_inventory/pages/04_03_01.htm#05

reaching maturity, which greatly affected the possibility of their adoption. Potential adopters would not put efforts into implementation of immature standards, especially when very few tools were readily available to integrate with existing solutions. An example of a standard with a (partial) success story behind is the IRT object in the RIPE database[66]. The standard was ready to be used by CERTs immediately after being implemented by RIPE. Some very good guides on creating and publishing objects were prepared[67]. Also, Trusted Introducer has assisted teams with accredited status in preparing objects and submitting them to the RIPE database. Alas, the adoption of the object even could be better. 13 out of 34 TI accredited teams that already have the object created for them by the service really linked it to their constituent's network information. Another problem is lack of tools for end users that would support easy queries for IRT information. Still, this example shows that in order for a solution to work, it should give benefits at low additional efforts and costs.

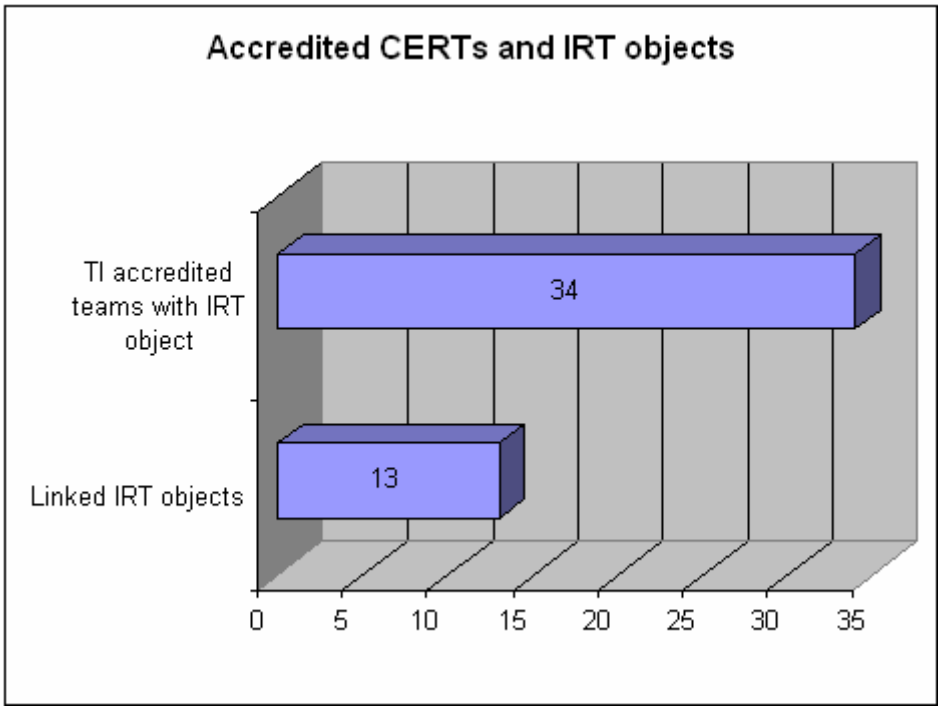


Fig. 6. Only 38% of the TI accredited teams use their IRT object

7.3 Barriers for cooperation

As proven in chapter *7.1 Benefits of cooperation*, cooperation results in many positive effects for the cooperating parties. Unfortunately there are also some barriers which limit the possibilities to cooperate or even make cooperation impossible. Some of them, identified as the most important, are discussed below. Alas, the fact that a particular obstacle is identified does not mean it cannot be resolved. On the other hand some barriers are a consequences of more important rules (like for example legal systems) and the possibilities to abolish them are very limited.

[66] IRT Object: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[67] see: RIPE IRT object – Technical HOWTO by Marco Thorbruegge: ww.ti.terena.nl/links/irt-object-howto.html and IRT object FAQ by Jan Meijer: http://www.surfnetters.nl/meijer/tf-csirt/irt-object-faq.html#q9

7.3.1 Necessity of confidence

During the incident handling process as well as other IT security related activities, CERTs get in contact with very sensitive information. The processing of this information is very often regulated by law. As usual, such regulations impose many limits for exchanging of information and its usage for different purposes. This is already true within a single country, but this problem increases even more when we consider international cooperation. Many teams are simply not allowed to share any sensitive information with other teams. In such case they just can produce abridged information that could then be used by third parties to undertake the adequate actions.

7.3.2 Financial issues

Closer levels of cooperation most often lead to larger financial expenses. Only the very basic cooperation activities like common mailing lists or some information sharing electronic platforms are very low cost issues (but even they are usually consequences of earlier meetings, workshops, conferences, etc.). Building a valuable level of cooperation is therefore also a monetary issue. Insofar as we depend on trust between cooperating sides, usually "real life" contacts between people interested in establishing cooperation are necessary. Thus money can be a barrier in building cooperation.

7.3.3 Lack of Service Level Agreements (SLA) between cooperating CERTs

This barrier especially concerns the team-team model of cooperation (see chapter *5.1 Models of cooperation*). It is not a barrier, which completely blocks cooperation between teams, but it can slow down the process. One specific problem concerns the incident handling process and especially request/response times. In the CERT world it is not a very much widespread practice to establish strict rules for reaction times towards reporting facilities other than their own constituency, which is not beneficial for the development of cooperation. Of course it should be noticed that this barrier is very much related to other ones like differences in legal systems (see chapter *7.3.4*) or the general lack of standards. Altogether: there are no generally known examples of CERT collaboration in accordance to an agreed upon service level agreement (SLA).

(Remark: as a SLA could be considered a too "strong" model of commitment for CERT cooperation we later propose the *Declared Level of Service* solution, a kind of compact SLA (see chapter *8.6.4*)

7.3.4 Differences in Legal Systems

Different CERTs work in different legal environments. Therefore they must fulfil the requirements of and operate in accordance with the legal system of their country. This obvious issue has influence on the way they provide their services. For example, it impacts how, when, and to whom they can make available the data they process (the same applies for exchanging the information). Sometimes particular kinds of network attacks are treated differently in different countries (see the *CSIRT legal handbook*[68]). This, as mentioned above, especially concerns international cooperation, but also can have an impact on cooperation on national level.

[68] CSIRT legal handbook: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#07

Sometimes even within the same country legal rules may not be the same for the collaborating parties. Affiliation to a specific sector for example might force adherence to specific regulations. Examples of regulations associated with Internet Service Providers are those concerning provider data retention requirements. (Such regulations usually do not concern CERTs operating beyond ISP structures.)

It is also worth to mention the barriers resulting from the internal regulations of organisations where CERTs operate. General regulations of many organisations, and also some more detailed, such as security policies, can include rules for dealing with information and other organisations' data. This concerns especially information sensitive sectors like finances or public administration.

7.3.5 No sufficient organisational and political support

Since CERTs are from a formal point of view usually part of bigger organisations like universities, corporations, public administration bodies etc, their role may often not be seen as "mission critical" from the large organisation point of view, resulting in not enough support from management of the parent institution. This seems to be one of the barriers in CERT team development and can have negative impact on CERT cooperation. For example, the management of a parent institution either may not understand the benefits resulting from supporting IRT capability or considers cooperation between different CERTs impossible because of competition issues, for example competitors on telecom market can have CERTs which collaborate with each other. As a matter of fact cooperation among CERTs of competing companies works very well on this level, for example in FIRST, TF-CSIRT or the German CERT-Verbund. So this specific barrier is probably only virtual and can be abolished very easy. For this, it is important to understand that CERT cooperation does not impact the competitiveness between the players on the market (for example ISPs). It is an important task for CERT teams to brief their higher management (persons responsible for cooperation policy of given institution and/or budgetary issues) about the necessity of CERT cooperation and the resulting benefit to the organisation.

It is worth to mention one more issue directly connected to the decision- and policy makers. In order to be able to actively participate in national and international cooperation, a CERT needs additional budget for participating in different events and in common projects. All these need a good management

Could FIRSTs CEP be a remedy for insufficient organisational and political support?

In this chapter the lack of support for CERT from management of the parental institution as one of the potential barriers in team development as well as in CERT cooperation is discussed. One of the interesting initiatives that potentially could lower this barrier is the Corporate Executive Programme (CEP) initiated by FIRST[69]. The aim of the CEP is to bring together cross functional senior executives with responsibility for decision making in their organisations. In this program, senior executives are encouraged (during special meetings) to understand the nature of future threats and risks which global organisations will be facing in the years ahead. They discuss and share intelligence and insights for risk assessment and management with other "blue chip" enterprises, the military, law enforcement and other government organisations. They also benefit from the interaction and networking with other CEP members and learn about how other organisations are dealing with similar issues.

[69] FIRST CEP: http://www.first.org/global/cep/

support and allocation of funds. Another solution could involve other organisations, companies, and institutions which see their interests aligned with developing the cooperation between CERTs.

How to deal with lack of support from the management was also addressed in ENISAs *CSIRT setting up guide*[70].

7.3.6 Lack of (adoption of) standards

Although the first CERT team was established almost 20 years ago (1988) there is still no well developed and adopted standard for CERT operation. There are some good practices documents available like for example RFC 2350 "Expectations for Computer Security Incident Response Teams"[71]. This fact is very important from the point of view of developing cooperation. It is worth to mention the lack of (adoption of) standards for CERT in the following areas:

Missing (or not widely adopted) standard	**Potential consequences**
Incident classification (IODEF – Incident Object Description and Exchange Format)	• Lack of common statistics • Ambiguous threat assessment • Impossibility of an phenomena assessment scale
Data Exchange Format (IDMEF – Intrusion Detection Message Exchange Format)	• Delayed exchange of significant data • Automatic incident data processing and handling more difficult
Incident handling process	• Unknown reaction time • Unknown problem resolving time • Unknown procedure sequence tracking
Contents of incident reports[72]	• Lack of some data important for problem resolution
Format for Security Advisories (EISPP Common Advisory Format Description) DAF (Deutsches Advisory Format) (VEDEF - Vulnerability and Exploit Description and Exchange Format)	• Additional overhead in preparing own versions of advisories instead of using existing ones • As consequence delayed reaction to threats
Threat assessment (CVSS – Common Vulnerability Scoring System)	• Change management decision is difficult • No change in the solution configuration when needed

Fig. 7. Impact of missing or not widely adopted standards

Probably the adoption of IODEF might solve more than one of the above-mentioned problems, but at least at the moment, due to the long periods of development and limited experiences in its implementation, it is difficult to assess its future usefulness and effectiveness.

[70] ENISAs CSIRT setting up guide: http://www.enisa.europa.eu/cert%5Fguide/index_guide.htm

[71] RFC 2350 "Expectations for Computer Emergency Response Team": http://www.ietf.org/rfc/rfc2350.txt

[72] For example the IP address of an attacker, IP address of a victim, operating system logs, attacked software logs, etc.

7.4 Relevant stakeholders

CERT cooperation is and should be further facilitated by various stakeholders who have a mission, power or direct or indirect goal for fostering such cooperation. On the list of stakeholders there are forums and associations but also governments or international agencies. Some organisations are aiming for coordination and cooperation among computer networks in various countries and thus they should also play the role of a facilitator in ICT security cooperation between appropriate parties. Other organisations are clearly set up to promote and facilitate the cooperation or coordination between CERTs in particular region or even globally. On the other hand national governments have to ensure proper interaction between all relevant ICT security elements (including CERTs and other security teams) within their country. Below we give some examples of relevant stakeholders in terms of facilitating cooperation between CERTs. They are listed in alphabetical order.

APCERT

The Asia-Pacific CERT initiative is a very important player in the area of facilitation of further cooperation, as this initiative covers some of the most dynamic and fastest growing economies around the world. This dynamic processes and the growth encompasses also the development of the Internet in this region and more hosts connected to the Internet means more threats and potential attacks coming from that region. Therefore, cooperation among CERTs from this region and cooperation between APCERT and other initiatives seems to be of rising importance.

CEENet

Network security is one of the key interests of CEENet. Sharing of information between more or less developed countries is a key element to achieve an acceptable average level of ICT security across the region. The CEENet community is planning to establish a network of CERTs in cooperation within those countries when such capabilities are already established (see chapter 7.5.3 for more information about CEENet).

ENISA

ENISA has a strong mandate to deal with CERT issues. In Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Agency in Article 2 the first objective is: “The Agency shall enhance the capability of the Community, the Member States and, as a consequence, the business community to prevent, address and to respond to network and information security problems.” ICT Security Incident Response Capabilities developed in CERTs, CSIRTs, Abuse Teams and other security teams are the natural element of building an overall capability of the community to combat security threats and incidents. Therefore, every year ENISA has a place in its Working Program for tasks related to the CERT topic and has published some important deliverables (this document being one of them).

ENISA also operates ad-hoc Working Groups devoted to this topic: the Working Group CERT COOPERATION AND SUPPORT[73] from 2005 and the Working Group CERT SERVICES in 2006[74].

FIRST

As the only truly global forum of CERTs with representatives from all kinds of teams and all sectors, FIRST is a well-positioned institution in the security area. Currently, FIRST affects non-members in limited ways. Most noticeable examples of this influence are:

- Annual conferences open to non-members with security workshops and seminars where technical, operational and organisational knowledge is shared. Conferences also provide excellent opportunity for networking for both FIRST members and non-members.
- Advocacy of CVSS (Common Vulnerability Scoring System)[75] – a standard metric for severity of vulnerabilities. Since June 2005, FIRST is also hosting CVSS in collaboration with CERT/CC and MITRE[76]
- Co-funding series of trainings based on TRANSITS project to facilitate development of CERT teams worldwide

National governments

National governments among other things are interested in protecting critical elements of the county's infrastructure as well as the regulation of several areas of activities of their citizens and organisations (for example the telecommunication market). Since regulatory bodies (especially in telecommunication) are engaged in monitoring and assessing smooth functioning of particular markets and even have important initiating role in national legal order, they are meaningful stakeholders in ICT security. In some countries national CERTs are even located inside regulatory authorities.

National critical infrastructure protection

In a green paper about the policy options for a European Programme on Critical Infrastructure Protection adopted by the European Commission (COM(2005)576) it is stressed that protection of communication and information infrastructure is a priority. According to the G8 principles for protecting critical information infrastructures: "Information infrastructures form an essential part of critical infrastructures.(…) Countries should have emergency warning networks regarding cyber vulnerabilities, threats and incidents It is only natural that many CERTs are involved in Critical Information Infrastructure Protection (CIIP). Generally speaking, teams that act as national CERTs are engaged in CIIP. Depending on the country there are various cooperation models:

---

[73] ENISA ad-hoc WG 2005: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_COOPERATION_AND_SUPPORT.htm

[74] ENISA ad-hoc WG 2006: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

[75] CVSS: http://www.first.org/cvss/

[76] The MITRE Corporation is a US-based not-for-profit organisation chartered to work in the public interest with the goal to apply expertise in systems engineering, information technology, operational concepts, and enterprise modernization to address its sponsors' critical needs; see http://www.mitre.org/

- **USA**: US-CERT as a government CERT is an important part of CIIP system responsible (among other duties) for incident response in national critical infrastructure. Additionally US-CERT closely co-operates with CERT CC – the "ancestor" of all CERTs.

- **Australia**: The relatively small governmental CERT does not handle incidents – this role is delegated to AUSCERT, the most experienced team in Australia and a motor behind APCERT.

- **Switzerland**: The Reporting and Analysis Centre for Information Assurance (MELANIE) responsible for CIIP is closely co-operating with SWITCH-CERT primarily responsible for the research network in Switzerland

- **United Kingdom**: UNIRAS, the governmental CERT is a part of NISCC (National Infrastructure Security Coordination Centre), and as such responsible for Critical National Infrastructure protection.

- **Finland**: CERT-FI is the national CERT for the whole of Finland, including government and critical national infrastructures, and acts as the alert, warning and response component of FICORA (Finnish Communication Regulatory Authority)

- **Poland**: CERT Polska is cooperating with the Polish National Internal Security Agency in building national capability of warning and alerting system devoted to CIIP.

Twenty countries are listed in "International CIIP Directory" provided by NISCC in which government representatives can find many entries about CERTs dealing with CNI in each country.

Regulating agencies

In many countries regulating bodies are entities within the public administration, which are very close to the "CERT world". Since they deal with ISPs on a daily basis, regulating agencies understand network phenomenon and aspects related to IT security and incident handling. Such agencies can play a very important role in facilitating domestic CERTs cooperation as well as establishing new CERT teams.

7.5 Evaluation of the most important cooperation initiatives

The evaluation presented in this chapter is mainly focuses on the following aspects:

- What was achieved (by an initiative)?

- What possibilities emerge for the future?

This evaluation covers cooperation at national, regional and sector levels.

7.5.1 National cooperation initiatives

National initiatives seem to be a very effective way of CERT cooperation. CERTs collaborating on a national level operate in the same legal system, know specific aspects connected to their country, speak the same language, and last but not the least, operate geographically close to each other that allows them to meet more often and more regularly. Thanks to these facts they are able to synchronise their efforts in both technical and organisational area. It seems possible

that the fact of a growing number of national cooperation initiatives might some day result in a new example of cooperation in the association-association model: cooperation between various national initiatives.

7.5.2 TF-CSIRT

The TERENA TF-CSIRT is a mature regional forum following a scheme that simply proved to work best for the European region and environment. Low travel costs allow many teams to be present during task-force seminars and meetings, which gives a great opportunity for networking, helping new teams to establish personal contacts and maintain them over the time. Particular tasks are delivered by volunteering individuals or small working groups. On the other hand, even though TF-CSIRT is a group of highly skilled professionals, it still does not get enough publicity and recognition. There is still much potential in acting as a group, allowing for development of best practices, code of conduct, or recommendations for legislation, etc. The abandonment of common projects that relate on the voluntarily commitment of the members resulting out of job-change of key persons, decrease of interest of other factors is also an issue that should be addressed in the future.

7.5.3 CEENET

CEENET as a regional cooperation in Central and Eastern Europe, which includes some adjacent countries from Asia (thus, can also be seen as a cross-regional cooperation), is an example of a system of collaboration working for many years (also thanks to the support of NATO with funds) with the goal of sharing computer networking knowledge between more and less developed members of the association. Since every network will face security problems in some phase of utilisation it is natural that CEENET includes ICT security issues in their workshops, seminars and programmes. During several years of activity a network of people from the academic environment (NRENs, National Research and Educational Networks) was established. There are representatives from such advanced NRENs like ACOnet (Austria), ARNES (Slovenia) or NASK (Poland) as well as members from countries like Albania, Azerbaijan or Moldova with substantially less experience. CEENET proved that such cooperation can be beneficial to very different parties. The trust model in CEENET relies upon face-to-face contact during events and participation in common projects. One of the important projects established lately is focused on building IRT capabilities in each member country and in continuously facilitating the process of cooperation between them. With budgetary support devoted to hard- and software and mentoring from countries in which CERTs have worked for many years there is a goal to establish a network of cooperation in incident handling across the whole region. This task is scheduled for the near future and, if successful, can be further developed in terms of enhancing CERT services.

7.5.4 North American CSIRT meeting

The North American CSIRT meeting is an example of a working, less formal cooperation between CERTs. A benefit of such model is its easy setting up, but on the other hand the model seems to be less feasible in long term cooperation, resulting from the lack of rules of cooperation (for example regular meetings). A final assessment can be made only after a couple of years.

7.5.5 FIRST SIGs

The fast growing SIG initiative in the FIRST framework proved to be a good platforms for international cooperation focused on common interest of particular groups. Concentration on concrete subjects like network monitoring, vendor issues or cooperation with LEA is a very good idea for tightening collaboration and establishing trust between teams. The survivability of a SIG depends, like in other forms of cooperation, highly depends on the commitment of its members, and thus the FIRST SIGs might face the same problems that other initiatives that are based on voluntary work suffer from.

Nevertheless: the SIGs are an interesting idea of cooperation among CERT focused on the same or very similar topics. This gives a big chance to developing concrete and beneficial cooperation on the fundaments of technical issues that for many CERT team members are the most important and interesting. They also turned out to be very good solution for introducing a new sub-structure into a big organisation which the FIRST, with almost 200 members, is.

7.5.6 E-COAT

E-coat, as an example of a sector cooperation initiative, is organisationally still in a very early phase While many teams recognise the benefits of meeting and talking to each other, there are only few ideas for deliverables, making the forum mostly a platform of networking and occasional exchange of opinions. In some cases the fact that abuse teams are just small parts of large telecommunication companies impacts the possibility to make decisions for example on self-regulation.

8 Ideas for Future facilitation of CERT Cooperation

This section introduces some specific ideas for future facilitation of CERT cooperation in fields directly relevant to topics discussed earlier in this document, such as national, regional, international and sector forums as well as models of trust.

The last section contains recommendations for improvement of the cooperation as well as suggestions for actions for relevant stakeholders identified in the previous chapter. Some possible incentives to help in development of this cooperation are also indicated.

8.1 National Cooperation

Awareness building

Security awareness should be built at a national level. This way language and culture of a nation can be used in the most efficient way. Nation-wide public education campaigns about computer security can be launched in the same way as campaigns about road traffic security or health care. A good example of this kind of campaign is "Protect Your Computer!" campaign launched in June 2006 in Lithuania. This campaign targeted home users, providing them with CDs containing security software and documents with advice. Those CDs were distributed for example in Internet cafes and computer magazines, altogether over 400 distribution spots. The campaign was coordinated by Lithuanian Communications Regulatory Authority and supported by the Ministry of Interior as well as many commercial partners, including Microsoft and major banks.[77]

Home users are not the only target in the need of security awareness rising. Similar campaigns can also promote security across the telecommunication industry. On the other hand, public campaigns can influence governments when new laws or other regulations are needed in the security areas.

The best option for funding such campaigns is a public-private partnership, as was the case in Lithuania. This is understandable as both industry and governments are lively interested in the promotion of security. Of course, CERTs and especially national CERTs can play an important role: using their potential and knowledge brings additional and higher level of quality to the materials, while the campaign itself can help advertise CERT services to a broad audience.

National Point of Contact

There are many cases when multiple CERTs coexist in the same country. Their constituency boundaries are usually not clear to other teams, especially those from abroad or even overseas. There are also white spots where some networks do not have an associated CERT or when a team has not developed any external contacts.

All this leads to situations where a CERT observing an incident related to a network abroad is often confused: who should be contacted? Ideally, there should be a single point of contact in each country, keeping current network of local contacts. In order not to repeat the co-

[77] "Protect your computer!" campaign: http://www.rrt.lt/index.php?-660430147

ordinational and hierarchical approach from EuroCERT, the national point of contact should not be a point to report an incident and should not provide any incident co-ordination let alone incident handling for the two parties involved. Rather, it should just direct the reporter to the appropriate contact. This approach takes a lot off burden on the point of contact and does not make resolution of incident dependant of willingness to submit information to an arbitrary body. CERTs would still maintain freedom of choice in regards of how and with whom they exchange information. It must be stressed that the point of contact should have an ancillary, not supervisory role.

Due to lack of formal points of contacts, teams that are most active or most widely recognised currently perform this role. This is usually not the most effective way to handle incidents as multiple instances, which are not operationally involved, have to record, forward and track the information.

The point of contact could be established by a national CERT or as an institution not affiliated with any CERT in particular, for example, by a telecommunication regulatory authority.

8.2 Regional Cooperation

8.2.1 Mentoring schema

One of the ideas for the future is the strengthening of mentoring initiatives. The idea is to build a good, long-term operational relationship between experienced teams and newly founded ones or organisations which are planning to establish a CERT. It is not enough to wait for new teams to contact more experienced colleagues. This process can be proactive, facilitated by various relevant stakeholders (for example TERENA TF-CSIRT, CEENet and ENISA). It could be based on a plan of how to fill the existing gaps on the map of CERT services, constituencies and geographical areas (for example identified by ENISA during its Gap Analysis research[78]). When developing this concept it is worth to take into consideration that many geographical (at the same time political) gaps are beyond some possible areas of investing money (for example funds managed by European Commission).

8.2.2 Filling the gaps

Filling the gaps in cooperation in incident handling (with respect to other CERT services) is one of the most important tasks whether we are talking about global culture of security. The active searching for new potential CERTs is possible for instance on the basis of „gap analysis" performed by ENISA. It is important to invent effective ways to reach respected people and decision makers who can be briefed to make a decision to establish a new CERT in particular country, organisation or sector. It can be facilitated for instance by the use of existing channels of cooperation between countries or organisations: for example economical or scientific cooperation. CERT establishment and cooperation might be enclosed to those existing channels of collaboration.

[78] Results of this research can be found in Appendix A of the Report of ENISA WG CERT Cooperation and Support from February 2006: http://www.enisa.europa.eu/doc/pdf/deliverables/CERT/20060227_chair_wg_cert_report.pdf

8.3 International cooperation

Since the SIG idea in international cooperation proved its usefulness, supporting this kind of initiatives is highly recommended. Building relations between teams based on technical knowledge and thematic interest seems to be very attractive for technical staff working for CERTs.

The case of SIGs shows that international cooperation should be developed towards thematic subjects. Forums like FIRST should (and do) play a role of umbrella for international sector and thematic cooperation initiatives.

8.4 Sector Cooperation

In sector cooperation there are two important issues in the opinion of the authors of this document:

- Searching the sectors in which there is no cooperation but it should exist,
- Expansion of existing cooperation

In the first task, sectors in which cooperation should be established and developed are the focus of analyses or studies. For instance cooperation between energy sector CERTs in adjacent countries should be important since power grids are cross bordered and energy systems are relying on SCADA (Supervisory Control And Data Acquisition[79]) control which can be vulnerable to some computer security threats.

The second task is about expanding existing cooperation. For instance, in national critical information infrastructure protection CERTs play an important role within a country. On the other hand, the cooperation between those CERTs is not prevalent at the moment despite the fact that it is easy to imagine a terrorist attack planned to destroy national critical infrastructure in many countries at the same time. Therefore, cooperation between CERTs involved in CIIP process is more than needed. Some respective conferences and seminars about CIIP (especially those with support of ENISA) should include this topic in their agendas.

[79] SCADA: http://en.wikipedia.org/wiki/SCADA

8.5 Models of Trust

Current problems with trust are not resulting from the lack of trust models. The models enumerated in chapter *5.3* are working and they suit particular needs well. However, a recognised authority that would perform a certification process for CERTs is lacking. The process resulting with a certificate for applying team should include:

- Verification of personnel's competence
- Verification of team's procedures and policies
- Verification of financial stability and sustainability
- Verification of basic operational factors, such as: reachability or response times

In order to complete the certification, the team should sign a code of conduct, specifying expectations the team would commit to meet, such as vulnerability disclosure policy, response times, etc.

The certifying institution could either come from industry or from international regulatory institutions as long as it has enough recognition that the certificate will give a team which earned it enough credibility and trust for team-team and other types of cooperation. Since the process of certification would likely require access to confidential information, the institution should be trustworthy itself. Potential conflicts of interest have to be avoided as well.

It must be noted that certification would apply only to CERT teams, which are usually not independent institutions, but rather parts of bigger companies. Thus, only processes regarding CERT work should be included in the certification. The nature of work performed by CERT teams would require the certificate to be renewed at least every two years.

Nevertheless, the issue of CERT certification seems to be an interesting topic that should be explored and evaluated further.

8.6 Recommendations for an improvement of cooperation

8.6.1 Idea of CERP (Computer Emergency Response Person)

There is no doubt that the idea of CERT is more and more popular. Together with an improvement of overall organisational culture and implementation of some international standards (for example ISO/IEC 17799) the number of CERTs is increasing. However it is also clear that always some part of organisations, companies and institutions will have no CERT team within their structures. The reasons for this are various: an organisation is too small to operate such unit, there is a lack of human resources, there is a lack of financial resources etc. Therefore, a way of ensuring an incident response capability within as many as possible organisations should be developed.

One of the concepts might be CERP (Computer Emergency Response Person) - a person who will be involved and responsible for incident response process. Such position needs special personal skills and should be supported organisationally and technically. Wide introduction of this concept could bear fruit in better cooperation between an extremely large number of

organisations and improve significantly the quality of the incident response cooperation not only between CERTs but practically almost all organisations.

8.6.2 Wider adoption of the WARP concept

WARP concept is a premium tool for sharing information among the members of smaller communities. They are easy to set up and maintain and are an inexpensive alternative to a full grown CERT. They are widely spread in the UK, but their usage can be much more facilitated and introduced also in other countries. With WARPs Internet users can be reached that usually would not be part of any kind of security related cooperation. By a wider facilitation and dissemination of WARPs also outside the UK the net of security aware Internet users could be meshed closer. By cooperation between CERTs and WARPs in the area of information sharing both sides will only benefit, and the security community can greatly enhance the clearing of "white spots" in the security landscape.

8.6.3 Information Handling Improvement

Since cooperation among CERTs strongly depends on trust it might be helpful to adopt common "protocols" of information sharing. The example of such a concept is "Traffic Light Protocol" (TLP) proposed by the British NISCC[80]. This concept is proposed to be used when security information is shared between relevant parties in the environment of CIIP. Under the TLP the originator of the information labels it with one of four categories (indicated by different colours) to suggest further dissemination undertaken by the recipient (for example "no dissemination", "limited distribution", "community wide", "unlimited"). If the involved parties understand and agree on a common protocol, less hesitation in sharing valuable information will occur among security teams. This can accompany the process of building trust among teams.

8.6.4 Declared Level of Service

As mentioned before, lack of information about expected reaction times of a CERT receiving security information during incident handling can be perceived as one of the main cooperation barriers. Comparing to the business world this drawback was labelled earlier in this document as a *Lack of SLA*, which means that there is no agreed procedure and timeframe of incident handling.

To overcome this drawback a set of rules concerning reaction measures and times of a particular team could be added to the publicly available description of this CERT. Since there are a lot of differences between business agreement schemes and CERT cooperation goals instead of "SLA" the authors of this document venture to propose another name. This could be named, for example, the *Declared Level of Service* in which some basic information could be placed like: hours of service (for example 24/7), priorities of incident handling (if any), reaction time and committed handling time, feedback to the originator, adopted rules of information handling or sharing and others.

[80] NISCC – National Infrastructure Security Co-ordination Centre: http://www.niscc.gov.uk

8.7 A possible framework for CERT cooperation development

It would be big incentive to CERTs and CERT cooperation if a programme aimed to promote culture of security (especially focused on solving ICT security problems/incidents by establishing and developing CERT cooperation) was initiated by the EU. This recommendation is based on observation of the success of the EU response to illegal and harmful content on the Internet that the Safer Internet Action Plan (SIAP) and then Safer Internet plus Programme brought.

Safer Internet plus Programme

The programme aims at the promotion of safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user as part of a coherent approach by the European Union.

The 4-year programme (2005–08) has a budget of € 45 million and has four main actions:

- Fighting against illegal content
- Tackling unwanted and harmful content
- Promoting a safer environment
- Awareness-raising

This programme as a continuation of SIAP promotes among others Hotlines (national contact points) for illegal content as well as “Awarenodes” (national awareness centres). On the European scale Hotlines and Awarenodes are organised in associations: INHOPE[81] for Hotlines and INSAFE[82] for Awarenodes.

Hotlines, Awarenodes and their associations are co-funded by the European Commission under agreements between accepted parties and the EC for a 3 year period. Such an incentive during SIAP operation time (3 years) resulted in Hotlines and Awarenodes in nearly every European Member State. A 50% level of co-financing is an important incentive and on the other hand there is an obligation to participate in association activities which fosters cooperation and common project between parties as well as common statistics, mentoring programmes and many others.

It is worth to analyse the possibility of either extending such programme from “safety” to “security” since those terms are very close to each other or to issue a new programme with separate budget that can cover CERT issues.

[81] INHOPE: http://www.inhope.org

[82] INSAFE: http://www.safereinternet.org

8.8 A new concept for CERT cooperation

If we consider the network of CERT collaboration of today as a basic "version 1" with some "sub-releases" featuring a set of enhanced functions (version 1.x) – for example in case of cooperation between members of regional initiative or sector cooperation - there is a need to "upgrade" this network to version 2 ("Next Generation CERTs") which can really solve ICT security problems of the near and distant future. This could include – among others some ideas presented above as well some obvious recommendations:

- DLS (Declared level of Service) – see chapter *8.6.4*
- IHI (Information handling Improvement) – see chapter *8.6.3*
- Certification – see chapter *8.5*
- Implementation of common standards and tools
- Active participation in deployment of network of contacts and international cooperation
- Mentorship programs
- Involvement in awareness raising

As a basis for DLS the set of CERT services should be defined by each team and published. In chapter *7.2 Influence of cooperation on CERTs services improvement* we gave an example of a set of services and the influence of cooperation on their better performance and improvement. It is recommended that when a set of services is defined for a particular team - a relation between the most important services (for example Incident Handling, Vulnerability Handling, Alerts and Warnings) and specified procedures and response timeframes and particular actions to be taken in specific situations should be put in place. This is important not only related to cooperation between CERTs but also in communication with the constituency.

DLS can be supported by information handling improvement (or enhancement). Various kinds of information are exchanged among CERTs and between CERTs and their constituencies. If the involved parties agree on some protocol or schema of sharing information, then this could result in less hesitation in sharing information in concrete situations. It is recommended to classify information and to attribute particular labels to

Regulation?

What to regulate and what not to regulate is always a subject of dispute among various concerned parties.

Better cooperation is without a doubt beneficial for all involved parties. However an effort should be directed towards convincing and not forcing cooperation, as this model proved very successful in the past.

Of course, wherever a close relationship between CERT cooperation and public safety exists, at least some regulation should be applied. "Public Safety" involves the protection of the general population from all manners of significant danger, injury, damage or harm, such as may occur in a natural disaster, and the prevention of the same. Although this protection is provided by those traditional organisations known as emergency services (police, fire and rescue and ambulance), in the preventative sense "public safety" must be the priority of all those who, in any way, engineer circumstances for others.[83]

It could be worthwhile to think about the extension of the definition of "public safety" to Internet and NIS related issues.

[83] Definition of "public safety" from Wikipedia: http://en.wikipedia.org/wiki/Public_safety

every piece of information (mail, alert, advisory) that clearly shows how it is to be handled by the recipient. Some of the information should be encrypted when send over the Internet, some should only be distributed to a limited number of parties and others are dedicated only for internal use. The "next generation CERT" should have a policy of handling information in place that is known to peer parties and also should expect the same from cooperating teams.

DLS can become a basis for certification described in chapter *8.5 Models of trust* as this process would include verification of compliance with DLS and published policies.

The possibility of implementing common standards is currently limited by their availability or by the lack of tools or software frameworks to put them in place (see chapter *7.3 Barriers for cooperation)*. In order to allow easy and effective sharing of incident related data, clearly some standardisation is needed that would facilitate handling of incident related data, proper prioritisation and comparison of trends and statistics between different teams. Along with the standards, tools supporting them need to be developed. In the future, CERTs should be able to use common set of tools for everyday incident handling. Some tendencies toward involvement of teams in development of such tools can already be observed.

The participation of CERTs in regional or international initiatives seems to be one of the most successful means to build a network of live contacts that supports the increase of trust between teams as well as sharing expertise. These initiatives (as pointed out earlier) could be joint research projects, negotiating common standards deployment, workshops or video/teleconferences. Especially the last possibility, establishing videoconferences via Internet between cooperating teams is rarely used these days, however it is a very convenient tool to supplement to personal meetings. Participation in various initiatives can also be an opportunity for engaging in mentorship process with new teams.

Awareness raising programs – hopefully growing in most European countries – are a good opportunity for CERTs to communicate their role in local community. CERTs can play their role as center of expertise and support such programs with concrete knowledge about main security problems in a country and provide "real life" security statistics. One idea that might be worth to consider is establishing relation between CERTs and the "Safer Internet" program in every country. There is an example of such cooperation in Poland between CERT Polska[84] and the Saferinternet.pl program initiated and being carried out as the parent organisation (NASK) is involved in both projects.

[84] CERT Polska: http://www.enisa.europa.eu/cert_inventory/pages/03_pl.htm

Annex I – Memorandum of Understanding between APCERT and TERENA TF-CSIRT

Memorandum of Understanding

Between

Asian-Pacific Computer Emergency Response Team (APCERT)

And

TERENA's Task Force of Computer Security Incident Response Teams (TF-CSIRT)

June 2005

The Asian Pacific Computer Emergency Response Team (APCERT) and TERENA's Task Force of Computer Security Incident Response Teams (TF-CSIRT) commonly recognised as the Regional Initiatives (RIs) for the Asian Pacific region (APCERT) and the European region (TF-CSIRT)

CONSIDERING that

- The issues of computer security incident prevention and response are a matter of joint collaborative effort;
- The global Internet is designed to interconnect large heterogeneous networks worldwide, and has, as such, become a common resource to large communities in both regions;
- Threats and vulnerabilities usually spread quickly with a world-wide impact;
- Strategic, tactical and operational nature of incident prevention and response is often the same, regardless of location;
- Despite many similarities, regions across the globe may sometimes have different approaches, depending on local differences based on cultural, economical, and political structures;

STATING that

- Further worldwide collaboration on all levels of incident prevention and response will make the Internet more reliable and trustworthy;

AGREE to

- Exchange information about current and future developments within their own RIs;
- Mutually appoint two liaison members to act as the point of contact with respect to the partner RI with regards to such information exchange;
- Dispatch, on a best effort basis, a delegation to the working meetings of the partner RI, to the extent that is deemed appropriate by the partner RI;
- Involve the partner RI in projects that have a relevant context beyond the boundaries of a single RI;
- Terminate this MoU bilaterally whenever circumstances so warrant.
- The parties agree to each bear their own costs in negotiating and signing this MoU. It is not intended that this Memorandum of Understanding shall be legally binding on the Parties and it may be amended at any time subject to mutual agreement of the Parties.

SIGNED in (city) on (date) BY

(APCERT) (TF-CSIRT)

Annex II – TERENA TF-CSIRT Terms of Reference

TF-CSIRT

Terms of Reference

1. A Task Force is established under the auspices of the TERENA Technical Programme (www.terena.nl/about/tech/ToR.html) to promote the collaboration between Computer Security Incident Response Teams (CSIRTs) in Europe. It will be known as TF-CSIRT (Collaboration of Security Incident Response Teams).

2. The aims of the Task Force will be:

a. to provide a forum for exchanging experiences and knowledge;

b. to establish pilot services for the European CSIRTs community;

c. to promote common standards and procedures for responding to security incidents;

d. to assist the establishment of new CSIRTs and the training of CSIRTs' staff;

e. to co-ordinate other joint initiatives;

f. to provide a vehicle for CSIRTs in Europe to liaise with the European Commission and other policy making bodies.

The Task Force will focus its activities on Europe and neighbouring countries and on (potential) CSIRTs operated by (national and international) research and education networks, commercial Internet Service Providers (ISPs), companies and governmental institutions as well as vendor-product teams and commercial CSIRTs. It will collaborate with other teams and with organisations outside the geographical area whenever such collaboration will assist in achieving the aims of the Task Force.

3. With a commitment to the development of collaboration between CSIRTs as

defined above, participation in the Task Force will be open to individuals, subject to the agreement of the Task Force chairman.

4. The chair of the Task Force will be Gorazd Božič. He will be responsible for preparing the agenda for each meeting and for co-ordinating the work of the Task Force. He will also be responsible for ensuring that any agreed deliverables are produced. The deputy chair of the Task Force will be Kauto Huopio. He will be responsible for chairing a meeting if the chair cannot participate.

5. The secretary of the Task Force will be appointed by TERENA. He/she will be responsible for taking the minutes at each meeting and for making logistical arrangements as necessary.

6. The Task Force will operate with a (renewed) two-year mandate, starting 15 May 2006. A mid-term milestone is set after one year; a report on the progress of the Task Force and the results achieved so far will then be presented at the TERENA Networking Conference 2007. The mandate of the Task Force may be renewed by the TERENA Technical Committee (TTC). If the mandate is not renewed, the Task Force will be dissolved. The Task Force may also be dissolved if the TTC considers that it is making insufficient progress or that its activities are no longer useful or relevant, or if the Task Force chair resigns and no replacement can be found.

7. The Task Force will meet at approximately 4-monthly intervals. Physical meetings will be held at various locations, taking care to reduce overall costs to participants.

8. Whilst respecting copyright and restrictions of use imposed by the owner of information, reports and other results of Task Force activities will be placed in the public domain, with the exception of information that is subject to a commercial non-disclosure agreement or other information that has been provided on a non-disclosure basis, and except in cases where disclosure of information would jeopardise the security of the networks and organisations involved.

9. The Task Force will have mailing lists for communication with and between the Task Force participants.

Work items, deliverables:

A. Meetings, seminars

Usually, a one-day or half-day seminar will be attached to Task Force meetings, in which experiences are exchanged and issues of common interests for CSIRTs are discussed.

B. Trusted Introducer

The Task Force will liaise with the Trusted Introducer (TI) service. The provision of the TI function is subcontracted by TERENA to a professional organisation. The TI provides a form of accreditation to CSIRTs and additional services for accredited CSIRTs. The TI will organise regular meetings of representatives of accredited CSIRTs adjacent to TF-CSIRT meetings. Major developments in the TI services will be reported to the Task Force.

C. Security Contact Information for Internet Resources

The Task Force will continue to track and support the deployment of abuse contact lookup mechanisms, help with improving documentation and propose changes in technology and procedures as appropriate; investigate the usefulness of extending those mechanisms to other unique Internet Resources (for example Autonomous System Numbers); track the impact of applying privacy and data-protection laws and regulations to this particular set of data, in particular with regard to the diverse legal landscape (national, EU-coordinated, international); and investigate possibilities, as well as support activities, to implement similar mechanisms in other Regional Registry or Routing Registry environments.

D. Clearinghouse for Incident Handling Tools

The Task Force maintains a web-based clearinghouse for security software, covering both free software and commercial products. The focus of the clearinghouse is on tools that are in actual use in CSIRTs whose staff members participate in TF-CSIRT. Developments in the clearinghouse service will be reported to the Task Force.

E. Training of new (staff of) CSIRTs

The Task Force will review the needs for specific training for staff members of CSIRTs and will promote the development and delivery of appropriate training materials to meet these needs. The Task Force will receive reports on the TRANSITS trainings organised by TERENA and by FIRST, and on the measures that are taken to guarantee the continuity of the TRANSITS training effort.

F. Assistance to the establishment of new CSIRTs

The Task Force will develop and maintain appropriate resources and services to assist the establishment and development of new CSIRTs. Where appropriate this will be done in collaboration with other groups or organisations working in this area.

G. Collaboration with FIRST and organisations in other world regions

The Task Force will investigate possibilities to collaborate more actively with FIRST, and with counterparts of TF-CSIRT in other continents.

H. Request Tracker for Incident Response

The Task Force will set requirements, investigate ideas, develop new modules and generally monitor the progress of the Request Tracker for Incident Response (RTIR) Incident Handling tool. This work will be carried out under a statement of work with Best Practical Solutions LLC or by Task Force participants themselves. The aim of the activity is to extend the current application, by making it more stable and adding new functionality, thus making it more adaptable for the general use of new, as well as established CSIRTs.

I. Collaboration with Information Security Metadata Activities

The Task Force will collaborate with relevant activities in the production and maintenance of Information Security Metadata, such as Incident Description (IODEF) and Vulnerability and Exploit Description (VEDEF), both of which were formerly activities of the Task Force. Progress reports will be provided on a liaison basis by

task force participants who have an existing co-ordination function in this area and will collate inputs from other Task Force participants as appropriate.

J. Collaboration with the Joint Research Activity "Security" in the GN2 project

The Task Force will collaborate with the Joint Research Activity "Security" (JRA2) in the GN2 project. Progress reports from JRA2 will be presented to TF-CSIRT meetings. Ad-hoc groups composed of TF-CSIRT participants may, on request, provide JRA2 with advice on specific topics. The JRA2 team will have meetings adjacent to TF-CSIRT meetings; possibly joint meetings of TF-CSIRT and the JRA2 team will be organised. The chairman of TF-CSIRT and the leader of the JRA2 activity will appoint the members of a JRA2 advisory panel.

K. Liaison with the European Commission

The Task Force will exchange information with relevant EU bodies - such as the European Commission services responsible for EU policies and actions related to data and network security, and ENISA - and advise them as appropriate. Meetings between deputations of TF-CSIRT and relevant Commission officials will be organised as necessary.

L. Liaison with the E-CoAT

The Task Force will liaise with E-CoAT (European Cooperation of Abuse fighting Teams). Major developments in the work of E-CoAT will be reported to TF-CSIRT.

M. Incident handling and security guidelines for NREN Grids

Task force members will work with Grid communities to identify, and encourage the adoption of good security practice. Key areas of work will be in Grid incident response and vulnerability management. Other activities such as development of Grid-related risk assessments, security policies, security guidelines and technical security implementations may also be considered. Results will be disseminated through a website and mailing list and will be reported to the Task Force.

Annex III – eCSIRT.NET Code of Conduct

eCSIRT.net Code of Conduct

Preamble

Today's networked systems and communications are fundamental for the working of industry, economy, research, administration and government. Networks, systems as well as their applications are complex, disruptable and the target of intentional attacks is a growing threat. There is a need for co-operation between European Computer Security Incident Response Teams (CSIRTs) to

- Improve the security posture of the European Information Technology (IT) infrastructure;
- Enable an appropriate and timely response by CSIRTs, to attacks upon the European IT infrastructure;
- Raise the awareness by documenting the work of CSIRTs and providing statistical data about attacks and incidents.

These are the aspired goals of the partners of the eCSIRT.net project in recognition of their responsibilities:

- CSIC/IRIS-CERT (E)
- DFN-CERT (D)
- INFN/GARRnet CERT (I)
- Stelvio b.v. (NL)
- NASK/CERT-Polska (PL)
- PRESECURE Consulting GmbH (D)
- RENATER/Le CERT Renater (F)
- UKERNA/JANET-CERT (UK)
- UNI-C/DK-CERT (DK)

Vision

From now on the participants of the eCSIRT.net project will co-operate in the field of incident handling and build a new community. The take-up of techniques that are proposed within the project will enable the establishment of new best practices and serve the following goals:

- to enable a standardised and unambiguous exchange of incident related information between the CSIRTs involved;
- to enable the collection of standardised and unambiguous incident statistics serving CSIRTs involved and in a generalised fashion, the public;
- to enable the collection of standardised and unambiguous incident related data. This will be followed by intelligent generation of warnings and emergency alerts serving the CSIRTs involved.

Guidelines

The co-operation is determined by the following guidelines:

- The co-operation is voluntary and can be terminated at any time.
- Co-operation within the project will not infringe on partners business.
- Information and intellectual property rights of all partners must be protected.
- The confidentiality of constituent data will be given highest priority.
- Services provided by the partners should steadily improve.
- Policies, procedures and workflows of all partners should be optimized by the exchange of knowledge and practice within the partner community.
- The partners will develop and enable means for an improved exchange of knowledge and practices and will provider training material.
- The work and co-operation of partners should set an example for other CSIRTs and should provide a model for similar initiatives around the world.

The eCSIRT.net initiative is open for participation by all European teams that have been shown to follow established best practices by joining the TI accreditation framework (http://www.trusted-introducer.org). Teams outside Europe are welcome to liaise with eCSIRT.net and participate in discussions to progress the goals described above, so they can be implemented internationally. This will also progress the methods and practices developed so they can be utilized and applied in other settings.

Accepted by the eCSIRT.net partners on 9 December 2002 in Amersfoort, The Netherlands.