

Dependability Development

DDSI

Support Initiative

**DDSI
IST-2000-29202**

**Roadmap:
Warning & Information Sharing**

November 2002

RAND Europe (NL, Project Coordinator); King's College London (UK);
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);
Ernst Basler + Partner (CH), Isdefe (E)

Project number IST-2000-29202,
supported by
the IST research programme
of the European Community,
managed by
the European Commission DG
Information Society.



DDSI

Report Version: Final

Report Preparation Date: 1 November

Classification: Public

Preparation led by: King's College London (UK)

Contract Start Date: 1 June 2001 Duration: 18 months

Project Co-ordinator: RAND Europe (NL)

Partners: RAND Europe (NL); King's College London (UK); Cell Networks (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR); Ernst Basler + Partner (CH), Isdefe (E)

Preface

The dependability of the information infrastructures upon which the Information Society relies are recognised as being of growing importance for European citizens, businesses and governments. The European Council has called for a “comprehensive strategy on security of electronic networks including practical implementing action”¹ and the eEurope Action Plan 2005 outlines a range of strategies to promote security practices, a culture of security and trustworthy networks.²

As yet, dependability is not being effectively designed into the information system of systems that constitutes the European information infrastructure. This is due to a number of factors, ranging from software complexity and implementation failures to market forces that have encouraged the deployment of vulnerable software. The problem is demonstrated by statistics from the Computer Emergency Response Team community, which point to a steep growth in vulnerabilities. At the same time, there is a growth in the number and capability of malicious actors seeking to exploit security vulnerabilities.³

Since dependability is not - yet – being sufficiently engineered into Europe’s information infrastructures, there is an onus upon users to adopt a “culture of security;” this involves managing their own risks. Steps can range from adopting robust password policies at the individual level to building resilience into Large Complex Critical Infrastructures at the infrastructure or national levels.

However, infrastructure dependability as a risk management problem still faces the challenge of a lack of data upon which to base decisions. Put simply, all stakeholders require better information about risks, including vulnerabilities and threats.

For governments, information about vulnerabilities, dependencies, threats and incidents is vital if they are to develop public risk management policies in order to provide a safe and secure environment for their businesses and citizens. For businesses, information sharing is a matter of risk management and good corporate governance. For citizens, information is required to enable them to protect themselves and avoid becoming a jumping off point for attack on others.

Most governments have recognised there is currently a failure by the market to supply the information required by the full range of stakeholders about dependability risks. There are various government initiatives to stimulate or, in some cases, supplement market provisions. Given the inherently transnational nature of information infrastructures and the growing internationalisation of dependencies, threats and vulnerabilities, collaborative public action at European level also seems appropriate.

Any such action must however add value to existing industry and Member State activities. This document provides a roadmap for such action and outlines the issues and options that should be considered.

Acknowledgement

This roadmap could not have been completed without the support and input of dozens of experts from the CERT community, from business end-users and suppliers, from government and from the research community. Appendix 4 lists individuals and organisations who participated in one or both of the

¹ *Network & Information Security*, Resolution of the European Council, 6 December 2001.

² European Commission, eEurope 2005: Possible Actions

³ See DDSI Conceptual Framework for detailed discussion of these issues.

Roadmap workshops. Particular thanks go to Andrew Cormack, Daniel Bircher, John Harrison, David Spinks, Jos Dumortier, Danilo Bruschi, Michel Miqueu, Patrick Van Eecke and Michael Ward who gave their time to lead and report on workshop sessions. Our thanks also to Taizo Nakatomi, David Broadhead, Damir Rajnovic, Mark Koek, Günther Welsch, Eric Luijff, Peter Nevitt, Anne Verkuyl, Otto Hellwig, Hans-Joachim Bierschenk, Franziska Ehrhardt, Cort Dreyer, Gilles André and Thierry Van der Pyl, Andrea Servida who provided presentations at the workshops.

This Roadmap could not have been completed without the assistance of Marc Wilikens and Marc Hohenadel of the JRC who co-hosted the October 2001 workshop. Andrea Servida, Maarten Botterman, Susanne Jantsch, Marc Wilikens, Klaus Peter Kossakowski and Andrew Cormack provided detailed comments on the final draft of the Roadmap. Ben Cuthbertson provided invaluable research support.

Whilst this roadmap cannot pretend to represent a consensus view across such diverse communities, every effort has been made to incorporate a variety of perspectives. Responsibility for any mistakes remains with the authors.

Andrew Rathmell
Lorenzo Valeri
August 2002

Executive Summary

This report provides a Roadmap or European action to promote information sharing about information security risks. It is based on a comprehensive review of the global and European state of the art and a systematic requirements analysis undertaken in consultation with dozens of European stakeholders.

The success of the Information Society depends upon improving trust and confidence in the information networks which citizens, businesses and governments are becoming increasingly dependent. Trust and confidence is however being undermined by increasing numbers of security incidents as malicious attackers exploit system vulnerabilities. These incidents also pose an increasing threat to society's critical infrastructures.

An important step towards addressing these risks would be to provide users with accurate, timely and useable information so that they can take the necessary steps to protect themselves.

Industry and EU Member States are taking some steps to provide this information but the risks and solutions are inherently transnational. Therefore:

Findings

- Policy makers, businesses and citizens need reliable information about electronic attacks and new threats and vulnerabilities.
- Experts and end-users agree on the need for a European initiative to supplement existing initiatives.
- The role of the initiative should be to ensure that an appropriate level of security information is available to all users of information systems in the EU. As far as possible, this information should be disseminated via existing, trusted networks. Information needs to be tailored to the specific requirements of different users.
- This will involve facilitating broader and more tailored provision of information to users.
- The deliverables of an information sharing initiative should include: warnings and alerts, threat assessments, helpdesk services and educational products.
- The tasks of an EU initiative should include:
 - Facilitating & stimulating development of CERTs
 - Enhancing performance of CERTs
 - Enhancing collaborative working amongst CERTs
 - Facilitating information dissemination
 - Facilitating added value analysis and assessment
 - Multidisciplinary research
- Customers for this initiative include policy-makers, senior managers, security managers, front-line staff, SMEs and the general public. The EU should focus upon SMEs and the general public, who are currently not well served.

- There is a need for strong leadership from EU institutions to stimulate and provide seed funding for an European-wide initiative.

Implementation of an EU initiative is not a straightforward process. This roadmap has identified three sets of tasks that need to be addressed before actual deployment can begin.

<p>Architecture</p> <p><u>Principle:</u></p> <p><i>Any initiative should comprise a small central organisation and build upon existing sharing networks</i></p>	<ul style="list-style-type: none"> • Analysis of the appropriate mix of an open/closed network model • Plan for integration with existing networks • Definition of requirements for a central facilitation body • Scoping of requirements for internal structure amongst experts • Specification of technical architecture for secure information sharing • Impact analysis of dissemination channels and mechanisms based upon gap analysis of user requirements
<p>Business Model</p> <p><u>Principle:</u></p> <p><i>A hybrid funding model should be adopted involving a mix of public and private sector funding</i></p>	<ul style="list-style-type: none"> • Detailed market research based upon marketing and demographic analysis of each category of potential customers • Societal cost-benefit analysis of alternative European funding models based upon each of the existing funding models • Analysis of possible added-valued services and opportunities for stimulation of new markets
<p>Legal</p> <p><u>Principle:</u></p> <p><i>Must operate in conformance with Community and national commercial codes & privacy legislation</i></p>	<ul style="list-style-type: none"> • Feasibility report on main legal challenges <ul style="list-style-type: none"> ▪ competition law ▪ data protection ▪ confidentiality ▪ liability

Contents

Preface	3
Executive Summary	5
Contents	7
1 Background	9
1.1 National and Sectoral Initiatives	9
1.2 The Global & Political Context for Future EU Initiatives	10
1.3 The DDSI Roadmap: Concept Development & Constituency Building	10
1.4 What's in a Name?	12
2 Is There a Need?	13
3 Roles	14
3.1 What Information?	14
3.2 Tasks	15
3.3 Measures of Effectiveness	16
4 Customers	17
5 Architecture	19
5.1 An Open or Closed Network?	19
5.2 Structure	19
5.3 Recommendations	21
6 Business Model	22
6.1 Government Managed Organisations	22
6.2 Public-private Partnerships	22
6.3 Private-sector-owned Sharing Organisations	22
6.4 Academic-sector organisations	23
6.5 A Business Process Analysis	23
6.5 Recommendations	25
7 Legal Considerations	26
7.1 Administrative Legal Concerns	26
7.2 General Commercial Legal Issues	27
7.3 Recommendations	28
Appendix 1: The Roadmap Process	29
The Workshop Process	29

Workshop 129

Workshop 2.....31

Appendix 2: Existing Capabilities32

Appendix 3: EC-supported CSIRT Initiatives33

Appendix 4: Workshop Participants34

Appendix 5: European CERTs & CSIRTs36

1 Background

The success of the Information Society depends upon improving trust and confidence in the information networks which citizens, businesses and governments are becoming increasingly dependent. Trust and confidence is however being undermined by increasing numbers of security incidents as malicious attackers exploit system vulnerabilities. These incidents also pose an increasing threat to society's critical infrastructures.

An important step towards addressing these risks would be to provide users with accurate, timely and useable information so that they can take the necessary steps to protect themselves. Although such information is available from various sources, it is generally not timely, comprehensive or reliable enough to enable users to protect themselves. Many users have no access to information and advice in forms they can use.

Industry and Member States are taking some steps to provide this information to stakeholders but the risks and solutions are inherently transnational; for instance, all European users need timely warning that a new virus is propagating through the Internet.

The need for a European wide initiative was recognised in the e-Europe 2002 Action Plan, which called for stimulating "public/private co- operation on dependability of information infrastructures (including the development of early warning systems) and improve co-operation amongst national 'computer emergency response teams.'" The June 2001 EC Communication on network and information security suggested to move towards a European Warning & Information System (EWIS).

In December 2001, the Transport/Telecommunications Council approved a resolution that called on Member States:

"by mid 2002 to review the effectiveness of national arrangements regarding computer emergency response, which could include virus alert systems, with a view to strengthening, where necessary, their ability to prevent, detect, and react efficiently at national and international level against network and information systems disruption and attack."

The June 2002 Seville Summit approved the draft eEurope 2005 Action Plan which included provision for a Cyber-Security Task Force. The CSTF:

"should become a centre of competence on security questions, e.g. to develop with Member States a concept for a European computer attack alert system; to facilitate cross-pillar discussion; to improve trans-border co-operation."

1.1 National and Sectoral Initiatives

These recommendations at EU level reflect intensive activity within the private sector and at national level to improve warning and information sharing.⁴

⁴ These initiatives have been comprehensively summarised in two sources. First, DDSI's workshops on early warning and its Country reports have covered in detail initiatives in EU Member States (see www.ddsi.org). Second, the Information Assurance Advisory Council in the UK covered global and US initiatives in detail in its paper *Sharing is Protecting* (www.iaac.org.uk).

The Computer Emergency Response Team (CERT®) and Computer Security Incident Response Team (CSIRT)⁵ concepts have become increasingly popular since the late 1980s and many European users in the corporate, academic and government sectors now benefit from the activities of CERTs/CSIRTs. Meanwhile, driven by US government policy, for-profit Information Sharing & Analysis Centers (ISAC) have emerged since the late 1990s to meet the needs of large companies in critical sectors.

In the USA, intensive efforts are underway to integrate existing warning & information sharing activities. For instance, there are initiatives underway to enable information exchange amongst ISACs. The Federal Government is also developing a Cyber-Warning & Information Network (CWIN) to link CERTs, ISACs and network operations centres.

Many EU Member States have begun to develop warning and information sharing systems that involve various elements of the private sector (e.g. ISPs, software vendors) and various public bodies and regulators (e.g. national infrastructure protection bodies; telecoms regulators). There is great variety in the models adopted by EU Member States and there are great differences in the extent to which such systems are operational and their breadth of coverage. Nonetheless, the overall trend is towards more integrated mechanisms involving the public and private sectors to provide timely warning and information sharing to government, companies and citizens.⁶

In addition to government-inspired initiatives and CERTs, an increasing number of ICT suppliers, from software vendors to communication service providers, are providing a range of alerting and monitoring services. These include provision of vulnerability alerts and patches; threat warnings and advisories; network monitoring; and managed security services.

1.2 The Global & Political Context for Future EU Initiatives

Though market forces and national initiatives are developing structures to improve collection, analysis and sharing of information, there is a danger that such initiatives will fragment or stovepipe in the absence of co-ordination. EU initiatives must be able to integrate with regional and global initiatives.⁷ Examples of such initiatives include the Global Watch Network involving the USA, UK, Canada, Australia and New Zealand and the APEC CSIRT Task Force.

EU initiatives also need to protect privacy and civil liberties, avoiding the negative public reaction that attended the mooted US Federal Intrusion Detection Network (FIDNET). European initiatives must also not disadvantage EU businesses with additional costs or burdens.

1.3 The DDSI Roadmap: Concept Development & Constituency Building

The DDSI Roadmap process⁸ aimed to develop strategic concepts and build a constituency for EU actions on warning and information sharing. The Roadmap process had two important features:

- i) It developed a strategic vision for action

⁵ In this paper, the terms CERT and CSIRT are used interchangeably. They are also taken to include related initiatives such as Warning, Advice & Reporting Points (WARP).

⁶ For a comprehensive review of initiatives, see the Country Reports at www.ddsi.org.

⁷ For instance, the UK, US, Canada, Australia and New Zealand have concluded sharing agreements. Belgium has done the same with Singapore and South Africa.

⁸ Detailed in Appendix 1.

- ii) It included consultations with a wide range of stakeholders comprising the CSIRT community, communications service providers, ICT suppliers, large corporate and government end-users, SME business associations, citizens groups and emergency management/law enforcement/critical infrastructure protection agencies.

The Roadmap was developed by asking this wide community the following questions, as laid out in Fig. 1:

- What is the state of the art? The dependability overviews presented in DDSI Workpackage 1 and 2 provided a comprehensive inventory of initiatives in Europe and around the world.
- Given existing provision, is there a need for further action at European level?
- What roles should any European initiative fulfil?
- Who should be the customers of any such initiative?
- How should an initiative be structured?
- What business model should be adopted?
- What legal issues need to be resolved?

The Roadmap Process has not provided definitive answers to all of these questions but it has made clear the options and laid out the issues that will need to be tackled before implementation of any new initiative. Further details of the Roadmap process can be found in Appendix 1.

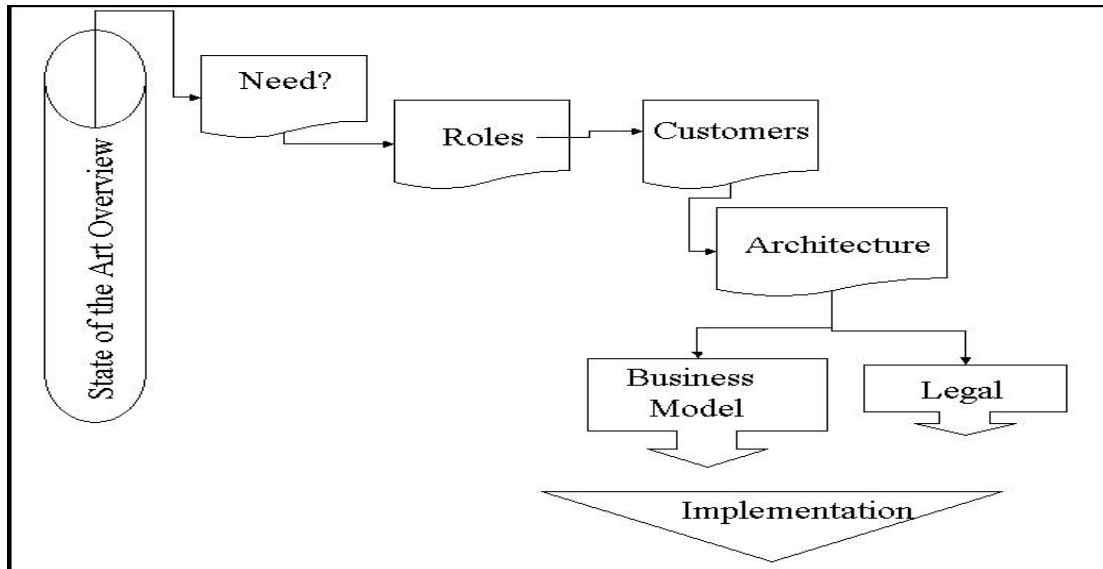


Fig. 1: Roadmap Process

1.4 What's in a Name?

Debate over a European initiative since 2000 has been complicated by the use of various terms. None of these terms is neutral as all can imply preference for one structural solution or another. Terms used include:

- EuroCERT. This was a pilot scheme run by Terena from May 1998 to September 1999.
- European Information Security Observatory (EISO). This term was used in Commission discussions with Member States and stakeholders in spring 2001. Although never developed, the EISO concept envisaged a body that could collect and disseminate information and act as both an operational liaison point for CERTs and a stakeholder discussion forum.
- European Warning & Information Sharing System (EWIS). This term appeared in the draft Commission Communication on Network and Information Security later in 2001. The draft communication proposed European actions both to stimulate the creation of CERTs, to network existing CERTs and to organise European level data collection and analysis.

The resolution adopted by the Council of Ministers in December 2001 did not include the term EWIS. Instead, it asked Member States to review their CERT and alerting provisions and requested the Commission to make proposals for a Task Force to respond to network security problems

- Cyber-Security Task Force (CSTF). The June 2002 EU Summit in Seville approved the eEurope 2005 Action Plan which, *inter alia*, called on the Commission to establish a CSTF by mid-2003.

One of the functions of the CSTF would be to “develop with Member States a concept for a European computer attack alert system.”

- Warning & Information Sharing in Europe (WISE). The title of a proposed FP5 project by an industry/CERT consortium to prepare a detailed roadmap for enhanced European capability to provide warning and information sharing.
- Cyberworld Awareness & Security Enhancement Structure (CASES). The title of a proposed *e-ten* project to link Member State CERT points of contact.

In many policy areas, it has been common to launch initiatives with a preconceived view of the organisational answer to a policy challenge. An important finding of the DDSI Roadmap is the need to start with a view of the service to be delivered to Europe's citizens and only then to systematically analyse the means by which that capability can be delivered.

2 Is There a Need?

European policy-makers have identified warning and information sharing as areas in which there are capability gaps. One of the aims of the DDSI Roadmap exercise was to examine this hypothesis by consulting with providers and users of information services.

Our consultations have indicated a consensus amongst providers and users that there is indeed a requirement for enhanced European-wide capability in this area. There is less of a consensus on the outputs or on how such a capability should be provided.

Our analysis and consultations indicate that:

- Governments and regulatory bodies need information about vulnerabilities, inter-dependencies, threats and incidents so as to devise policy responses
- Industry views better sharing of information about electronic risks as necessary for risk management and corporate governance
- Civil society seeks independent data about online vulnerabilities and threats to counter widespread “technical ignorance” about online risks

Most existing services provided by CERTs/CSIRTs within the EU deliver essential and highly technical services to tightly defined user communities. Whilst some countries are experimenting with national warning systems, as yet no Member State has a comprehensive warning and information sharing system that identifies its core community as all members of a certain nationality. Therefore, we have found that:

As the majority of citizens and small businesses do not fall into the government, academic or corporate communities, they have no adequate current level of information provision

3 Roles

The starting point for European action to improve capabilities for warning and information sharing must be a clear definition of the desired outputs and results.

It is first necessary to define the high level goals of European action. This roadmap proposes that the aim of European action should be⁹:

To ensure that an *appropriate level* of security information is available to *all users* of information systems in the EU.

This will involve facilitating *broader* and *more tailored* provision of information to users.

Broader provision is required since, whilst research, government and large corporate users of information systems have a degree of coverage from existing CERT and commercial services, coverage of the broader business community, SMEs and the public is minimal.

More tailored information provision reflects the fact that existing services do not yet meet the needs of all users.

3.1 What Information?

Information sharing on network security has many facets. Information may be shared about system behaviours; about vulnerabilities and exploits; about infrastructure dependencies and interdependencies; about aggregate threat trends and risk profiles; about real-time incidents and attacks; and about best practice solutions, including security awareness programmes.

EU policy documents have focused upon “warnings”¹⁰ and “alerts”¹¹ as the goals of enhanced European capabilities. In fact, these are necessary but not sufficient parts of the information services that should be provided.

The nature of network security is such that providing warnings/alerts alone will be of limited benefit. Warnings are likely to be both too general and too frequent to persuade users to take effective action. Most ICT users, in particular SMEs and individuals, lack the technical and operational knowledge required to respond to alerts. Providing warnings and alerts without also providing tailored advice and assistance may be worse than useless.

⁹ Decisions will need to be made about the extent to which the information focuses upon electronic attacks, versus, for instance, physical, natural or business threats. Decisions will also need to be made about the extension of the service to EU citizens and businesses based outside the territory of the Union and extension of the service to Newly Associated States.

¹⁰ **Warnings:** Urgent predictions about imminent short-term *threats* that often include information about the intent of attackers. Occasionally, longer-term specific warnings may be practical.

¹¹ **Alerts:** Collated and validated information about *vulnerabilities* gathered from sources including software vendors, CERTs and from detection monitoring. These can be disseminated individually in an ongoing trickle, or after collation as weekly or fortnightly bulletins.

In order to ensure effective management of network security risks across society, users need access to a set of products:

- | |
|--|
| <ul style="list-style-type: none"> • warnings and alerts • threat assessments • helpdesk services • educational products |
|--|

Warning products range from urgent warnings, to mid-term vulnerability alerts. Warnings and alerts trigger escalation of defensive status and the patching of vulnerabilities. It is important to define precisely the purpose of warnings; for instance, warnings of a virus outbreak need to be broadcast widely whereas warnings of a Distributed Denial of Service attack need to be channelled to key nodes, such as ISPs.

Threat assessments comprise aggregated trend and statistical information concerning the likelihood and impact of cyber-threats. They are necessary for policy-making and risk management, including risk sharing and transfer via insurance.

Broader helpdesk services are important to enable users to make effective use of warnings and alerts and to recover from incidents. In addition, when users receive help, they reciprocate by supplying detailed incident information that may generate warning products.

Education and outreach products range from best practice and standards development to dissemination, and mentoring activities and training for new CERT teams. The aim of education and outreach is to ensure that all information system users have an appropriate level of understanding concerning security and understand how to react and who to contact in the event of a security incident. In respect of most users, the real challenge is not simply production of more materials but rather communication and take-up activities.

3.2 Tasks

In order to achieve the goals outlined above, this roadmap proposes that the EU can add value to existing initiatives by focusing upon the following tasks:

- Facilitating & stimulating development of CERTs
- Enhancing performance of CERTs
- Enhancing collaborative working amongst CERTs
- Facilitating information dissemination & take-up
- Facilitating added value analysis and assessment
- Multidisciplinary research

Three initial projects launched under IST FP5 have made a good start in addressing some of these tasks. TRANSITS seeks to enhance CERT performance through training of staff; eCSIRT.net seeks to improve

collaborative working through developing data exchange; EISPP facilitates information dissemination by targeting the user requirements of SMEs.¹²

3.3 Measures of Effectiveness

Information sharing on network security operates in a resource-constrained environment. There are relatively few experts capable of providing warning, alerting and analysis services. Users of information, whether corporate or individual, have relatively limited desire for additional sources.

Therefore, any action at European level must add value to existing efforts and must not subtract value. For instance, it must not draw resources from operational units, confuse users with mixed messages or undermine existing trusted international sharing arrangements.

Any European investment should also be rigorously assessed to ensure it is achieving its goals. Metrics to assess the effectiveness of European action will be an important component of any additional activity. Measures of effectiveness in this domain are often simplified into input measures (e.g. number of warnings issued); anecdotal evidence (e.g. self-selected feedback from users); or financial measures (e.g. commercial sustainability of the service).

While these measures have the benefit of being easy to assess, a more reliable audit should be designed to address the impact of the information sharing investments against the EU's social and economic goals. Operational output metrics (e.g. rate of virus propagation before and after service enhancements) and user behaviour metrics (e.g. utilisation by users of warnings or educational products to patch software) could be combined with wider measures of trust and confidence.¹³

¹² These projects are detailed in Appendix 3.

¹³ See: Statistical Indicators Benchmarking the Information Society (IST-2000-26276)

4 Customers

Once the general products of an enhanced warning and information sharing capability at European level have been defined, these can be matched against the needs of potential customers.¹⁴

The five potential customers are:

- Policy-makers: who need reliable updates about electronic threats to assess potential national and international social and business implications
- Senior managers: who need threat and trend analysis to structure appropriate internal IT and operational controls and good corporate governance
- Emergency management/Information security managers: who need warning information to plan appropriate management responses to large-scale electronic attacks that can lead to operational, market and reputation disruptions and regulatory compliance failures
- Front-line staff: who need technically detailed information and data about recent, current and potential future attacks to develop protection, detection and reaction mechanisms
- SMEs and general public: these two actors require less-technically specific information to operate safely online and, at the same, acquire the necessary basic skills to implement information security management and technical procedures

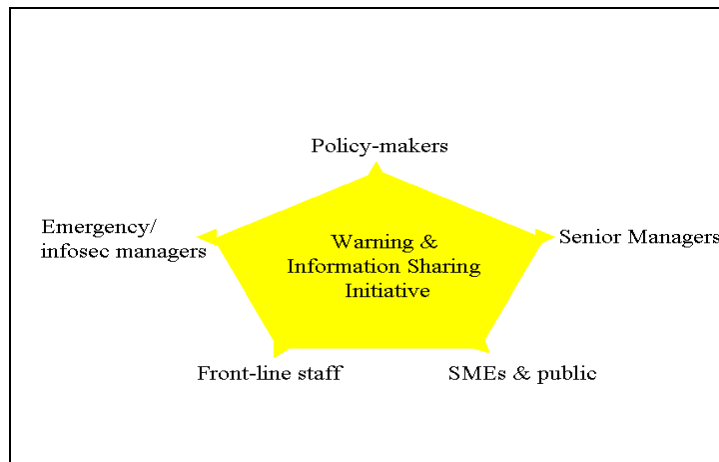


Fig. 2: Potential Client Structure for a Warning and Information Sharing Capability

These customers can be matched against the information products outlined above as follows in Fig. 3:

¹⁴ See the October 2001 and January 2002 Workshop reports for more detailed breakdowns of customers. The R&D community also requires various elements of this information.

	Warnings/alerts	Threat Assessments	Helpdesk	Education/ Best Practice
Policy-makers		X		X
Senior Managers		X		X
Infosec managers/emergency management	X	X		X
Front-line staff	X		X	X
SMEs & public	X		X	X

Fig. 3: Customer/Product Matrix

Within each category, each target audience will require various information products tailored to their needs.

5 Architecture

Once the tasks and customers are defined in detail, the next step is to undertake a detailed analysis of architectural and technological structures. There is substantial experience on which to build from other information collection, analysis and collection mechanisms.

The main challenges will be around building effective business processes that link added value European capability into existing networks.

5.1 An Open or Closed Network?

The customers listed above should not be viewed merely as recipients. They are also potential providers of data. In order to foster two way information exchange, it is necessary to create a two way sharing network, which can be either open or closed. In the first case, everybody can provide electronic attack information to the European network. In the second case, access to the network is restricted to selected individuals or organisations.

The main benefit of an open network is that collection and distribution of data involves a larger number of individuals. However, the quality of the information may be severely compromised due to widespread “technological ignorance” and also by the possibility of malicious insertion of misleading data.

In contrast, access to a closed network will be determined according to technical and professional criteria. There are already several examples of selection processes such as Terena’s Trusted Introducer Initiative CSIRTs¹⁵ and the Forum for Incident Response and Security Teams (FIRST)¹⁶.

Although the closed network approach may be more conducive to the satisfaction of legal, business and commercial requirements, it may also alienate those who are outside as they may not be allowed to provide electronic attack data. This is significant since it is important that any architecture permit the infrastructure to experience “**network externalities**,”¹⁷ i.e. a virtuous circle of growing use.

Any architecture should therefore allow for a larger number of actors to provide information, something that will benefit them and the incumbents of the warning and information sharing network.

5.2 Structure

Based upon wide consultation, this roadmap advises against the concept of a large, centralised coordination centre. This was felt to be unnecessary, impractical and ineffective. Instead, any European initiative should build on existing networks of trust and expertise since information sharing cannot be mandated but needs to be built upon voluntary trust relationships.

A European initiative should therefore be characterised as a programme of activities focused upon delivering the information and actions outlined above.

¹⁵ For more information see <http://www.ti.terena.nl/> (visited on 25 April 2002)

¹⁶ For more information see <http://www.first.org> (visited on 25 April 2002)

¹⁷ Concerning the notion of network externalities see Michael Katz and Carl Shapiro, 'Network Externalities, Competition and Compatibility', *American Economic Review*, vol. 73 no.3 (April 1985), pp.424-440.

It should have the following components:

- A small centre that would have the role of facilitating networking, undertaking analysis and assessment, facilitating best practice and guidance for security community. This centre could be either real or virtual.
- A network of experts who would form an active community in frequent contact. This network would be built on existing networks but would be extended outwards to ensure other networks of experts and dissemination channels were included.
- Dissemination channels based upon systematic analysis of the needs of differentiated audiences and partnerships with communication channels at sectoral and national levels.

The diagram below captures the structural requirements for a European network.



Experts would consist of individuals and organisations who originated analysed information products (warning, educational or assessments). These could include CERTs/CSIRTs/ISACs, R&D centres or government bodies. Disseminators would provide channels to users and could include business associations and corporate IT or security departments. CERTs and the like would also disseminate directly, so there would be overlaps between the categories. Users represent those individuals and organisations who are the victim of incidents and who need to take action to improve the security of their systems.

This model means that three distinct parts of the structure need to be developed.

- First, a small central body to facilitate networking.
- Second, the internal architecture, i.e. communication and collaboration between the experts. This is the sort of activity currently carried out through mechanisms such as TF-CSIRT and bilateral national agreements. This internal architecture needs to build upon these, often personal, trust relationships but needs to be expanded to include more organisations. This architecture poses a number of technical and organisational challenges including: procedures and techniques for secure and anonymised communication and reporting; trust relationships, possibly including certification procedures.
- Third, dissemination channels to users. The key point is that different end-users require different messages, different products and different levels of helpdesk support. Certain users are fairly well provided for, such as system administrators in large corporations and central government. Other users are hardly covered at all, such as home users and SMEs who require easy to act upon information and advice as well as access to more detailed info on pull basis.

Previous research has identified the key stakeholder and user communities and a start has been made on identifying the most effective communication channels and messages. The next step should be a systematic review of the gaps in provision.

5.3 Recommendations

Principle:

Any initiative should comprise a small central organisation and build upon existing sharing networks.

The next steps should be:

- Analysis of the appropriate mix of an open/closed network model
 - Plan for integration with existing networks
 - Definition of requirements for a central facilitation body
 - Scoping of requirements for internal structure amongst experts
 - Specification of technical architecture for secure information sharing
 - Impact analysis of dissemination channels and mechanisms based upon gap analysis of user requirements
-

6 Business Model

Any European initiative requires financial commitment. Consequently, a sustainable business and funding model needs to be devised.

A comparative analysis of existing warning and information sharing initiatives suggests four generic funding templates¹⁸:

6.1 Government Managed Organisations

These employ civil service or military personnel depending on their organisational setting. The National Infrastructure Security Coordination Centre (NISCC) in the UK and the National Infrastructure Protection Centre (NIPC) in the USA are examples.¹⁹ The former provides free information products (alerts, briefing and help-desk) to UK government institutions and, through its website, to the public as a whole. The NIPC's Infragard Program collects, analyses and disseminates electronic attack related data to the general public. Certain information is provided only to individuals and organisation with the appropriate security clearances.²⁰

Other examples are provided by France's CERT-A, the Netherlands' CERT-RO, Germany's CERT-BUND, and Finland's CERT-FI.

6.2 Public-private Partnerships

These partnerships come in various forms. One model is partially or wholly owned companies created by government institutions whose staff are a mixture of personnel from private and public organisations. An interesting example was **Action 2000**, a private company owned by the UK Department of Trade and Industry²¹ set up to tackle Y2K.

Another model is provided by the Belgian e-Security Platform (BIPT). This national virus alert system is a joint project of the Ministry of Telecommunications and stakeholders such as ISPs. Austria's CIRCA is likewise a partnership between the Federal Chancellery and the Austrian ISP Association. Norway's VDI, a joint project between the intelligence services and major companies to monitor intrusions, is an example of a more formal partnership for information exchange.

6.3 Private-sector-owned Sharing Organisations

Whilst an increasing number of organisations have their own CERTs/CSIRTs which sometimes interact through sectoral bodies or global structures such as FIRST, there are other bodies structured around, for instance, industry sectors that provide functionalities to their membership. These bodies have various

¹⁸ For more detailed assessments of these business models, see: European Warning & Information System: Issues & Options Paper for Workshop, 16 October 2001 and Information Assurance Advisory Council (IAAC), "Threat Assessment and Early Warning Working Group: Information Sharing Review" available at <http://www.iaac.org.uk>.

¹⁹ see <http://www.nissc.gov.uk> (visited on 21 April 2002) and <http://www.nipc.gov>. (visited on 21 April 2002).

²⁰ More information about this initiative is available at <http://www.infragard.net> (visited on 25 April 2002)

²¹ For more information see <http://www.taskforce2000.co.uk/> (visited on 25 April 2002)

structures. Some are run by for profit service providers, others are not for profit industry consortia. European examples include CERT-IST and CERT-Intexxia in France and BITKOM CERT in Germany.

A particular form of the privately-owned sharing organisation is the Information Sharing & Analysis Center (ISAC) which emerged from the USA in the late 1990s. ISACs have been formed in vertical industry sectors. They are funded by member subscription and often outsource the management of the service to a for profit provider. ISACs have had varying success; large companies seem willing to pay for some of their services but are often reluctant to share information with their peers.

In addition, a number of commercial organisations offer warning information as part of their broader range of security or network management services. Whatever the particular structure, the sharing of incident and vulnerability information is strictly regulated through contracts and service level agreements (SLAs).

6.4 Academic-sector organisations

These are academic initiatives that freely deliver their information and data to all interested parties. The primary example is Computer Emergency Response Team Coordination Centre (CERT-CC), based at Carnegie Mellon University.²² It collects and distributes information and data provided by CERTs based all around the world. Government organisations or national research bodies usually fund academic CERTs.

Some of these academic institutions are starting to provide commercial services. CERT-CC, for example, is delivering a premium service to members of the Internet Security Alliance, a joint initiative between CERT-CC and the US Electronic Industries Alliance, a leading US trade association. This move towards commercialisation is in part a result of declining funding from core government sponsors such as the Department of Defense.²³ AUSCERT in Australia, although based at a University, counts companies among its membership base.

In Europe, the trans-European academic network (TERENA) constitutes the most important forum for international networking and cooperation amongst CERTs, via its Task-Force CSIRT. Although originally an academic body, TF-CSIRT now also involves many private sector and government bodies.

6.5 A Business Process Analysis

A business model for a European initiative must take account of customers, funding sources and information providers. At one extreme it is possible to envisage a public sector model in which the EU and/or Member States fund the service and make the products free at point of use. Another extreme is a wholly for profit service in which the service is run on a commercial basis and all users are charged. In practice, most countries are experimenting with hybrid and partnership approaches. At European level, such an approach is also likely to be attractive. An important output of a European initiative would be to sensitive users to the value of information security. The service will need to be paid for by all users, even if indirectly.

²² For more information see <http://www.cert.org> (visited on 25 April 2002)

²³ For more information see <http://www.isalliance.org/aboutus/> (visited on 25 April 2002)

After an examination of customers, services and possible funding sources, this roadmap proposes a hybrid funding model along the lines of figure 4 below. The principle is that public funding is only used where the market will not provide; one of the purposes of EU investment would be to stimulate the market and so encourage the development of new markets, for instance for integrators and infomediaries.

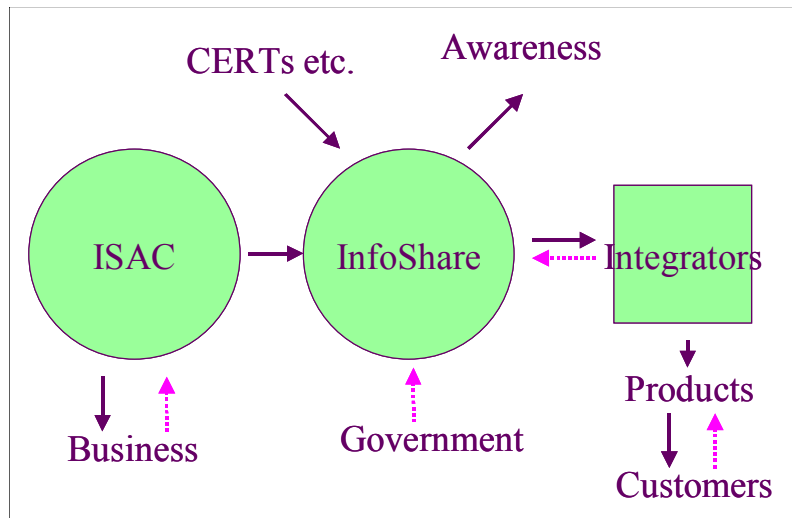


Fig. 4: A Funding Model

In Fig. 4:

- *Information flows are solid arrows. Funding and information flows are broken arrows.*
- *'Integrators' is used as a collective term to include ISPs, Vendors and Developers. It also includes Consultants, who would use information sharing to enhance the service they offered.*
- *'Business' is used to describe both large commercial companies and SMEs, and will also include some Integrators.*
- *'Infoshare' could be a deliverable of the European warning work; it could comprise a framework and solution components. The helpdesk function, perhaps the most costly component, may be best decentralised.*

6.5 Recommendations

Principle:

A hybrid funding model should be adopted involving a mix of public and private sector funding but sufficient public funding should be provided for the European capability to retain its objectivity. EU investment should be targeted to stimulate the development of a sustainable market for network security information.

European Commission actions should include:

- Detailed market research based upon marketing and demographic analysis of each category of potential customers
- Societal cost-benefit analysis of alternative European funding models based upon each of the existing funding models

Assessment of market opportunities provided by new ICT technologies and business models (wireless, web aggregators, the GRID, etc)

- Analysis of possible added-valued services and opportunities for stimulation of new markets
-

7 Legal Considerations

Whatever the business model chosen, any European initiative will face legal challenges.²⁴

7.1 Administrative Legal Concerns

The first legal issue would be the administrative status of any European central body or network. For example, this body may be established as a partnership or a semi-partnership. It is also viable to conceive the case of a company with or without limited liability. Alternatively, it may be established as a not for profit entity.

Whatever the specific administrative status, competition or “anti-trust” concerns may need to be addressed in the case of direct involvement of private sector entities. Due to the activities of this network and its expected membership, it is possible to consider this undertaking as a “horizontal agreement” between private companies.

Assuming that the main function of this body is to foster warning and information sharing, it is possible to speculate that it would not face anti-competition restrictions from the Commission. Therefore, it should restrict itself to “simple exchanges of information (statistics, market research or comparative studies)”. More importantly, it should “not involve any restrictions on the actions of the undertakings (i.e. private companies)” and any “recommendations that might induce parties to behave in an identical way”.²⁵

This European body may also want to undertake research and development projects. The Commission may allow competing private companies to cooperate providing that the following conditions are satisfied:

- a) joint research and development of products or processes with joint exploitation of the results
- b) joint exploitation of the results of the research and development jointly carried out pursuant to a prior agreement
- c) joint research and development of products and processes excluding joint exploitation of the results

The assumption above has been the establishment of a private entity to which companies and public institutions may have access upon the payment of some sort of due. However, it is also possible to consider the establishment of an agency as part of the European Union institutional framework. Whatever the staffing and geographical location, the main issue would be to determine carefully the degree and nature of authorised access to information submitted by public and private organisations.

This is particularly relevant if the electronic attack data may be related to criminal offences. Recent developments such as the proposed Council Framework Decision on attacks against information

²⁴ It should be noted that a substantial part of the resources devoted to establishing the IT-ISAC in the US was consumed dealing with legal issues.

²⁵ For more information see D.G. Goyder, *EC Competition Law*, (Oxford, Oxford University Press, 2002) or Alison Jones and Brenda Sufrin, *EC Competition Law*, (Oxford, Oxford University Press, 2001).

systems,²⁶ the creation of a European-wide arrest warrant²⁷ and the establishment of judicial cooperation structure like Eurojust,²⁸ will impact on the activities of this body.

Roadmap consultations failed to resolve the extent of law enforcement involvement in this network. In general, there was a recognition that there was some need for law enforcement visibility of data but that an intimate involvement of law enforcement in the network may hamper the open disclosure of information.

7.2 General Commercial Legal Issues

Whatever its proposed administrative status, a European network would be considered as an “information society service provider” according to the terms of the May 2000 European Union Directive on Electronic Commerce.²⁹ These activities may open this body to liability concerns.

First, this organisation may be viewed as liable in relation to the information it provides and disseminates. Information, for instance, may be incorrect or delayed. Further, actions based on the provided information may lead to additional vulnerabilities when implemented.

In addition to the potential liability issues related to the information disseminated, the body may also need to comply with business confidentiality requirements. This is particularly relevant if the body receives un-sanitised attack information from a private and/or public institution. Without legal and operational assurances about the preservation of this data, the body will not be able to fulfil its mandate since organisations will be reluctant to provide information and data.

Another legal issue to be addressed refers to the intellectual property rights concerning the data provided to this body. Although this point requires additional investigation, one option would be that the third party providing electronic attack data may forgo any commercial rights to it. However, the situation becomes more complicated in cases where a specific revenue-generating product (ad-hoc advisory or software security solution) is developed based on this freely provided attack data.³⁰

A final concern refers to the eventuality of the network handling personal information. In this case, it will need to fulfil all the necessary statutory requirements detailed in national and European data protection legislative measures.³¹

²⁶ European Commission, “Proposal for a Council Framework Decision on Attacks Against Information Systems” Doc. COM (2002) 173(01), 19 April 2002 available at http://www.europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf (visited on 25 April 2002)

²⁷ European Commission, Framework decision on the European arrest warrant and surrender procedures between Member States, available at http://www.europa.eu.int/eur-lex/en/com/pdf/2001/en_501PC0522.pdf (visited on 25 April 2002)

²⁸ For more information see the website of the European Justice Network at <http://ue.eu.int/ejn/index.htm> (visited on 25 April 2002)

²⁹ European Union, “Directive on Electronic Commerce” Directive 2000/31/C available at http://www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000L0031&model=guichett (visited on 25 April 2002)

³⁰ It is interesting to note that the US IT-ISAC appears to have taken a different approach to IPR from the FS-ISAC.

³¹ An interesting overview of the potential complexities associated with privacy and data sharing is provided in UK Cabinet Office, Performance and Innovation Unit, Privacy and Information Sharing: The Way Forward for Public Services (London: Cabinet Office, April 2002)

7.3 Recommendations

Principle:

Any initiative must operate in conformance with Community and national commercial codes & privacy legislation.

The Commission is invited to carry out the following initiatives:

- a detailed feasibility report on the main legal and operational hurdles potentially faced by this body
 - a detailed comparative analysis of legal frameworks of EU and non-EU member states in the area of warning and information sharing
 - establishment of a small legal team to both assist in the establishment of this body and to provide continuous legal support
-

Appendix 1: The Roadmap Process

DDSI used the following roadmap process:

- Country overviews that collected information about warning and information sharing initiatives from EU Member States, Newly Associated States, other states (e.g. USA, Canada, Australia) and international organisations.
- Focused surveys of providers of warning and information sharing services and selected end-users, using semi-structured phone interviews and participation in expert workshops, e.g. TF-CSIRT
- Preparation of background issues and options paper
- Knowledge capture and options analysis in two workshops:
 - *European Warning and Information System Workshop* co-organised by the Joint Research Centre of the European Commission and DDSI, Brussels, 25-26 October 2001; final report available at <http://ewis.jrc.it>
 - *Warning and Information Sharing: Technical, Legal and Commercial Issues* - 17-18 January 2002, Brussels; final report available at <http://www.ddsi.org>
- Draft of final roadmap; circulation for comment to identified stakeholders in Europe
- Final Roadmap completion

The Workshop Process

The October 2001 and January 2002 workshops were vital milestones in the development of this Roadmap. These workshops involved a wide range of stakeholders from both providers and users of warning and information sharing services. The workshops:

- enabled the roadmap to capture the state of the art and emerging trends in Europe
- enabled the roadmap to build and reflect a broad consensus on the way forward
- catalysed a range of initiatives to take practical steps towards implementation of the roadmap recommendations

The workshops were designed as short-term roadmapping exercises. The desired high-level end-state was floated in the issues paper presented to the October workshop and endorsed by participants. Discussions during the remainder of the workshop sessions focused around the short and medium-term steps that would be required to achieve this end-state.

The full workshop reports, presentations and background papers are available from www.ddsi.org but it is helpful to recap the main results here.

Workshop 1

The October 2001 workshop was intended to “advance the European Commission’s action on the development of improved EU capabilities to provide early warning” of network and information security

threats”. Workshop participants included CERT/CSIRT experts, telecoms and Internet Service Providers, ICT vendors, private sector end-users and public officials.³²

Workshop Questions

The workshop was structured around discussion of the following questions:

- What is the added value of a European Warning & Information System (EWIS)? In other words what is the European dimension of network security incidents and what is the rationale for transnational action and co-operation?
- What is required in terms of warning and information exchange? What is technically feasible?
- Who would EWIS serve and who would be engaged in the network?
- How might EWIS operate? How centralised/decentralised a model should be adopted?
- What actions are already underway in member states & industry that may be complemented by EU-level action?

Participants were asked to focus upon the following themes which were identified as central to answering the above questions:

- Social and economic aspects (e.g. business models, legal & privacy requirements)
- Business and end-user requirements including scope of EWIS (early warning; threat assessments; information exchange; alerting; response)
- Co-operation mechanisms (e.g. collaboration between CERTs & ISACs, interactions of CERTs with end users; funding and structural issues)
- Technical aspects (e.g. infrastructure for incident response, incident taxonomy, standardisation and security of data exchange, data aggregation, integration with intrusion detection/fault tolerant R&D initiatives, etc.)
- Legal aspects (e.g. liability issues, contractual issues, privacy/confidentiality requirements, etc)
- Global standards (e.g. establishment of common architectures with emerging global industry/government warning & alerting mechanisms)

Workshop Results

Workshop participants agreed that any European warning and information sharing capability should ensure an appropriate level of security information and advice to all users of information and network systems. A European capability should build on Europe’s existing networks of trust and expertise.

There was a majority view that a large, centralised coordination centre was unnecessary and should not be established.³³ Instead, participants agreed on the need to create **a small “added value” centre** to

³² The final report of this workshop is available at <http://ewis.jrc.it/>. Prior to the workshop, an issues and options paper was released to all participants. See Lorenzo Valeri, Andrew Rathmell, Michael Knights, Marc Wilikens and Marc Hohenadel, European Warning and Information System: Issues and Background Paper, Available at <http://ewis.jrc.it/>

³³ Though some participants did make the case for a more centralised, top-down structure along the lines of the CMU CERT-CC.

facilitate networking activities, to coordinate a group of experts and to define dissemination channels to cater to the needs of various users.

Delegates agreed upon several particular tasks for a warning and information sharing initiative:

- First, to stimulate warning and information sharing initiatives beyond the already established CERTs/CSIRTs and ISACs.
- Second, to structure training measures, as well as technical and management standards. These programmes should be organised to accommodate Europe's linguistic and cultural differences.
- Third, to develop multidisciplinary research approaches including "softer information security issues" related to human factors and social communication.

Workshop 2

The January 2002 workshop built upon these findings.³⁴ The workshop had the following aims:

- To consolidate the cross-sectoral and international community of stakeholders and other interested parties with a direct interest in early warning
- To provide analysis & recommendations on three priority topics:
 - Commercial and funding issues
 - Architecture
 - Legal Issues
- To prepare the way for future activities and initiatives in this area

Concerning the legal challenges, delegates emphasised concerns about data protection, privacy, competition, liability, intellectual property, criminal law and regulatory concerns in the context of the evolving EU legal framework concerning electronic commerce and telecommunication services.

In relation to commercial and funding issues, delegates focused on trying to structure the demand for a European warning and information sharing (WIS) body and, consequently, its revenue stream.

The architectural and technical discussions were devoted to assessing data collection, processing and distribution strategies. In addition delegates discussed the technical complexities related to providing data and information in different languages and timescales.

³⁴ The final report was prepared by Lorenzo Valeri and Andrew Rathmell and is available at <http://www.ddsi.org/DDSI/Events/>

Appendix 2: Existing Capabilities

An important finding of the DDSI Roadmap was that substantial capabilities already exist for providing information about dependability-related vulnerabilities and threats to European stakeholders. It is crucial to build on these existing structures since information sharing depends upon the establishment of trust relationships; this will differ in each industry and in each society.

This appendix provides an overview of the capabilities identified during DDSI. A full list of European CERTs/CSIRTS is attached as appendix 5. Further details of the initiatives can be found on www.ddsi.org.

CERTs & CSIRTS

There are currently some 120 members of FIRST around the world. Seventy nine are in Europe. These can be subdivided by category:

Academic/Research Network CERTs:	38
Government CERTs:	8
Private Enterprise CERTs:	30
General:	3

As noted in appendix 5, there are also a number of warning and information sharing initiatives such as CIRCA and BIPT which are not CERTs. A significant development in the past two years has been the evolution of government CERTs into bodies with wider remits, sometimes reaching out to industry or citizen users as a whole.

There are significant variations in national approach. For instance, the Netherlands has a great many CERTs, typically each connected to a single university, most are not involved in FIRST. However, two of the largest CERTS (CERT-RO and UNI-CERT) are connected to FIRST. By contrast, of the UK’s 13 CERTs, only one does not belong to FIRST. The UK also has the largest number of government-related CERTs.

ISACs

Commercial information sharing initiatives such as the US ISAC model are not yet well-established within the EU, though European organisations with US subsidiaries receive products via internal communications channels. The WorldWide ISAC, based in London, has a small number of members from UK-based end users. However, efforts to replicate US ISACs in the EU, such as the SAINT initiative in the UK, have been hampered by the reluctance of US-based market leaders to replicate the US experience. No European country has yet followed the South Korean or Japanese model of establishing a “national” ISAC.

Other Information Sharing Experiences

Both private and public sectors have long experience of information sharing at many different levels and through many different channels. Within economic sectors, notably banking and telecoms, there are long-established mechanisms for confidential exchange of information on fraud and crime. In safety-critical industries such as rail and air traffic, there are proven channels to encourage “no-blame” reporting of safety incidents. In the energy and electrical sectors there are facilities to share information on faults.

Appendix 3: EC-supported CSIRT Initiatives

The European Commission IST programme currently supports three CSIRT initiatives, which began work in 2002.

- *TRANSITS, Training of Network Security Incident Teams Staff*³⁵ (IST-2001-39118)

TRANSITS is a three-year European project to promote the establishment of Computer Security Incident Response Teams (CSIRTs) and the enhancement of existing CSIRTs by addressing the problem of the shortage of skilled CSIRT staff. This goal will be achieved by providing specialist training courses to train staff of (new) CSIRTs in the organisational, operational, technical, market and legal issues involved in providing CSIRT services.

In particular, TRANSITS

- develops, updates and regularly revises modular training course material
- organises training workshops where the course materials are delivered
- enables the participation of staff members of (new) CSIRTs in these training workshops, with a particular emphasis on the participation from the EU Accession States
- disseminates the training course materials and ensures exploitation of the results.

- *eCSIRT.net, European CSIRT Network* (IST-2001-37558)

eCSIRT.net focuses on the deployment of new techniques and practices that will satisfy the basic, nay existential, need of incident response teams (CSIRTs) to much more efficiently cooperate and exchange incident related data, and to collect shared data for statistical and knowledge-base purposes. The take-up of techniques in trial form that is proposed here will serve the following goals:

- 1) to enable a standardised and unambiguous exchange of incident related information between the CSIRTs involved;
- 2) to enable the collection of standardised and unambiguous incident statistics to serve the CSIRTs involved, and in a generalised fashion the public;
- 3) to enable the collection of standardised and unambiguous incident related data, followed by intelligent generation of warnings and emergency alerts, to serve the CSIRTs involved.

- *EISPP, The European Information Security Program* (IST-2001-35200)

The European Information Security Program (EISPP) project aims at providing European SMEs with IT Security services in order to give them the necessary trust in e-commerce which is important in developing their businesses. To meet the objectives of the project, a European consortium composed of highly competent and complementary technical and user/stakeholder partners has been created: the participants come from 7 different countries, and are prominent members of the IT security industry sector, from the service supplier sector and Universities. Some of them have close relations with SMEs, like Chambers of Commerce and Industry and CLUSIX, and will be key actors of the project. Through project completion, it is expected to set up an "open" European CERT network of expertise that will stimulate private/public sector co-operation in the prevention domain.

³⁵ <http://www.ist-transits.org/>

Appendix 4: Workshop Participants

Albert, Jason: Covington & Burling (on behalf of Microsoft)
Arvidsson, Jimmy: Telia AB HQ
Asher, Lawrence: IGSS - Integralis Global Security Services
Beccari, Giuseppe: TILAB
Bertagnolio, Luca: Cisco Systems Europe
Bierschenk, Hans-Joachim: BITKOM
Bircher, Daniel: Ernst Basler + Partners Ltd
Botterman, Maarten: RAND Europe
Bowden, Caspar: Foundation for Information Policy Research
Brouaye, Françoise: Ministère de l'éducation Nationale & Ministère de la Recherche
Bruno, Stefano: Ernst Basler + Partner
Bruschi, Danilo: CERT-IT/ CLUSIT
Bryant, Ian: Ministry Of Defence, UK MOD CERT
Burnett, Peter: NISCC, UNIRAS CERT
Christiansson, Henrik: Swedish Defence Research Agency (FOI)
Coolen, Rutger: TNO
De Stempel, Camille: AOL Europe
Deswarte, Yves: LAAS-CNRS
Dreyer, Cort: Netherlands Ministry of Trade & Industry
Dumortier, Jos: University of Louvain
Ehrhardt, Franziska: TimeKontor AG
Einzinger, Kurt: ISPA Internet Service Providers Austria
Gantzias, George
Gattiker, Urs E: EICAR
Gellert, Olaf: DFN-CERT GmbH
Gilles, André: CERTA
Giovenca, Pietro: Istituto per la Promozione Industriale
Haering, Kurt: Infosurance Foundation
Harris, John: PricewaterhouseCoopers
Harrison, John: Smart421/CSSA
Hellwig, Otto: Austrian Bundeskanzleramt
Henrik, Christiansson: Swedish Defence Research Agency
Herrero, Jose: ISEDEFE
Hohenadel, Marc C: Institute for the Protection & Security of the Citizen
Hubner, Gerold: Microsoft Germany
Jahren, Eivind: Netherlands Ministry of Trade & Industry
Jantsch, Susanne: IABG GmbH
Kelter, Ernst: IBM Germany
Koek, Mark: TERENA Trusted Introducer
Koeppel, Thomas: Federal Office of Police Affairs
Kossakowski, Klaus-Peter: Kossakowski GmbH
Lacey, David: Consignia
Laga, Joost: Cabinet of the Belgium Minister for Telecommunications

Leitert, Thomas: TimeKontor AG
Leemans, Hans: Member EuroISPA
Lointier, Pascal: CLUSIF
Luijff, Eric: TNO
Maj, Miroseaw: Head of Cert Polska
Manso, Candido: Head of Research
McCutcheon, Tom: Defence Science and Technology Lab
Micca, Stefano: TILAB
Miqueu, Michel: CERT-IST
Montolivo, Emilio: Securteam Marconi
Mullen, Thomas: British Telecommunications
Nevitt, Peter: Interpol
Pastor, Oscar: Ingeniería de Sistemas para la Defensa de España (ISDEFE) (ES)
Rafting, Anders: Swedish National Post & Telecom Agency
Rathmell, Andrew: King's College London
Rocca, Daniela: Studio Notarile Genghini
Rytzy, Rued: Swiss Federal Strategy Unit for Information Technology
Schweigert, Udo: Siemens-CERT
Silicki, Krzysztof: m
Spinellis, Diomidis: Department of Management Science and Technology
Spinks, David: EDS
Taylor, Pamela: CBI
Thornby, Charlotte: Sun Microsystems, Inc
Valeri, Lorenzo
Veit, Thomas: BSI-CERT/CERT-Bund
Vietsch, Karel: Terena
Verkuyl, Anne: Microsoft Europe
Wallström, Peter: Cell Network
Ward, Michael: BT Ignite Solutions
Welsch, Günther: Deutsche Telekom AG
Wilikens, Marc: JRC

Appendix 5: European CERTs & CSIRTs

Name	Funded by	Constituency	Products	Contact	FIRST
Albania					
1	INIMA	Government public?	Provides services to academic and research organisations.	inima@inima.al	No
Austria					
2	CIRCA		Authorised ISPs, ASPs and members of the public	Not technically a CERT: Incident Reporting Network Detection and alerting system Help and discussion lists Issues alerts and warnings	No
3	ACOnet-IRT	Federal Ministry for Education, Science and Culture	All sites and organisations connected to ACOnet (Academic and Research Network)	domain-admin@univie.ac.at	No

Name	Funded by	Constituency	Products	Contact	FIRST
Belgium					
4	BE-CERT	Belgian Government	Operated by BELNET the team provide services to Universities and Research Centres.	sst@belnet.be	No
5	BIPT	Belgian Government	Entire Belgian network	www.bipt.be	No
Bulgaria					
6	BGUUG-CERT	?	Major Universities in Bulgaria, all organisational members of BGUUG (ISP, IT companies, banks, etc.) and other UNIX-based organisations with Internet connectivity	www.bguug.bg/BGUUG-CERT/	No

Name	Funded by	Constituency	Products	Contact	FIRST
Croatia					
7 CARNet CERT		Service is provided to CARNet (Croatian Academic and Research Network) members. Since there is no other CSIRT team in Croatia, CARNet-CERT provides support for all organisations within Croatia (the ".hr" top-level domain).		c-cert@carnet.hr	Yes
Cyprus					
8 CYPRUS		Users of CYNET, the Cyprus university network (informal organisation – not strictly a CERT)		efty@zeus.cc.ucy.ac.cy	No
Czech Republic					
9 CERT-CZ		Academic and Research Network (?)		http://www.cert.cz/	

Name	Funded by	Constituency	Products	Contact	FIRST
Denmark					
10 CSIRT.DK	Private ISP	Internal and external customers of TDC A/S, ranging from domestic dial-up users to SMEs and large corporations	Information resource to customers Provides assistance following incidents	http://www.csirt.dk csirt@csirt.dk	Yes
11 DK-CERT	Public/private?	National organisation UNI-C. Danish research- and educational networks. Entire Danish community,	24x7 e-mail assistance Advice on potential risks Publishes warnings and alerts Co-ordinates information between parties involved	http://www.cert.dk cert@cert.dk	Yes
12 KMD IAC	Private ISP	Vendor customer base, Internal to host organisation, ISP customer base		http://www.kmd.dk alarmcenter@kmd.dk	Yes

Finland

13 FUNet CERT	Finnish Ministry of Education	ISP Customer base – Finnish University Network member organisations.		http://www.cert.funet.fi/english.html cert@cert.funet.fi	No
14 CERT-FI	Finnish Communications Regulatory Authority	All telecommunications network operators, service providers and end-users in Finland		cert@ficora.fi	No

Name	Funded by	Constituency	Products	Contact	FIRST
15	CERT-Intexxia Private company	ASP, ISP, high technology, industry, non profit, governmental organisations.	Daily bulletin on weaknesses Weekly statistics bulletin Co-ordinates response network	http://www.intexxia.com/cert.php	Yes
16	CERTA Government (SGDN/DCSSI)	All French public offices and services as well as local territorial offices.	Issues warnings, alerts Investigate incidents Coordinate resolution of incidents remotely.	http://www.certa.ssi.gouv.fr	Yes
17	CERT-IST French Industry	French industry and service sectors	Issues security bulletins, advice Vulnerability database On-site intervention Emergency contact number	cert@cert-ist.com	Yes
18	CERT-Renater French Government	French government, research and academic networks		http://www.renater.fr	Yes

France

Name	Funded by	Constituency	Products	Contact	FIRST	
19	CERT-BUND	German Government	Provides services to Federal Government departments in Germany	24x7 emergency response line Detailed incident analysis Security recommendations Warning and news service	certbund@bsi.bund.de http://www.bsi.bund.de/ce-rtbund/	Yes
20	ComCERT	Private company	Commerzbank Group.		contact@cert.commerzbank.com http://www.commerzbank.com	Yes
21	dCERT	T-Systems ISS	Customers of T-Systems	Daily and monthly information bulletins Emergency phone number Forums and seminars	dcert@dcert.de http://www.dcert.de/index_e.html	Yes
22	DFN-CERT	Private company funded by German Ministry for Science, Education, Research and Technology	German Universities, educational and research facilities or industrial research facilities.	Issue information bulletins Provide assistance if an incident occurs	dfncert@cert.dfn.de	Yes
23	PRE-CERT	PRESECURE Consulting GmbH	PRESECURE Consulting GmbH, associated partners and customers	Training in network security Incident response consulting	https://www.pre-secure.com precert@pre-secure.de	Yes

Germany

Name	Funded by	Constituency	Products	Contact	FIRST
24 RUS-CERT	Stuttgart University	Internal to host organisation	Will perform scans of networks Provide information on website Examination of password security	http://cert.uni-stuttgart.de	Yes
25 S-CERT	German Savings Banks Organisation	Internal to host organisation		cert@s-cert.de	Yes
26 Secu-CERT	Secunet Security Networks AG	Internal to host organisation		http://www.s-cert.de security@secunet.de	Yes
27 Siemens-CERT	Siemens AG	Internal to host organisation – based in Germany and US.	Private server (not on WWW) deals with all incidents	cert@siemens.com	Yes
28 T-Network CERT	ISP	Deutsche Telekom AG		http://www.telekom.de	No
29 Telekom-CERT	Deutsche Telekom AG	Internal users of the Deutsche Telekom AG and their subsidiaries with stock-majority	(Private server) 24x7 service	CERT@telekom.de	Yes

Greece

30 GRNET-CERT	Government?	Greek National Research Network	Responds to incidents Provides information	grnet-cert@grnet.gr http://www.aegean.gr/grnet-cert	No
---------------	-------------	---------------------------------	---	---	----

Name	Funded by	Constituency	Products	Contact	FIRST
Hungary					
31	HungarNet-CERT	Member organisations of HungarNet (Academic and research network) and the member's networks.		cert@if.hu	No
Iceland					
32	Isnet CERT			http://www.cert.isnet.is/	No
Ireland					
33	JANET-CERT	See UK JANET-CERT entry.			
Italy					
34	CERT-IT	Milan University	Seeks to raise awareness of security issues. Promotes new research Incident handling Mailing list and discussion fora Statistics	http://security.dsi.unimi.it	Yes
35	GARR-CERT	?	Assist in incident management Disseminate warnings and alerts Training in network security Product development	http://www.cert.garr.it/	No

Name	Funded by	Constituency	Products	Contact	FIRST
36 SSG	University of Salerno	Scientific and academic communities of Central Southern Italy		http://cert.unisa.it	No

Lithuania

37 LithNet NOC-CERT		Service is primary provided to all LITNET (academic) users but team also serves for the whole ".lt" domain.	9-6 Monday-Friday contact	http://www.litnet.lt/cert	No
------------------------	--	---	---------------------------	---	----

Luxembourg

38 Lux-CERT		All sites (connected to the Net or not) physically located in Luxembourg are invited to become members of LUX-CERT	Public: Information services; Mailing List Constituents: Help Desk; Incident Response; Mailing Lists; Statistical data.	http://www.cert.lu/	
----------------	--	--	--	---	--

Name	Funded by	Constituency	Products	Contact	FIRST
Macedonia					
39 MARNet CERT	Sts. Cyril and Methodius University, Skopje	Users of MARNet, Academic and Research Institutes.	Responds to and resolves problems within the “mk” domain Issues incident information to MARNet users (planned) Training on computer security	http://ii.pmf.ukim.edu.mk/marnet-cert/	No

Netherlands

40 AMC CERT	?	Academic Medical Centre (Amsterdam)	Emergency contact e-mail	http://www.amc.uva.nl/cert/	No
41 CERT-IDC	Energis N.V (ISP)	Banking Organisations and Top 500 Dutch Industry		http://www.energis-idc.net	No
42 CERT-KUN	Nijmegen University	Organisations and employees of Nijmegen University	Incident co-ordination and advice	http://www.kun.nl/cert	No
43 CERT-NL	Hosted by SurfNet, but includes employees from the CERT NL constituents	Higher Education institutes and many research organisations in the Netherlands	Handles all incidents involving SurfNet customers, either as victim or suspects. Daily bulletins and alerts.	http://cert-nl.surfnet.nl	No

	Name	Funded by	Constituency	Products	Contact	FIRST
44	CERT-RO	Government funded	Central government organisations	Coordination of incidents Central point of information – stores reports from other CERT's too Provides advice on security	http://www.cert-ro.nl/	Yes
45	CERT-RUG	Rijks University of Groningen	Internal to host organisation	Emergency contact number	http://www.rug.nl/securit y	No
46	CERT-UU	Utrecht University	Internal to host organisation	Security bulletins (also those from other .NL CERT's on website) Emergency contact number	http://www.cs.ruu.nl/cert -uu/	No
47	UNI-CERT	KPN Telecom	All customers of KPN Telecom	Solve customer security problems. Advises customers on security related issues. Patches available on website	http://www.uni-cert.nl/	Yes
48	UvA-CERT	University of Amsterdam	Internal to host organisation	24x7 Emergency contact	http://ic.uva.nl/cert/	No
49	KCSIRT	nl.tree b.v	Schools	Normal service during daytime	http://www.trusted-introducer.org/teams/team-s-k.html#KCSIRT	No

Name	Funded by	Constituency	Products	Contact	FIRST
50 UNINETT	Royal Norwegian Ministry for Church, Education and Research	All Norwegian universities and colleges, non-commercial research institutions and other research- and education-related institutions	provide assistance on handling and investigating incidents Information bulletin Advice on network security Relaying of information to other CERT's.	http://cert.uninett.no	Yes
51 VDI	Government & industry	Large corporations; public administration	Network & intrusion monitoring; incident reports; threat assessments		

Norway

Name	Funded by	Constituency	Products	Contact	FIRST
Poland					
52 Abuse TP S.A	Tpnet	All users, sites and organisations connected to Tpnet.	Incident co-ordination Alerts and warnings	http://www.tpnet.pl/abuse-english.html	No
53 CERT POLSKA	Government?	Naukowa i Akademicka Siec Komputerowa (Research and Academic Network)	Provide statistics and information on incidents Technical assistance and advice Issues alerts and warnings	http://www.cert.pl	Yes
54 POL34	Poznan Supercomputing and Networking Centre	Systems connected to Polish Scientific Broadband Network POL34/155 (i.e. networks of most academic and scientific institutions in Poland)	Incident investigation and coordination Technical advice (Limited) technical response Information sharing with other CERTs	http://cert.pol34.pl	No
Portugal					
55 CERT.PT	Ministry of Science and Technology and the Ministry of Education	Portuguese Academic and Research National Network	?	http://www.fccn.pt/RCCN-CERT/CertTeam/	No

Name	Funded by	Constituency	Products	Contact	FIRST
------	-----------	--------------	----------	---------	-------

Scandinavia

56	NORDUNet	Danish Limited Company owned by the Nordic Ministries for Research and Education	The Nordic Academic CERT Teams; DK-CERT; FUNET CERT; ISnet CERT(Iceland); Uninett CERT; SUNET CERT	Incident handling Advise the Nordic national networks Dissemination and coordination of information	http://cert.nordu.net	Yes
----	----------	--	--	---	---	-----

Slovenia

57	SI-CERT		ARNES, Academic and Research Network of Slovenia	Coordination of security incidents Distribution of security-related information to the constituency. Providing technical expertise on network security related issues.	http://www.arnes.si/english/si-cert	Yes
----	---------	--	--	--	---	-----

Name	Funded by	Constituency	Products	Contact	FIRST
58	EsCERT-UPC (Universitat Politècnica de Catalunya), but is now self-funded.	Internal to UPC organisation, but available to all companies/organisations in Spain	Information dissemination Can be contracted to: <ul style="list-style-type: none"> Coordinate incidents Give technical assistance 	http://escert.upc.es	No
59	IRIS-CERT RedIRIS (Spanish Research and Academic Network)	Full Service to all organisations connected by RedIRIS. Limited Service (incident handling and coordination with other IRT's) for hosts under the .es domain.	Incident detection Coordination of incident handling Advice and alerts Training and technical advice	http://www.rediris.es/cert/index.en.html	No
60	SIAPI-CERT Siapi Networks; Eleno, Morell & Sanchez Asociados S.L.	Full service to all organisations connected by Siapi Networks and/or advised by Eleno, Morell y Sanchez Asociados S.L. Limited service to others		cert@siapi.es	No

Spain

Name	Funded by	Constituency	Products	Contact	FIRST	
Sweden						
61	SUNNet-CERT	Ministry of Education and Science.	SUNet connects universities, higher education- and research organisations in Sweden. SUNNet CERT serves these.	Provide advice and assistance on network security	http://www.cert.sunet.se	Yes
62	Telia	Telia AB	Internal to host organisation		http://www.telia.net	Yes
63	UU-IRT	All networks of the University of Uppsala.	Emergency contact e-mail Advice on threats		http://www.irt.uu.se	No

Switzerland

64	CERN	EU	Responsible for CERN, the European Organisation for Nuclear Research	Advice on password security Warnings and alerts Security scans Advice and information	cert@cern.ch	No
65	IP+CERT	Swisscom	All customers of the Swisscom IP-Plus Internet Services	Provide advisories and an information archive	http://cert.ip-plus.net	Yes
66	ITC	T-Systems	Customers of T-Systems	Security bulletins Risk management Early warning systems Certification	http://www.t-systems.ch/itc_security/	No

Name	Funded by	Constituency	Products	Contact	FIRST
67 OS-CSIRT	Open-Systems AG	Customers of Open Systems AG, managed security provider	?	support@open.ch	Yes
68 SWITCH		Swiss academic and research network.	Advises customers on security issues Not a 24x7 service	http://switch.ch/security	Yes

United Kingdom

69 BTCERTCC	British Telecom	Computer security incidents involving BT's own-use computer systems and networks	24x7 monitoring of BT networks Handles all reported incidents	http://www.btcert.bt.com	Yes
70 BT SBS	British Telecom Ignite	Customers of BT Ignite Solutions who subscribe to the Secure Business Service product and reach the Vigilance stage.	Consultancy offering Advice on risk management, security architecture and policy. Benchmarking. Certification Vigilance (24x7 intrusion detection)	http://www.btignitesolutions.com/security/	Yes
71 CITIGROUP	Citigroup	Citigroup (employees/contractors)	?	first-team@citicorp.com	Yes

Name	Funded by	Constituency	Products	Contact	FIRST
72 DAN-CERT	DANTE?	TEN-155 ("ten-155.net") and DANTE US ("dante.net") customers (the European national research networks).	Coordinates incident response between the European national research networks connected to TEN-155, and between TEN-155 and the US.	http://www.dante.net/sf/	Liason
73 E-CERT	Energis Squared Limited	Customers of Energis Squared Limited, and internal users.	?	http://www.energis.co.uk/support	Yes
74 EUCS-IRT	Edinburgh University	All networks of the University of Edinburgh	?	irt@ed.ac.uk	No
75 JANET-CERT	JNT Association Ltd, trading as UKERNA	Customers of the JANET network; higher and further education and research organisations in the UK & Ireland	Emergency incident response assistance Publish advice Deliver training courses	http://www.ja.net	Yes
76 MLCIRT	Merrill Lynch	All employees, contractors and staff of Merrill Lynch.	24x7 Service	first-team@ml.com	Yes
77 MODCERT	Ministry of Defence	Internal to host organisation	Central Co-ordination Centre; A number of Monitoring and Reporting Centres (MRCs); Warning, Advice and Reporting Points (WARPs); Incident Response Teams (IRTs).	http://www.mod.uk/cert/	Yes

Name	Funded by	Constituency	Products	Contact	FIRST
78 OGCBS	Office of Government Commerce in the Treasury	Domestic OGCBS and customers of OGCBS Internet services.	?	http://www.ogcbuyingsolutions.gov.uk/	Liaison
79 OxCERT	University of Oxford	All networks of Oxford University	Security scans Advice and information	oxcert@ox.ac.uk	Yes
80 Q-CIRT	QinetiQ	Research, managed IDS customers	Consulting services including risk assessment and health checks for business; Firewall management, intrusion detection and forensics; Training people on IT security systems	http://www.qinetiq.com/services/security/data_security/index.asp	Yes
81 UNIRAS	Government – NISCC	UK government departments and agencies, companies holding sensitive government contracts, Critical National Infrastructure (CNI) organisations.	Real-time help desk and early warning function. Emergency helpline. Warnings and information. Co-ordinates the NISCC's EARG, which responds to serious electronic attack incidents affecting the CNI.	http://www.uniras.gov.uk	Yes

Dependability Development

DDSI

Support Initiative

DDSI

DDSI
IST-2000-29202

For more information on the project DDSI,
please visit

www.ddsi.org

Project number IST-2000-29202,
supported by
the IST research programme
of the European Community,
managed by
the European Commission DG
Information Society.

