

Dependability Development

DDSI

Support Initiative

**DDSI
IST-2000-29202**

**Securing the Information Society:
A European Policy Agenda**

Summary of DDSI findings

November 2002

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



DDSI

These findings were developed as a result of the following analysis undertaken by the DDSI project team: a conceptual review of the issues from the technical, business and societal perspectives; a global inventory of dependability-related policies in international organisations, leading non-EU states and all EU and Newly Associated States; in-depth analysis and workshop-based consultations on three priority issues – public private partnerships; warning and information sharing; Research & Development All project documentation is available at www.ddsi.org

Report Version: Final
Report Preparation Date: 1 November 2002
Classification: Public
Preparation led by: RAND Europe (NL)

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)

Dependability and information security are increasingly recognised as vital elements for ensuring wide participation in the Information Society. The success of the Information Society depends upon trust and confidence in our information infrastructures; this involves effective management of risks.

What if?

The year is 2010, ten years since European leaders tied Europe's economic future and social development to the success of the Information Society. European citizens, businesses and public authorities are immersed in a global ambient intelligent environment in which their mobile, always on Internet connections provide a range of services ranging from health-care to integrated transportation management. Economic growth has been stimulated by the integration of information networks into business value chains; citizen services and democratic participation have been enhanced by the adoption of e-government practices.

However, in order to achieve this result, major efforts were needed to move from a situation in which information networks were notoriously insecure to one in which risks are routinely understood and effectively managed. Significant innovations in relation to policy, legislation and policing, organisational structures and technology were necessary to prevent the emergence of an electronic society in which confidence in information networks was undermined by a tide of cyber-crimes and infrastructure disruption. Without these innovations, increasingly complex applications and infrastructures would have led to a proliferation of vulnerabilities. These could have been exploited by cyber-criminals and cyber-vandals to attack corporate and government systems; it may have been beyond the capacity of under-resourced law enforcement and archaic legislation to deter and catch these attackers. The result would have been that public confidence in e-government and e-business would never have been able to develop. Further threats could have included wide-scale disruptions to Europe's other critical infrastructures, which have all become dependent on the information infrastructure.

Fortunately, the infrastructure and systems developed across Europe have created a situation in which information infrastructures are dependable and in which information systems reliably support power, transportation and government services. The economic and social gains of the Information Society could have never been so great without the justified trust that European citizens now have in their information systems.

The Business Case for Action

Information and Communication Technologies hold the potential to revitalise European businesses, to spur economic growth and competitiveness and to revolutionise working practices. However, customers and business partners will only use electronic networks if they can be trusted. Today, cyber-crime and information security incidents are deterring consumers and imposing costs on businesses. Tomorrow, as organisations become ever more dependent upon networks, insecurity will be a business critical issue.

Although corporate leaders are increasingly aware of the importance of managing information risk, many lack effective controls. For instance, a fraction of European companies have achieved compliance with the most common industry standard for information security management.

In the Knowledge Economy, only companies that build a trusted brand will succeed. Companies that fail to build this trust, in part through building dependable networks, will lose customer confidence, be overtaken by their competitors and face liability and regulatory pressures.

Table of Contents

The Challenge.....3

Managing the Risks.....5

A Framework for European Policy.....6

Proposals for Action8

 Industry8

 Individual Member States.....8

 Role of the European Commission9

 Legal & Law Enforcement.....9

 Awareness & Market Stimulation10

 Operational Support10

 R&D.....10

 Europe’s Contribution to International Governance10

ANNEX 1: Findings from Dependability Policy Overviews11

 Summary of Findings of National Dependability Policy Overviews11

 Summary of Findings of International Dependability-relative activities.....12

ANNEX 2: Findings of DDSI Policy Roadmap Exercises.....14

 Warning and Information Sharing: Main Findings.....14

 Research and Development: Main Findings.....16

 Public/Private Partnership: Main Findings19

Annex 3: DDSI Project Final Report21

The Challenge

A review of policy initiatives undertaken by EU and Newly Associated States as well as by leading non-EU states and international organisations indicates a consensus that the hoped for benefits of Information & Communication Technologies (ICT) for business, public affairs and citizens will only be realized if there is trust and confidence in these systems. There is growing awareness of the risks in today's reliance upon networked information systems and of the need to manage these risks through integrated policy approaches.

The challenge is that, as the economy becomes more dependent upon electronic communications and upon the Internet, critical business and social processes are becoming more vulnerable to accidental or malicious failures in information systems. Most visions for the future of ICT, including EU Information Society visions of an ambient intelligent environment in which mobile and embedded devices are linked into always-on communications networks, depend upon robust, secure and resilient networks. This vision is at risk if a combination of growing vulnerability and increasing threats is not adequately addressed.

Vulnerabilities in today's information systems are all too evident. Commercial software and the Internet were not designed with a focus upon dependability,¹ with the result that vulnerabilities have been increasing at the same time as business and citizens have become more dependent upon these systems. Vulnerabilities are injected into our information systems at many levels; from poor initial coding of software by vendors, through ineffective management controls imposed by companies, to the insecure practices of individual citizens. Despite a greater focus upon trust and security in recent months by software vendors, the growing complexity of information systems, commercial pressures to be first to market and a rapidly growing population of individual users, often using always on and mobile devices, means that our vulnerabilities are likely to increase in the near future.

Disruptions of information systems are mostly a result of human error, ranging from system integration mistakes to accidental cutting of fibre optic cables, and natural disasters, such as weather conditions. Malicious attacks are only one source of failure. However, the incidence of deliberate attacks on information systems is increasing. Whilst there is a lack of good, comparable data, available surveys and criminal statistics point to rising levels of cyber-vandalism and crime. Most governments surveyed also emphasise the emerging risk of more serious disruption by cyber-saboteurs and terrorists.

An additional reason for vigilance is the growing convergence between the information infrastructure and other societal infrastructures. The Information Society is not just about the delivery of e-government to citizens, Business to Consumer or Business to Business services. It is about the integration of ICT into all infrastructures to make efficiency gains. Physical control systems, for instance in the water and power sectors, are increasingly migrating online whilst the extended value chains of most industries have become dependent upon ICT and make more and more use of public telecommunications networks and the Internet. Therefore, disruptions to the information infrastructure are likely to rapidly propagate across other infrastructures. The degree and nature of such "cascading" effects is being examined by some governments but remains poorly understood.

¹ DDSI views security (comprising Confidentiality, Integrity & Availability) as a component of dependability.

This combination of vulnerabilities and threats is already impacting upon efforts to build an Information Society. Surveys throughout the EU and further afield demonstrate that public concerns over online security are one barrier to the growth of e-business and the take-up of e-government services. Governments and businesses alike recognize that improving public trust and confidence in information networks is an important policy goal. Public safety, especially in the light of a heightened terrorist threat, is also a concern given the potentials for systemic disruption posed by threats to globally connected and interdependent information-based infrastructures.

Managing the Risks

DDSI's inventory of global policy developments has revealed no single "magic bullet" to ensure information infrastructure dependability. This area poses peculiar challenges for policy-makers because the dependencies are so pervasive, the vulnerabilities so poorly understood (and dynamic), and ownership of the solutions is so widely dispersed. Furthermore, policy and operational responses will always be in part dependent upon the social, political, economical and legal frameworks in place. Three general conclusions can nonetheless be drawn.

1. The challenge must be dealt with by public authorities in a joined up manner. Information infrastructure dependencies affect all areas of government, business and society. Solutions will not come from any single domain. Governments will need to adopt a balance of policies taking into account all aspects including national security, criminal justice, public safety, commerce, and the interests of citizens.

In EU terms, this leads to the observation that information security and dependability is inherently a cross-pillar challenge requiring an integrated response.

2. Neither the market nor the state alone can solve the problem. Most governments have acknowledged that the state alone cannot secure society's information networks. They have also concluded that the market alone is unlikely to build sufficient security and resiliency into these networks. Therefore, public intervention is required to fill the market gaps and to stimulate market action. However, modern infrastructures are "joint products" and need novel governance mechanisms.

Partnership approaches are needed to ensure joint action by all stakeholders.

3. Information infrastructure risks are inherently transnational. Governance solutions must therefore be found not only at the European level but at the global level. Solutions to the risks brought about by our dependence upon interconnected, vulnerable information networks are being sought by Europe's partners, such as in North America and Asia, as well as via international bodies such as the Council of Europe, G-8, OECD, UN and ITU.

Any EU effort needs to engage actively at the international level.

A Framework for European Policy

The risks posed to society by dependence upon interdependent networked computer systems have been recognised for some time. What is new is the combination of a rising threat from malicious attackers with the evolution of the global information infrastructure into the pervasive “nervous system” of contemporary society.

Many of the solutions to these risks are likely to come from the private sector which has a growing stake in ensuring the dependability of business critical systems. The market is now moving to develop mechanisms to reduce, transfer and share the risk but there are areas that the private sector cannot address, such as law enforcement, and areas in which there are market failures, such as the lack of a mature insurance market. In general, the state retains important responsibilities for providing a trusted framework for commerce, for public safety and for delivering e-government and e-democracy.

Member States have endorsed the view that public policy will therefore play an important role in helping society to manage these risks. Indeed, they have asked the Commission to undertake a number of initiatives to promote dependability and security.²

At present, management of information infrastructure dependability risks is a matter of “retrofitting” dependability functionalities. At one level, this is evident in the way that users have to expend time and effort installing software patches. At another level, it is evident in the way that computer crime legislation and policing practice is constantly under pressure to catch up with new technical and criminal developments.

To build robust foundations for the European Information Society, dependability needs to be “engineered in” to Europe’s information infrastructures. A review of global practices and lessons learned demonstrates that there are a range of issues that need to be addressed and that there are a range of policy instruments that can be used to build a robust information infrastructure and a society that is resilient in the face of new threats.

Many of these measures are being undertaken, or being considered, by individual EU Member States. Since the dependability of anyone entity connected to an information network is dependent upon the dependability of the weakest link in the chain, it is important that Europe acts at three levels. First, ensure that all Member States (and Newly Associated States) implement adequate levels of dependability within their jurisdictions. Second, ensure that actions requiring coordinated, European-wide action are undertaken by European institutions, Member States and other stakeholders. Third, ensure that Europe as a whole contributes to international efforts to manage risks arising from dependence upon information networks.

Based on the analyses of the current state of affairs as reported in the country reports and on detailed discussions with experts and stakeholders, DDSI has devised the following schema of policy actions grouped around the elements of good practice in dependability policy. This schema provides a model for implementation at the level of individual Member States, the EU as whole and for EU intervention in international initiatives. The schema recognises that both accidental and malicious faults are important; that there is a dependent relationship between the two (for instance, many cyber-attacks depend on “accidental” vulnerabilities in software); and that some policies will address both problems. Most attention is however given to addressing

² See: *Council Resolution on Network & Information Security* (28 January 2002); *eEurope 2005 Action Plan* (June 2002).

risks arising from malicious behaviour, since these threats are increasing rapidly and there are not yet well established policy responses.

Three important concepts underlie the DDSI recommendations. First, the need for states to encourage the market to lead development of solutions rather than imposing unnecessary regulatory burdens. Second, the importance of promoting a “culture of security” in accordance with the OECD Guidelines on Information Security. Third, the concept of the “weakest link.” All participants in global networks are as vulnerable as the weakest link in the chain. Therefore, a culture of security needs to be inculcated based on the translation of today’s sound practices into minimum standards that all stakeholders are expected to meet, whilst striving to implement best practices.

The proposed schema includes the following elements:

- ***Policy Making Mechanisms***
 - The need for a central policy lead
 - The need for a strategic, cross-pillar approach
 - Partnerships among all stakeholders
- ***Deterrence***
 - Development of criminal justice mechanisms to deter cyber-abuse
 - Development of educational programmes to prevent cyber-abuse
 - Strengthening of deterrent and investigative measures to counter “high-end” cyber-threats
- ***Protection***
 - Promotion of dependable software & system design and implementation
 - Promotion of information governance & security management good practice, including management tools
 - Updating, revision and wider dissemination of standards such as Common Criteria and ISO17799
 - Promotion of dependability aware cultures & education encouraging ethical and responsible user behaviour
- ***Detection***
 - Promotion of warning and information sharing initiatives
 - Development of reliable statistical indicators for trend analysis
- ***Risk Management***
 - Policy should be informed by the principles of risk assessment, risk reduction, risk transfer and risk sharing
 - Encouragement of good practice in business continuity & risk management
 - Development of scaleable risk management methods across interdependent infrastructures
 - Development of uniform criminal codes and law-enforcement procedures
 - Provision of emergency and consequence management capabilities able to deal with systemic risks on a European-wide basis

Proposals for Action

To date, dependability has lagged behind new technologies and infrastructures. Europe has, in general, lagged behind in the Information Revolution. Europe now has a window of opportunity to build in dependability to the emerging new information infrastructure. In doing so, Europe can and should take a lead in ensuring that the Knowledge Society is built on firm foundations.

Based on the schema of desirable actions outlined above, DDSI recommends that industry, Member States and the Commission consider adopting the following actions to ensure the emergence of a dependable information infrastructure in Europe within eEurope 2005 and beyond.

Industry

Most investments made in creating the infrastructure and applications for the Information Society come from the private sector. Although industry has a direct business interest in promoting confidence by consumers and business partners, it also has responsibilities as a “corporate citizen” to design out opportunities for misuse and crime.

Therefore contribution by industry should be expected in the following areas:

- Software and hardware vendors adopting secure product development practices as a minimum standard. Exploring greater use of open source solutions, standards such as Common Criteria (ISO 15408) and warrantable software.
- Network providers adopting operational best practices including using existing security features, employing security teams, collaborating with other providers and providing managed security features for users.
- Users of information systems adopting minimum standards for information security management such as ISO 17799. Larger organisations taking the lead in imposing minimum security standards across interconnected networks.
- Developing and deploying new security technologies. In particular, developing identity management solutions that are scalable and compliant with privacy concerns.
- “Infomediary” services to aggregate risk data to stimulate the insurance and investment markets.
- Development of industry standard practices upon which to base legally binding standards of “due care” in the production, use and management of ICT.

Individual Member States

On the principle of subsidiarity and multi-level governance, EU Member States and Newly Associated States could be encouraged to take the following steps:

- Benchmark national policies against global minimum standards in dependability policy. Policies should include establishing a firm policy lead, pan-government action and use of the partnership approach.
- Update criminal law on cyber-crime to ensure harmonisation with European standards.

- Effectively resource policing and investigative bodies to deter, trace and prosecute cyber-criminals.
- Develop and deploy educational initiatives targeted at citizens, consumers and students to prevent cyber-abuse in context of the OECD Guidelines for a “culture of security”.
- Promote good information governance, security management and business continuity in the private and voluntary sectors through the mechanisms of corporate governance, company law, audit guidelines and the development of automated risk management tools for large and small enterprises.
- Disseminate and encourage take-up of standards such as Common Criteria (ISO 15408) and (ISO 17799)
- Use public procurement and e-government interfaces to impose minimum security standards across interconnected networks.
- Promote warning and information sharing initiatives covering all sectors of society; ensure standardised approaches to reporting and incident response in conformance with emerging international standards.

Role of the European Commission

The European Commission has an important role to play in promoting trust and confidence in Europe’s Information Society. The Commission can play a vital role in stimulating the market, raising awareness, orchestrating knowledge and reducing unevenness between jurisdictions.

The first step should be for the Commission to adopt good international practice by acknowledging the need for coherent policy-making mechanisms, including:

- *A central policy lead*
- *A strategic, cross-pillar approach*
- *Mechanisms for partnerships among all stakeholders*

Therefore, for instance, the Cyber-Security Task Force could be given a clear, cross-pillar mandate under eEurope 2005 and could institutionalise a partnership with the private sector and civil society. If the Task Force can set the strategic agenda for European wide activities to promote dependability, it will also be able to contribute effectively to action with Europe’s international partners.

The Commission can add value to national efforts in the following areas:

Legal & Law Enforcement

- Harmonisation of EU Member States and Newly Associated criminal codes on cyber-crime
- Harmonisation of procedural criminal law and facilitation of police cooperation on incident investigation
- Investigation of legal mechanisms to encourage adoption of minimum standards (company law, product liability) and good practices (corporate governance)

Awareness & Market Stimulation

- Development of educational programmes to raise awareness of cyber-security and encourage ethical behaviour online
- Raise awareness amongst stakeholders, especially large businesses, of their dependencies upon information infrastructures

Operational Support

- Development of European-wide warning and information sharing networks building on existing CSIRT communities to provide services to European citizens and SMEs
- Support for emergency and consequence management capabilities able to deal with systemic risks on a European-wide basis
- Stimulate the market for more secure products and services by collecting, sharing and publishing data on cyber-risks

R&D

- R&D should be used to shape the long-term future of the European information infrastructure. Activities should include:
 - Using FP6 to meet the short and medium term needs of government, business and citizen users
 - Promotion of dependable software & system design and implementation
 - Promotion of approaches to manage risks to Large, Complex, Critical and interdependent Infrastructures
 - Tools for holistic risk management
 - Identity management & authentication

Europe's Contribution to International Governance

Coordinated international action is important to ensure there are no “weakest links” and that there are no “cyber-sanctuaries” for criminals. EU action at the global level could add significant value in the following respects:

- Contribution to the development and dissemination of standards and guidelines (esp. ISO and OECD)
- Contribution to good governance of the Internet, e.g. via ICANN or alternative bodies to protect the rights of the global community of users in a balanced and fair manner
- Contribution to education of public authorities and other stakeholders (e.g. within ITU, UN)
- Integration of EU-wide warning and alerting infrastructure with emerging global information sharing infrastructure including both governments and business
- Coordination of R&D with key external partners, especially USA, to ensure maximum added value. In particular, joint research into information infrastructure interdependencies and risk management would ensure rapid international progress.

ANNEX 1: Findings from Dependability Policy Overviews

The DDSI consortium undertook a systematic review of existing and emerging policy approaches to dependability and information security in 28 EU and non-EU countries.³ A similar overview of dependability-related activities amongst selected international government and non-government organisations was also completed.⁴ The primary objectives of this survey were to:

- a) provide policy makers with extensive background information
- b) assist in policy development at European and international levels
- c) pace the way towards benchmarking activities

Summary of Findings of National Dependability Policy Overviews

- All the surveyed countries have shown a widespread appreciation of the social and economic benefits of information society technologies. This is confirmed by rising Internet and mobile penetration, although broadband take-up is still limited.
- Electronic commerce is still in its infancy with most progress being made by established companies or technologically advanced countries such as the United States, Canada, the United Kingdom, Germany and several Scandinavian states.
- All surveyed countries have indicated a commitment to devise overarching regulatory frameworks and strategies for the promotion of the Internet and other information communication technologies.
- Insofar as governments have considered using legislation or regulation to promote dependability and security, their preferred approach has been to take a light regulatory touch, the main exceptions being privacy/data collection and electronic signature regimes.
- In all the surveyed countries it appears that computer-related malicious activities are on the rise. However, a detailed quantification of security incidents and crimes is difficult to compile due to a lack of incident reporting and the lack of commonly agreed definitions to guide data collection and analysis.
- The extent of government reactions to these cyber-risks and vulnerabilities has varied. There has been a proliferation of cyber-crime and high-tech crime policing initiatives and a growing interest in early warning and information sharing mechanisms. However, only certain states, including the United States, Canada, Australia, Japan, Sweden, Norway, Netherlands, France, Switzerland and the United Kingdom have adopted a more or less comprehensive approach to dependability. A common feature has been the general failure to build upon the experience acquired in dealing with the Y2K computer problem.

³ Australia, Austria, Belgium, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Liechtenstein, Luxembourg, Netherlands, Japan, Norway, People's Republic of China, Portugal, Russia, Slovenia, Spain, Sweden, Switzerland, United Kingdom, United States.

⁴ APEC, International Chamber of Commerce, Internet Alliance, Alliance for Global Business, Business and Industry Advisory Committee to the OECD, Global Information Infrastructure Commission, Council of Europe, Group of Eight, Interpol, Internal Telecommunication Union, North Atlantic Treaty Organisation, Organisation for Economic Cooperation and Development, United Nations

- There are substantial differences in industry's attempts to address dependability. In several countries, industry and trade bodies have been actively addressing these topics, although often in an uncoordinated fashion. The United States is the most active arena in which industry is closely engaged with government in dependability policy related discussions, for instance with the draft national plan for cyber-security.
- Notwithstanding generally limited industry involvement, all surveyed countries recognise the importance of joint government-private sector approaches to dependability and information security. Useful initiatives have been launched in the United States, Australia, United Kingdom, Switzerland, Netherlands and Germany.
- Applied and fundamental R&D has been recognised as a vital tool to improve the dependability of globally interconnected information infrastructures. At present, most countries lack integrated, strategic and multidisciplinary R&D programmes, with fragmented research focusing often upon narrow technical aspects.

Summary of Findings of International Dependability-relative activities

- All surveyed international organisations have recognised the urgent need to address the global legal, commercial and economic intricacies of electronic commerce; dependability-related issues have been addressed mainly by specific working groups specifically devoted to areas such as information security, cyber-crime, illegal digital content and electronic signatures.
- The remit of these working groups, as well as their composition, nevertheless, is usually defined by the covenant and mandate of each the international organisation; nevertheless, there seems to be a trend of increased involvement of industry and civil society in the activities of these bodies.
- There are several organisations that have been involved in dependability-related areas such as privacy, information security, cyber-crime and cryptography for a long time. Primary examples are the Council of Europe, the OECD, International Telecommunication Union and the United Nations as a whole; although their international legal remit varies, these organisations have established processes to engage all the stakeholders ranging from industry, research community and civil society such as consumer associations. In some cases, stakeholders have created "permanent" representation to ensure participation during the deliberations of specific international organisations, such as in the case of the Business-Industry Advisory Committee to the OECD.
- The activities of all surveyed international organisations seem to lead to similar conclusions:
 - a) Mandatory solutions are not viewed as appropriate for fostering the dependability of information infrastructures; voluntary solutions, based on a consensual process, are more suitable to govern the highly complex technical and commercial environment created by the Internet and other information networks.
 - b) There is a strong need for reliable and comparable international statistics to both measure malicious and accidental on-line activities and assess dependability-related national and international policies; particular attention should also be given to issues such as "economics of security" and "economics of privacy" with the overarching objective of devising appropriate "technologically neutral" methodologies in the areas of risk assessment and risk management.

- c) The dependability of global information infrastructures requires public-private partnerships, which should not be restricted to government institutions and industry, but should involve all sections of civil society; this multi-stakeholders' dialogue should be structured around an open dialogue and interaction in order to devise common approaches and solutions to the many policy and management facets of dependability.
- d) The need to establish common international civil and legal norms is emphasised; particular attention is directed to issues such as mutual recognition of standards and practices. "Consensus-based" international technical and managerial standards are viewed as essential for fostering dependability.
- e) All surveyed international organisations have called for increased and better co-ordinated R&D activities; since most of the surveyed organisations do not have internal budget for this kind of activities, this request has been aimed at national governments and industry; they have been invited to share the efforts for both pure and applied dependability-related R&D.
- f) With the exception of those with a military focus such as NATO, all international organisations agree on the need to improve general public awareness on dependability related issues; in particular, this involves educational activities to prepare the most vulnerable users of information and network technologies to handle online risks and threats and, at the same time, appreciate their overall responsibilities and duties to create a safer Information Society.

ANNEX 2: Findings of DDSI Policy Roadmap Exercises

DDSI was tasked to prepare three policy roadmaps⁵ to assist the European Commission and other institutions in addressing three priority dependability-related areas. These roadmaps are based upon thorough research of global state of the art; detailed, primary source analysis of the requirements and capabilities in Europe; and consultations with all stakeholders including users and suppliers from public and private sectors.

Warning and Information Sharing: Main Findings

The warning and information sharing Roadmap provides a rationale and plan for 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.

An important step towards addressing cyber-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 Member States are taking some steps to provide this information but 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 deeper 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 such an 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.

The Roadmap recommends that there is a need for strong leadership from EU institutions to stimulate and provide seed funding for an European-wide initiative. Nonetheless, 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. These are outlined in the table below.

⁵ These documents are available at <http://www.ddsi.org>

<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

Research and Development: Main Findings

Vision

A unique opportunity exists for Europe to assure the emerging infrastructures that will support the Information Society, whilst at the same time benefiting European industry. This opportunity can be realised if Europe develops a strategic approach to dependability R&D.

Today, there is a “dependability gap” between the expectations being placed by society upon contemporary information infrastructures and the robustness of these infrastructures. European society is become more dependent upon the large, unbounded, multi-jurisdictional socio-technical systems that constitute the information infrastructure but infrastructure vulnerabilities are legion, ranging from the component level (e.g. “buggy” software) to the societal level (e.g. inadequate legal regimes).

Meanwhile, Europe is moving towards a new infrastructure paradigm, that of an Ambient Intelligent Space. In this environment, intelligence is distributed, pervasive and unobtrusive. New applications such as telemedicine, intelligent roads and personalised e-government will ride upon this infrastructure. Dependable infrastructures are central to this new paradigm.

A strategic European approach to R&D must meet the unresolved dependability needs of users operating in the existing infrastructure paradigm *and* “engineer in” dependability to the emerging infrastructures.

A strategic European dependability R&D programme could have the following societal impacts:

- Ensure the achievability of the business, political and social aims of the Information Society vision. The R&D programme must fill the “Dependability Gap”.
- Enable the development of Information Society services by building dependable components and systems of systems.
- Enhance the competitiveness of European industry, notably the software and IT sectors, by enabling them to take the lead in building components for the Ambient Intelligent Space infrastructure, perhaps exploring concepts such as warrantable software.

Dependability as an Approach

Dependability, as a concept that integrates elements such as reliability, safety and security, provides a proven conceptual framework for developing intellectually robust solutions to these challenges. However, attempts to improve dependability are hampered by the fact that information infrastructures have undergone a radical change from the paradigm of centralised control to the *economics of functionality*. Whether one considers the demand for functionality by individual PC users or the reliance by power companies upon the public telecommunications system, it is evident that the traditional approach that pits functionality against dependability is failing to deliver adequately dependable infrastructures to all users.

Therefore, the philosophy of the R&D programme should be to make dependability an integral property of all aspects of the Knowledge Society and to treat it as an enabler rather than an add on. The functionality-dependability dilemma needs to be replaced by an approach in which dependability is a prerequisite for functionality.

A paradigm shift in dependability is required to address this new environment. A wider range of communities should be embraced so as to develop a truly multi-disciplinary approach to

dependability. These communities should be invited to apply their methods to the dependability challenges posed by the system of systems and societal levels. Disciplines and approaches that may be able to contribute include complex systems theory, bio-mimetics (e.g. computational immunology), complex physical systems (e.g. meteorology and oceanography), complex virtual systems (e.g. agent-based systems) and economics.

Research and Policy

In order to fulfil the potential of an enhanced dependability initiative, appropriate research policies need to be developed to derive systematic roadmaps, to optimise research management and to develop effective funding structures as well as to evaluate R&D impacts. R&D policy should embed a continuous process of “envisioning the future,” including drivers, challenges and needs. This will help to systematically categorise and prioritise research requirements.

An important additional function of the European research programme should be to provide analytical support for public policy-making. Currently, the scientific knowledge base upon which policy-makers can base their decisions in the area of dependability is inadequate. A transnational network of experts should be established to develop this knowledge base and to ensure a two-way communication channel with policy makers.

It is increasingly evident that today’s large-scale socio-technical systems can only be assured if the political, social and economic contexts and drivers are understood. The research programme should encompass these environmental factors, for instance on the economics of information security.

The Research Agenda

The European dependability research agenda needs to build on existing strengths (e.g. at the component level) but to devote more effort to the system of systems and societal levels. The research programme must address the short-term needs of users of existing systems (“fixing today’s problems”) and lay the foundations for the future infrastructure (“engineering in dependability”).

There are numerous “shopping lists” of possible dependability research topics; the next phase of roadmap activities should systematically categorise and prioritise topics. An initial categorisation could include the following:

- Policy Issues
- Basic Research
 - e.g. Interdependencies; Threats & Risks; Implications of new technologies
- Human Factors
 - e.g. User/Customers; Service Providers & Vendors
- Economic Aspects
- Technical Measures & Capabilities
 - e.g. Protection; Detection; Reaction
- Organisational Measures
- Measurement, Simulation & Testing

Technology Take-up

R&D will only benefit European stakeholders if its results are taken up. At the same time, many user requirements can be met not by long-term research programmes but by exploitation of existing or near to market technologies.

The overarching aim of a dependability initiative in the ERA and FP6 should be to inculcate a *culture of dependability*. To achieve this aim, it will be important to widen the involvement of stakeholders outside existing dependability projects, i.e. the wider research community, national governments, industry, consumers, privacy groups and research policy makers. The research programme therefore needs to include:

- Embedded dialogue between researchers, implementers and users
- Mechanisms for “tactical” research, for instance assisting users with adaptation of existing solutions
- Links between the R&D programme with standardisation bodies
- Support for market mechanisms and awareness activities to stimulate demand for more dependable systems from private and corporate users (e.g. via corporate governance, liability, insurance, legal)
- Education & skills at all levels from young researchers to practitioners, policy-makers and individual users.

Public/Private Partnership: Main Findings

“Each participant in information systems and networks is an important actor for ensuring security. Participants should be aware of the relevant security risks and preventive measures, assume responsibility and take steps appropriate to their roles and positions to enhance the security of information systems and networks.”⁶

The principle of distributed and universal responsibility outlined in the OECD Guidelines cited above is an invaluable reminder that the global information infrastructure is a “joint product”; jurisdiction over its various elements is shared between private and public sector actors as well as all users across the globe. It is no longer possible for governments alone to assure the infrastructure. It is vital for states and multilateral institutions to take what steps they can to secure infrastructures. Market actors will also take precautions that make business sense. But risks to global information infrastructures can only be managed by coalitions involving public-private & national-supranational cooperation.

There will naturally be a range of such partnerships. In countries that have gone a long way towards liberalising their economies and infrastructures, a great deal more work will be required than in countries that retain intimate relationships between government and industry. Likewise, where incumbent companies, such as in the telecommunications sector, retain a dominant market share, it will be easier to impose security standards than in a more liberalised environment.

Given this variety of environments, public and private sectors are finding a range of innovative ways of partnering to share the risks. Examples include the Partnership for Critical Infrastructure Security and (some) Information Sharing and Analysis Centers (USA), Infosurance (Switzerland), Information Assurance Advisory Council (UK), AKSIS (Germany), SIS (Norway), ECP-NL (Netherlands) and the Business Government Task Force (Australia). Tasks for these partnerships include:

- Information Sharing/exchange
- Awareness, Education
- Best Practice Exchange
- Policy co-development

Although all stakeholders should have a common interest in cooperating to manage risks to information infrastructures, in practice it has proven hard to establish partnership mechanisms that really make a difference. To support the development of successful partnerships, the DDSI Roadmap analysed and consulted with leading examples of partnerships.

Lessons learned include the following:

- Although market forces can drive the establishment of these partnerships, private sector funding is very vulnerable to cyclical economic fluctuations. Therefore, public sector funding from either national or international bodies is invaluable to support basic infrastructure and set-up costs. Partnerships however need also to conduct realistic and detailed assessments of the products and services they can deliver to private sector end-users, so as to ensure they are meeting clear business needs.

⁶ OECD, *Information Security Guidelines*, 2002

- Where possible, partnerships should build on existing trusted relationships and representative bodies rather than creating elaborate new structures.
- A central function of public/private partnerships should be public awareness and education. Partnerships can harness complementary expertise and exploit multiple dissemination channels to take the lead in well-crafted information campaigns.
- One of the useful functions of such partnerships is to provide a two-way exchange of information about risks and solutions between government and industry. Such exchanges will however be limited by concerns about the commercial sensitivity or official classification of information. Partnerships should draw on good practice in other fields to identify mechanisms for overcoming such sensitivity (e.g. accident reporting, counter-terrorism and disease control).
- Fostering mutually beneficial dependability-related R&D is another key function of these partnerships.
- International networking of existing partnerships is important to:
 - Ensure mutual support & advice
 - Exchange lessons learned
 - Undertake joint activities
 - Stimulate new partnerships

To date, most partnership activities are in an embryonic form. Without the enthusiasm of a small number of key individuals, companies and government departments, they would be ineffective. The goal for all stakeholders should be to move from ***enthusiasts*** to ***institutions***.

Annex 3: DDSI Project Final Report

DDSI was a Framework 5 Information Society Technology research programme Accompanying Measure supported by the European Commission's Directorate General Information Society from June 2001 to November 2002.

The goal of DDSI was to support the development of dependability policies across Europe. The overall aim was to establish networks of interest, and to provide baseline data upon which a wide spectrum of policy-supporting activities can be undertaken both by European institutions and by public and private sector stakeholders across the EU and in partner nations.

In addition to addressing conceptual and comparative issues and surveying European dependability policy environments, the project identified three priority thematic areas in which policy roadmaps were to be produced:

- Early Warning
- Public-private cooperative models
- Research & Development

DDSI had the following features:

- It focused upon the dependability of *information infrastructures*
- It marked the transition of information infrastructure dependability from a bottom up, technical concern to a public policy & strategic business concern
- It viewed dependability as a business enabler
- It took a view across national and sectoral boundaries
- It had a European focus but in a global context
- It was designed to inform the policy debate

Who was DDSI?

DDSI involved a consortium of research organisations from nine European countries. The organisations combined policy and technical expertise as well as cultural and political understanding of their environments. DDSI was coordinated by the lead partner (RAND Europe); King's College London, IABG and Cell Network led work packages. The partners were:

- RAND Europe (NL)
- King's College London (UK)
- Cell Network (S)
- IABG (D)
- Almaweb (I)
- Link (P)

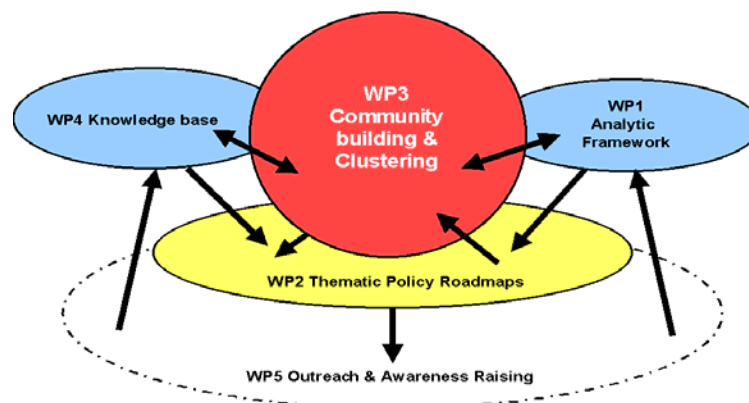
- ELIAMEP (G)
- Ernst Basler + Partner (CH)
- Isdefe (E)

In addition to the project team, DDSI benefited from a Reference Group composed of senior representatives from the academic and industrial sectors. Both European and US institutions were represented. The Reference Group met three times in the course of the project and provided invaluable guidance to ensure that DDSI's findings addressed high-level business, political and academic needs. The Reference Group was coordinated by Derek Long. Its members were:

- Yves Deswarte (LAAS-CNRS, France)
- Pieter van Dijken (consultant, Netherlands)
- Brendan Murphy (Microsoft, UK)
- Lars Nicander (Swedish National Defence College, Sweden)
- Brian Randell (Newcastle University, UK)
- Eugene Spafford (Purdue University, USA)
- Giuliano Tavaroli/Luca Tenzi (Pirelli, Italy)
- Ken Watson (Cisco/PCIS, USA)

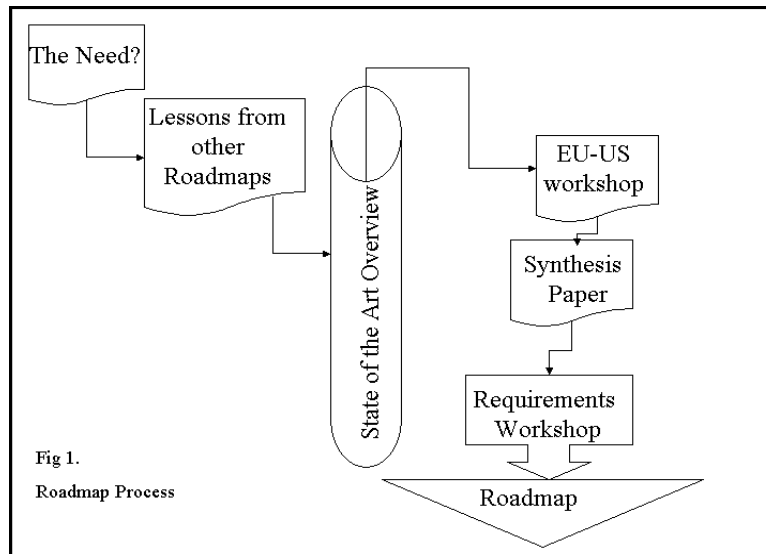
Project Structure

The project structure is outlined below. The significance given to work-package 3 (Community Building and Clustering) is a reminder that, whilst DDSI's findings were underpinned by thorough research, it was vital to consult widely as the findings were being developed. By building communities amongst disparate stakeholders, DDSI made sure that its findings were more likely to be implemented and acted upon.



For each roadmap, an analytical process similar to that outlined below for the R&D roadmap was undertaken. This involved identifying the need and analysing lessons from any similar roadmaps, and undertaking a global state of the art overview. One or more workshops were then held to

elicit further input. Findings were then developed into draft roadmaps that were circulated widely before being finalised.



Project Deliverables

DDSI's written outputs are collated on the project CD-Rom and website (www.ddsi.org). They can be grouped into the following categories.

- Synthesis Paper: Securing the Information Society (D1)
- Summary Presentation (D1)
- Concepts
 - Conceptual Framework (D1)
- Dependability Overviews
 - National Dependability Overview (D2)
 - International Organisation Dependability Overview (D2)
- Public Policy
 - Public Policy Workshop (D6A)
 - Final Public Conference (D12)
- Public Private Partnerships
 - Public Private Roadmap (D3)
 - Public Private Workshop (D9A)
- Early Warning
 - Warning & Information Sharing Roadmap (D4)
 - Warning & Information Sharing Workshops (D8A)
- Research & Development
 - R&D Roadmap (D5)
 - R&D Workshops (D7A)

- Knowledge Base
 - Website & online archive (D10)
- Exploitation
 - Outreach & Awareness-Raising Plan (D11A)

For the workshops, DDSI produced terms of reference and a background paper as input, and a workshop report as output. The available presentations by participants have been included on the CD Rom. The written deliverables above were input to and/or reflected the outcome of the following events:

- European Warning & Information System Workshop, in collaboration with JRC, Brussels, 25-26 October 2001
- EU-US Workshop on R&D Strategy, in the context of the IST Conference 2001, Düsseldorf, 1-2 December 2001
- Warning & Information Sharing Workshop, Brussels, 17-18 January 2002
- Public Policy Workshop, Brussels, 28 February-1 March 2002
- Public-Private Partnership Workshop, Stockholm, 6-7 June 2002
- R&D Strategy Workshop, Brussels, 19-20 September 2002
- Final Conference, Brussels, 10 October 2002

Lessons Learned

The DDSI project team faced a number of challenges in completing its tasks. Challenges included:

- i) Building a cohesive project team with a clear analytical focus from nine different organisations, with different specialisms, languages and cultures. Few of the organisations involved had extensive experience of working together. Whilst this demonstrated the project team's desire to bring fresh perspectives to bear, it was a management challenge.
- ii) Engaging with industry, member states and building trust amongst often "stovepiped" research, operational and policy communities. Over time, DDSI's consultative approach gained support from many of the key communities. Nonetheless, and with notable exceptions from key players in the ICT sector, ensuring deep industry buy-in to the work remained a challenge. In general, industry is content to react to European policy initiatives rather than taking the time to engage in shaping that policy in its very early stages.
- iii) Working in a fast-moving policy environment. During the course of DDSI, information infrastructure dependability rose up the agenda with events such as the new eEurope 2005 Action Plan, the September 11 attacks on the US and the completion of the OECD Guidelines. DDSI therefore had its work cut out to remain abreast of these developments and to contribute rapidly and meaningfully to policy discussions in Europe.
- iv) In part as a result of the growing prominence of the issues, and other drivers such as the development of the FP6 research programme, DDSI faced an escalating number of requirements. These included additional workshops, additional written deliverables and additional dissemination activities. Whilst welcome in making the project relevant, these demands posed a strain on project resources.

These challenges notwithstanding, DDSI achieved the following:

- ✓ It embedded the technological debate into the socio-economic & policy debate
- ✓ It brought together technical, government, operational security and large corporate communities
- ✓ It facilitated understanding of Large, Complex Critical Infrastructures as (global) socio-technical systems
- ✓ It identified national policy benchmarks & policy options

What Next?

DDSI has provided a model for how Europe can systematically approach the challenge of information infrastructure dependability. It is important to leverage the investment to date to ensure that European policy continues to be informed by comprehensive data, expert analysis and extensive consultation with stakeholders. This can be done by consolidating a sustainable multi-disciplinary platform for analysis of the policy aspects of information infrastructure dependability. Building on the lessons of DDSI, this would involve three elements:

- Knowledge Platform This would entail developing a knowledge infrastructure for policy analysis, including human capital, baseline data, intellectual tools, physical & virtual community building. An important element of the knowledge platform will be the DDSI website which needs to be regularly updated.
- Research
 - Featuring both prospective & reactive elements
 - Multi-disciplinary
 - Involving community building to common ownership of knowledge
- Outreach
 - To systematically gather policy/societal/business user needs & requirements
 - To communicate research results & raise awareness
 - To liaise with European partners (e.g. USA)

Based on the lessons of DDSI, it is recommended that this activity involve the following elements:

- A European-wide consortium of research bodies already active in dependability/ICT policy-analysis. The entities must have complementary expertise (policy, legal, technical, business, etc) and must be drawn from across Europe, with strong international links.
- The consortium should be supported by a high-level international advisory body. This would combine senior representatives from EU institutions, national governments, industry, the R&D community and European partners in other countries and international organisations.
- The follow on activity must emphasise strong links with industry, the research community and have strong international links.

Dependability Development

DDSI

Support Initiative

www.ddsi.org

RAND Europe (NL)
(Project Coordinator)

www.randeurope.org

RAND *Europe*

KING'S
College
LONDON

University of London

King's College London (UK)

www.kcl.ac.uk

Cell Network (S)

www.cellnetwork.com

CELL
NETWORK

IABG (D)

www.iabg.de

IABG

ALMAWEB (I)

www.almaweb.unibo.it

ALMAWEB

LINK (P)

www.link.pt

CONSULTING
link

We Manage Knowledge. With you

ELIAMEP (GR)

www.eliamep.gr

ELIAMEP

Ernst Basler + Partner (CH)

www.ebp.ch

Ernst **Basler + Partner**

Isdefe (E)

www.isdefe.es

Isdefe

DDSI

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

