

Dependability Development

DDSI

Support Initiative

**DDSI
IST-2000-29202**

Conceptual Framework

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 2002

Classification: Public

Preparation led by: RAND Europe (NL), 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

As Europe's economy and society become more dependent upon electronic communications and upon the Internet, so critical business and social processes are becoming more vulnerable to accidental or malicious failures in information systems. The emergence of an Information Society in Europe has therefore led to a growing recognition of the need to ensure an environment in which dependable and trustworthy information infrastructures can be developed.

The objective of the Dependability Development Support Initiative (DDSI) is to support the European Commission in the development of dependability policies across Europe and across sectoral boundaries. It aims to establish networks of interest, to provide baseline data and to develop policy roadmaps. These products will support policy activities by European institutions and by public and private sector stakeholders across the EU, in Accession States and in partner nations.

DDSI contributes to the European Community policy initiative eEurope2002¹, and in particular its Action Line "Stimulating public/private co-operation on dependability of information infrastructures (including the development of early warning systems)". It also supports the European IST Research Programme's² aim "to realise the benefits of the Information Society for Europe".

Although several European institutions and Member States have been examining certain aspects of dependability, the rationale for DDSI is that developing policy to assure the dependability of Europe's information infrastructures necessitates a multidisciplinary and transnational approach. Europe's Member States, businesses and citizens are part of the global electronic village; they are increasingly dependent on globalised and interdependent information infrastructures. These dependencies need to be matched by transnational and cross-sectoral governance mechanisms; policy and technical solutions can no longer be developed in isolation.

Scope and Focus of DDSI

It is important to be clear at the outset about the scope and focus of DDSI. DDSI is not concerned with dependability in all systems in relation to all potential faults. The primary focus is on the dependability of the information infrastructures and services that underpin the Information Society in Europe (i.e. the telecommunications and Internet infrastructures and networks). This primary focus meets the requirements of the Commission and Member States who have requested the Commission to consider the dependability aspects of emerging information infrastructures as the first step towards a wider understanding of Community-wide dependencies.

DDSI however emphasises that the dependability of information networks cannot be considered in isolation since a wider set of infrastructures that support post-industrial societies are becoming increasingly dependent on networked information systems. These include energy generation & distribution, transport, water and sewage, healthcare, food production and distribution, finance and government services. By focusing upon measures to improve the dependability of the information infrastructures, DDSI complements work being undertaken to promote the dependability of these infrastructures.

¹ See http://www.europa.eu.int/comm/information_society/eeurope/

² See <http://www.cordis.lu/ist>

DDSI has a primary and a secondary focus in relation to the faults, vulnerabilities and threats of concern. The primary objective is to assist in the development of policies that address threats and vulnerabilities susceptible to short and medium term solutions. These include, for instance, detection and prevention of malicious attacks in the form of Denial of Service or virus attacks over the Internet.³ Wider issues that will be addressed in less detail include the problems associated with increasing reliance on Commercial Off The Shelf (COTS) technologies⁴ and the vulnerabilities of global supply and value chains on which European infrastructures are increasingly reliant.⁵

Aim & Content of this Document

This document is the first component of Work Package 1, the Conceptual Framework for DDSI. Together with the international comparative overview (WP1.2), it constitutes Deliverable 1 of DDSI.

The aim of this document is to provide a conceptual basis for understanding and identifying the public policy challenges posed by dependability. It provides a baseline of conceptual knowledge on information infrastructure dependability that will be used to inform policy-makers as to the key issues that need to be addressed.

This framing study outlines the concept of dependability; describes the societal and technological environment within which dependability has become a policy issue and clarifies the public policy challenges posed by dependability.

The paper is structured as follows: Section one provides a review of the concepts involved in dependability and information security; as well as related concepts in the business and governmental communities. Section two provides an overview of what is meant by European information infrastructures. Section three discusses risks to information infrastructures. The fourth section discusses the broader societal implications of a lack of dependability and identifies a number of market failures. The fifth section introduces the global and European policy environment and situates dependability policy within the broader context of the development of the European Information Society. The sixth section discusses means for enhancing dependability and security. It provides an initial roadmap of policy options, some of which will be examined in more detail by other DDSI workpackages. The seventh section provides a selected glossary of terms. The eighth section provides a comprehensive bibliography.

³ See for an overview of potential threats and techniques RAND publication MR-993-OSD/NSA/DARPA by Robert H. Anderson e.a., 1999, which represents the outcomes of a study on minimal essential information infrastructure.

⁴ Including risks arising from software monocultures. See, *The implications of COTS vulnerabilities for the DOD and Critical U.S. Infrastructures*, Anderson and Hundley, RAND 1998, P-8031

⁵ For instance, dependence on single sources of supply for microchips.

Acknowledgements

This concept paper was completed with the assistance of all DDSI partners. Thanks are due to the DDSI team: Kevin O'Brien, Leon Cremonini, Andreas Ligtvoet, Ingrid Geesink, Carine Dartiguepeyrou (RAND Europe), Peter Wallström (Cell Networks), Susanne Jantsch (IABG), Alessandro Politi (Almaweb), George Gantzias (ELIAMEP), Luis Amorim (LINK), Daniel Bircher and Stefano Bruno (Ernst Basler & Partners), Luis Martinez Miguez (ISDEFE) and Derek Long (CISA Ltd).

The DDSI Reference Group also provided invaluable input. Thanks to Brian Randell (Newcastle University), Brendan Murphy (Microsoft Labs), Lars Nicander (Swedish National Defence Academy), Yves Deswarte (LAAS – CNRS), Pieter van Dijken (formerly Shell International), Luca Tenzi (Pirelli), Ken Watson (Cisco Systems) and Professor Eugene Spafford (Purdue University). Andrea Servida (DG Info, Marc Wilikens & Marcelo Masera (JRC) also provided valuable advice and guidance.

Any mistakes remain the responsibility of the authors alone.

Maarten Botterman
Lorenzo Valeri
Andrew Rathmell

Executive Summary

Public trust and confidence in Europe's information infrastructures are vital if the Information Society is to succeed. Dependability is a vital element in promoting this trust and confidence. This paper examines the requirements for European action to promote dependability through a range of policy instruments aimed at managing risks to Europe's information infrastructures. The intention of the paper is to provide concepts and options for policy discussion within the European Commission.

A logical outcome of the current process would be the development of a policy Roadmap that provides a strategic overview of EU objectives, lays out the structures by which policy should be made and implemented, identifies the steps that are required to enhance dependability and the policy levers that can be used to stimulate market, technical and governmental solutions to these challenges.

Concepts & Definitions

- Dependability must be seen as a business enabler. Rather than being viewed as a burden on the exploitation of new ICTs, dependability and security are a necessary prerequisite for the emergence of the Information Society in Europe.
- The concept of dependability, which includes the attributes of Availability, Reliability, Safety, Confidentiality, Integrity & Maintainability, is valuable when dealing with risks to large, complex and unbounded systems of systems like the information infrastructure. The concept of survivability has particular resonance when applied to open systems operating in a hostile environment,
- Information security is an important functionality of a dependable system.
- In order to promote an understanding of dependability at the right levels amongst suppliers, users, owners and operators of information systems, it may be advisable to adopt the concept of information assurance and to embed this in the broader concepts of business assurance, underpinned by the concept of information risk management.

European Information Infrastructures

- The information infrastructure has traditionally been defined as “that system of advanced computer systems, databases and telecommunications networks ... that make electronic information widely available and accessible. This includes the Internet, the public switched network and cable, wireless and satellite communications.”
- The shape of the emerging information infrastructure is captured in the concept of “ambient intelligence.” The future European information infrastructure will involve the convergence of networked embedded and hybrid systems that will immerse citizens in an information environment and in which physical control systems will increasingly migrate online.
- For policy-making purposes, it is important not to limit attention to information networks. For European citizens and users, the focus is upon Information Society service delivery; hence the policy focus should be upon business assurance as whole, rather than information systems security as a separate topic.

Risks to Information Infrastructures

- Threats to information systems arise from multiple sources, including design faults, human error, natural disaster and malicious acts.
- Malicious threats may arise from recreational hackers, criminals, terrorists and states.
- Assessing the extent of these malicious activities is difficult due to a lack of reliable and consistent data.

Dependability Requirements for Trust and Confidence

- Dependable information infrastructures are vital elements for enhancing trust and confidence. That the current information infrastructures fail to sufficiently promote trust and confidence is evident from numerous surveys in Europe and the USA.
- Dependability is even more crucial to support critical infrastructure activities and safety-critical activities such as telemedicine.
- There are a number of evident market failures, on both the supply and demand sides, which have meant that the market has not yet solved the problems of dependability and information security.
- Given these failures, there is a need to approach dependability-related issues from a public policy perspective. Public policy has a role in addressing the economic and commercial factors that lead to the development of faults and vulnerabilities and those situations where these faults lead to failures.

Towards European Dependability Policy

- The need to ensure “trust in cyberspace” has been rising up the global public policy agenda since the 1990s. In Europe, policy-makers became aware in the late 1990s that the development of an Information Society required dependable information infrastructures.
- The transformation of this topic into a broad public policy issue was the result of two trends. First, the increased reliance by governments, businesses and citizens on networked ICT. Second, the parallel growth in “cyber-abuse.”
- The European Union has initiated efforts to address information security and dependability through integrated policy initiatives. EU policy has included: dependability & trust R&D; cyber-crime initiatives; eEurope implementation.
- Critical Infrastructure Protection has remained a Member State responsibility. Nonetheless, a combination of the growing competencies of European institutions in relation to the nascent European foreign and security policy arena and the increased European policy focus on large scale terrorist attacks are leading to a recognition that enhanced European-wide cooperation is required if risks to interdependent infrastructure are to be managed.

Policy Options

- The risks that face Europe are increasingly transnational. Indeed, the emerging information infrastructure is a global socio-technological system. Policy responses and governance mechanisms therefore need to be as multi-disciplinary and as transnational and global as the challenges.
- Public policy should be designed to “engineer in” dependability to Europe’s information infrastructures. Public policy needs to deploy a range of instruments ranging from legislation and

regulation, through direct intervention to stimulating further R&D and technology take-up as well as good practice.

- Possible EU policy areas and instruments can be categorised as follows:

Policy Making Mechanisms

- The need for a central policy lead
- The need for a strategic 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
- Understanding of the motives, intentions and value systems of threat actors

Protection

- Promotion of more dependable software & system design and implementation
- Promotion of information governance & security management good practice
- Updating and revision of standards
- Promotion of dependability aware cultures & education encouraging ethical and responsible user behaviour
- Promotion and exploration of technical and organisational solutions to priority issues, such as authentication and access control

Detection

- Warning and information sharing
- Development of reliable statistical indicators for trend analysis

Risk Management

- 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

Research & Development

- *Underpinning all of the above areas will be research and development that is multi-disciplinary and combines “blue-skies” research with technology take-up activities.*

Contents

Preface 3

Executive Summary 6

1 Definitions & Concepts 11

 1.1 Dependability 11

 1.2 Trustworthiness 13

 1.3 Survivability 13

 1.4 (Network and) Information Security 14

 1.5 Information Assurance 15

 1.6 Critical Infrastructure Protection/Assurance 16

 1.7 Business Assurance & Corporate Governance 16

 1.8 Conclusion 17

2 European Information Infrastructures 18

 2.1 Defining the Information Infrastructure 18

 2.2 European Information Infrastructures: Regulatory, Technological & Commercial
 Developments 19

 2.2.1 Convergence 21

 2.2.2 The Wireless Era 21

 2.3 Global Information Infrastructure Dependencies 22

 2.4 Wider Societal Dependencies 22

3 Risks to Information Infrastructures 24

 3.1 Faults & Vulnerabilities 24

 3.1.1 Physical Faults 24

 3.1.2 Design and implementation faults 25

 3.1.3 Malicious Logic 26

 3.1.4 Intrusions and Attacks 26

 3.2 Errors and Failures 27

 3.3 Threats 28

 3.4 Conclusion 29

4 Dependability Requirements for Trust and Confidence 30

 4.1 The Lack of Trust in Online Activities: A Perspective from the United States 30

 4.2 European Perceptions of Trust 31

 4.3 Critical Infrastructures 32

 4.4 The Need for Public Policy 33

 4.5 Conclusion 34

5 Towards European Dependability Policy 36

- 5.1 The European Policy Context36**
- 5.2 The Future Technology and Policy Environment39**
 - 5.2.1 Technology & Market Trends 39
 - 5.2.2 European Policy Developments..... 41
- 5.3 The Global Context 41**
- 6 Policy Options42**
 - 6.1 Approaches to Enhancing Dependability42**
 - 6.2 Dependability Policy Development.....43**
 - 6.3 The Content of Public Policy43**
 - 6.3.1 Policy Making Mechanisms..... 44
 - 6.3.2 Deterrence..... 44
 - 6.3.3 Protection..... 45
 - 6.3.4 Detection..... 46
 - 6.3.5 Risk Management 46
 - 6.4 Cross-Sectoral Partnerships.....47**
 - 6.5 Warning and Information Sharing48**
 - 6.6 Research & Development.....48**
 - 6.7 Conclusion.....49**
- 7 Selected Glossary50**
- 8 Bibliography 51**
 - Official Documents, Final Project Reports and Speeches 51**
 - Books52**
 - Articles, Book Chapters, Papers and Conference Proceedings53**
 - Technical Reports and Surveys 54**
 - Newspapers/Weekly Reports..... 55**

1 Definitions & Concepts

This section discusses definitions of various terms that apply to DDSI's domain of interest. The aim of this section is to describe and bound the topic that DDSI addresses.

Dependability is a term that is well understood by the research community but is not widely used by other Information Society stakeholders such as policy-makers, businesses and citizens. Amongst these groups, terms such as information risk, information security, information assurance and infrastructure protection are more common. Since clarity in language must precede clarity in policy-making, this section examines the various terms in use. Fortunately, many of these concepts cover similar functionalities and behaviours. Whilst it is important to work towards glossaries and taxonomies that enable dialogue between communities, it may be unnecessary to engage in the lengthy process of definitional standardisation.

This section outlines five terms that are often used to characterise the subject matter of DDSI: dependability; trustworthiness; survivability; (network and) information security; and information assurance. Concepts that are also relevant to the subject include: critical infrastructure protection/assurance; business assurance; (information) risk management; and business continuity.

1.1 Dependability

Over the past two decades, considerable effort has gone into bringing together disparate research communities to arrive at commonly agreed definitions that allow dependability to be used as a “unifying concept.”⁶

Dependability can be defined as “that property of a computer system such that *reliance can justifiably be placed on the service it delivers.*”⁷ Dependability should be seen as: “the ability of a system to avoid failures that are more frequent or more severe, and outage durations that are longer, than is acceptable to the users.”⁸ In other words, the dependability of a system is defined by its users' expectations. The “**service** delivered by a system is its behaviour *as perceived* by its user(s); a **user** is another system (human or physical) interacting with the system.”⁹

The dependability of a system is expressed in terms of the following attributes:¹⁰

⁶ Brian Randell, "Dependability-A Unifying Concept", Paper presented at the workshop Computer Security, Fault Tolerance and Software Assurances: From Needs to Solutions, 1998, available at <http://www.ise.gmu.edu/~csis/conf/fns98/> (visited on 20 July 2001)

⁷ David Powell and Robert Stroud (Eds), MAFTIA Conceptual Model and Architecture (November 20 2001), MAFTIA deliverable D2, p.3. See also the International Federation for Information Processing (IFIP) definition: dependability is “the trustworthiness of a computing system that allows reliance to be justifiably placed on the service it delivers” in J. C. Laprie (ed.), Dependability: Basic Concepts and Terminology (New York: Springer-Verlag, 1992), p.4. See also J.C. Laprie, "Dependable Computing and Fault Tolerance: Concept and Terminology", in Proceedings of the 15 IEEE International Symposium on Fault Tolerant Computing, Ann Harbour, MI, USA, June 1985 (IEEE Press, 1986), pp.2-11

⁸ A. Avizienis, J.C. Laprie and Brian Randell, Fundamental Concepts of Dependability.

⁹ MAFTIA Conceptual Model and Architecture, p. 3.

¹⁰ MAFTIA Conceptual Model and Architecture, p. 3. See also: Neil Storey, Safety-Critical Computer Systems, (Harlow, UK: Addison-Wesley, 1996).

- **Availability**, involving *readiness for use*
- **Reliability**, involving *service continuity*
- **Safety**, involving *non-occurrence of catastrophic consequences* for the environment
- **Confidentiality**, involving non-occurrence of *unauthorised disclosure* of information
- **Integrity**, involving the prevention of *unauthorised modification* or deletion of data
- **Maintainability**, involving the *ability to conduct repairs* and introduce evolutions¹¹

Security is generally taken to encompass confidentiality, integrity and availability relative to authorised users. *Confidentiality* covers the restriction of access to data and systems to authorised users according to defined policies. The concept is often associated with the notions of privacy and secrecy. Privacy indicates the capacity of an individual to prevent un-authorised access to their personal data. Secrecy involves the implementation of controls over access to information and data.¹² *Integrity* “is the confirmation that data which has been sent, received and stored are complete and un-changed.”¹³ *Availability* refers to a system’s ability to perform as expected by its users.¹⁴

Security also encompasses the elements of authentication (& anonymity) and non-repudiation. *Authentication* refers to the ability of users to identify their transactional counterparts. Anonymity refers to the ability of a user (human or machine) to use a system without having to reveal a partial or full identity. *Non-repudiation* ensures that the actions of authenticated users cannot subsequently be refuted.¹⁵

Bringing Security and Dependability Together

It will be noticed from the discussion above that availability has a dual role – both as an attribute of a dependable system and as a sub-element of security. This dual role has led some researchers to devise a framework in which security and dependability can be viewed simultaneously. Championed by Erland Johnson, this approach focuses on the preservation of the overall integrity of system resources. Integrity controls do not only fulfil a specific security functionality. They also allow the system to withstand abuses of resources, which may affect its overall behaviour as expressed by the attributes of reliability, availability and safety. This same logic can be applied to confidentiality. Security functionality calls for the regulation of access to data and information. Consequently, argues Johnson, confidentiality should be:

“understood in a broader sense, i.e., the prevention of the delivery of the service to a non-user, even if this service delivery would not include harm to the user or disclosure of secret information.”¹⁶

¹¹ A. Avizienis, J.C. Laprie and Brian Randell, Fundamental Concepts of Dependability, LAAS Technical Report n. 01145, April 2001, p.6

¹² Ross Anderson, Security Engineering (Chichester, UK: Wiley Computing Publishing, 2001), p.10 and Network Security Communication p.5

¹³ Commission of the European Communities, "Network and Information Security", p.5

¹⁴ Charles Pfleger, Security in Computing (New Jersey: Addison and Wesley, 1996)

¹⁵ It is possible to conceive situations where a user will complete non-repudiable transactions with an anonymous counterpart. For example, certain money transfer companies allow the transfer of funds to an anonymous recipient who will use a pre-arranged password and code to collect the money.

¹⁶ Erland Johnson, "An Integrated Framework for Security and Dependability" in Proceedings of the 1998 New Security Paradigm Workshop (New York (?), ACM Press, 1999, p.25

As a consequence of this combination of functionality and behaviour, Johnson categorises security into two classes: *preventive security* and *behavioural security*. He argues that these two classes should also be called *preventive dependability* and *behavioural dependability*. In this argument, the terms can be used interchangeably since they combine functionalities and behaviours. Preventive security or dependability aims at stopping the insertion of faults into a system. Behavioural security or dependability aims at preserving the behavioural attributes of a system as expressed in terms of its reliability, availability and confidentiality.

1.2 Trustworthiness

Some confusion has been caused by the widespread use of the term "trustworthiness". According to the US National Research Council, a system is defined as *trustworthy* when it performs as expected despite environmental disruption, human user and operator errors and attacks by hostile parties. Trustworthiness encompasses the following attributes: "correctness, reliability (conventionally including secrecy, confidentiality, integrity and availability), privacy, safety, and survivability".¹⁷ Another definition refers to a trustworthy component as being a "component that has been shown to be deserving of the trust placed in it. A trustworthy component from a security point of view is dependable with respect to its security properties."¹⁸

At the system level, there appears to be some consensus that the concepts of dependability and trustworthiness are similar in content. The benefit of the term "trustworthiness" is that it may be more intuitively understandable to policy-makers than "dependability".

1.3 Survivability

The term "survivability" has also become increasingly prevalent in recent years. There has sometimes been confusion between the terms dependability and survivability but, as indicated in the definition of trustworthiness given above, it may be more helpful to regard survivability as providing a focus upon the dependability requirements of large scale systems operating in hostile environments.¹⁹

Peter Neumann from SRI International defines survivability as the ability of a "computer-communication system application to satisfy certain critical requirements in the face of adverse conditions".²⁰ A survivable system has four requirements: *security*; *reliability*; *availability*; and *performance*.

Thomas Longstaff *et al* from the Software Engineering Institute at Carnegie Mellon University define survivability as "the capacity of a system to fulfil its mission, in a timely manner, in the presence of attacks, failures and accidents".²¹ In particular, the term "system" encompasses "networks and large scale system-of-systems", which include the Internet and information infrastructures.²² According to Longstaff, any system is survivable when it:

¹⁷ National Research Council, Trust in Cyberspace, (Washington, DC, USA: National Academy Press, 1999) p.14

¹⁸ MAFTIA Conceptual Model and Architecture, p. 25.

¹⁹ Whereas the origins of "dependability" lie in the world of closed systems where the emphasis was upon faults rather than malicious attacks.

²⁰ Peter Neumann, Practical Architecture for Survivable Systems and Networks-Phase II: Final Report, ARL DAKF 11-97-C-0020, 30 June 2000, available at <http://www.csl.sri.com/neuman/survivability.pdf> (visited on 19 July 2001).

²¹ Thomas Longstaff, Survivable Network Systems: An Emerging Discipline, Technical Report CMU/SEI-97-TR-013 and ESC-TR-97-013, November 1997 and May 1999, pp.2-3

²² *ibid.* p.4

- Resists attacks
- Recognises attacks and the extent of damages
- Recovers full or essential services after the attack
- Adapts to reduce the occurrence of similar events in the future²³

Survivability and dependability often seem to refer to the same functionalities and behaviours. By withstanding an attack or failure, or even recognising one, a survivable system is able to preserve integrity, while safeguarding its overall availability, reliability and safety. Similarly, by being able to recover from attacks, a survivable system retains functionality in terms of confidentiality and integrity and displays dependable behaviours and processes.

However, Peter Neumann makes the distinction between the two concepts by arguing that dependability refers "to the extent to which a given requirement is perceived to be satisfied ... by the implementation".²⁴ Lipson and Fisher argue that survivability concentrates more on the trade-off between functional and non-functional requirements of a system.²⁵

Although there is an overlap between the two concepts, the language of survivability is particularly applicable to open systems operating in hostile environments. Notably, the concepts of "graceful degradation" or "failing soft" are embedded in the notion of survivability.

1.4 (Network and) Information Security²⁶

Although the elements of information security are a well-understood component of dependability (and trustworthiness), there is a tendency in many communities to focus upon information security as a topic and end in itself. European Commission documents have begun to prefix the term "Network" to this phrase in an effort to focus attention on the changing nature of information systems. Hence the definition in the June 2001 European Commission Communication on Network and Information Security:

"Network and information security can ... be understood as the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems."²⁷

The advantages of the term "information security" are that it refers to an intuitively straightforward concept (security) and that the discipline of information security²⁸ is widely understood and practised in

²³ Robert Ellison *et alia*, "An Approach to Survivable Systems", available at <http://www.cert.org/research>. (visited on 19 July 2001).

²⁴ Peter Neumann, Practical Architecture for Survivable Systems and Networks, p.6.

²⁵ Howard Lipson and David Fisher, "Survivability: A New Technical and Business Perspective on Security" in Proceedings of the 1999 New Security Paradigms Workshop, 22-24 September 1999 available at <http://www.cert.org/research/> (visited on 19 July 2001).

²⁶ Cyber-security is sometimes used as a journalistic shorthand but adds little to the established definitions given here.

²⁷ Commission of the European Communities, "Network and Information Security: Proposal for a European Policy Approach"

²⁸ And its cousins, "information systems security," "IT security" and "computer security."

both public and private sectors. Most public and private sector organisations have experience of physical security activities and many also have an entity or an individual responsible for information security. Indeed, the term is incorporated in the titles of some of the largest professional conferences in Europe (e.g. Infosec, Compsec, ISSE).

There are three disadvantages to the term. First, the discipline has traditionally focused more upon confidentiality/secretcy than on availability and integrity. Whilst this bias is vanishing, it can still distort the application of security guidelines. Second, it is a narrower concept than dependability. Third, in presentational terms, information security (like security more generally) often appears unattractive to senior management. It is often regarded as an unproductive cost-centre, especially in the private sector; there is therefore a problem of translating information security messages from technical and professional staff to senior management.

1.5 Information Assurance

In recognition of the need to broaden the scope of the concept beyond traditional information security, the concept of information assurance has become increasingly prevalent. The concept emerged from the US defence establishment which sought to emphasise that assurance of its information assets was critical to support its core business processes; i.e. it was becoming more than a specialist, technical security issue.

According to one definition, information assurance consists of “operations undertaken to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.”²⁹

In the words of Professor Eugene Spafford, the term information assurance is helpful

“because the issues are really larger than simply computer security. Information assurance covers issues of building safe and reliable information systems that are able to weather untoward events no matter what the cause — whether natural disaster or caused by a malicious individual. Whether critical data in a financial institution or defence agency is affected by a hardware failure, a power outage, a computer virus or a hacker doesn't matter in at least one sense: unless the system is resistant to the damage and built for assured operation, the data is gone.

... [In addition to cryptography] Information assurance also involves issues of physical security, malicious software, privacy, authentication technologies, software engineering, database security, network security, computer forensics, intrusion detection, and a number of other fields.”³⁰

The point is that the term information assurance ensures that the focus is on protection of information and information systems as a business enabler relevant to the highest levels of management.

²⁹ David E. Luddy, “Defense in Depth Strategy,” presentation to RSA 99 Security Conference *Industry/Government Partnerships: The Key to LA*, San Jose, 17-21 January 1999.

³⁰ Statement of Eugene H. Spafford, Professor of Computer Science and Director of Purdue University's Center For Education and Research in Information Assurance and Security, House of Representatives Science Committee, 10 October 2001.

1.6 Critical Infrastructure Protection/Assurance

Another term that has become prevalent is Critical Infrastructure Protection (CIP). In most communities, what is really meant by CIP is Critical Infrastructure Assurance but few are willing to adopt the acronym CIA due to its connotations.³¹ Although much of the focus of CIP activities in various countries is upon information systems dependability and information security/assurance, the concept is of course broader. Contemporary CIP activities build upon a long tradition of protecting critical physical infrastructures from physical disruption. Today's focus upon logical infrastructures and logical disruptions is a natural development of such work.

The benefits of the CIP/A concept are that it focuses attention upon the services that are being protected or assured rather than upon the technical sources of vulnerabilities and threats. The CIP/A concept can therefore be seen as one that originates from the perspective of government and society end-users of infrastructures rather than "bottom up" from researchers or technical specialists.

The disadvantages of the CIP/A concept are both political and conceptual. Politically, CIP has traditionally been seen as a national security question over which European institutions have no competence. Conceptually, by focusing attention upon "critical infrastructures" it remains rooted in the industrial era paradigm of distinct physical infrastructures. This may be outmoded in an era of converged and globalised infrastructures; it may be more helpful to focus upon service delivery as the goal rather than infrastructure protection as such.³² This may also help to define differential criticalities for different Information Society stakeholders.

1.7 Business Assurance & Corporate Governance

Critical Infrastructure Protection/Assurance tends to represent the perspective from national authorities. Dependability, trustworthiness and survivability tend to represent the perspective from the R&D community. Information security and assurance tend to represent the perspective from the operational security community in the public and private sectors. In the public and private sectors alike, however, none of these concepts tend to address the concerns of managers and executives.

Instead, concepts such as business assurance are emerging that highlight the fact that, in the Information Society, information will be the basis of economic value. Corporate value will therefore derive from effective management of risks to information-based assets. Citizens will also have to take responsibility for protecting the security (and privacy) of their information assets.

In a tangible sense, business assurance is being implemented through corporate governance guidelines, regulations and good practice that encompass management of information assets and information risks. One example was the UK's Turnbull report that explicitly assigned responsibility for management of risks, including information risks, and business continuity to corporate executives and Boards of Directors. Instantiation of this approach has been assisted by the shift in audit techniques to risk-based approaches.

(Information) Risk Management

³¹ Therefore, for example, US federal structures have adopted the following titles: President's Critical Infrastructure Protection Board (PCIPB), Critical Infrastructure Assurance Office (CIAO), Partnership for Critical Infrastructure Security (PCIS).

³² Revisions of the CIP concept are being explored in initiatives such as the UK's "National Resiliency Framework."

Attempts to assess risk, defined as “the uncertainty of loss,” seek to balance the cost of implementing assurance policies and technologies against the business costs posed by the potential downside from misuse. The process seeks to estimate the value to an organisation of possessing a given configuration of assurance capabilities by asking the logically inverse question: what would be the cost of the consequences of not possessing these assurance capabilities?

This approach has the advantage of translating the assurance valuation process to the well-understood domain of risk analysis.³³ Risk is defined as the product of vulnerability, impact and threat. Therefore: *Risk is a function of Vulnerability \times Impact \times Threat.*

The shift to risk-based approaches to information security, corporate governance and audit is in part due to a recognition that ensuring 100% dependability or trustworthiness in the future will not be possible due to the inherent “nature of information systems, their growing complexity, interconnection and susceptibility to intentional meddling.”³⁴ Rather, dependability or trustworthiness is about “making information (and communication) systems more ... (likely to) do what they are supposed to do and also ... (less likely to) do what they are not supposed to do.”³⁵

1.8 Conclusion

The philosophy underpinning DDSI is that dependability must be seen as a business enabler. Rather than being viewed as a burden and a drag on the exploitation of new ICTs, dependability and security are a necessary prerequisite for the emergence of the Information Society in Europe. eEurope can only be built if European-wide dependability policies are implemented that have the confidence of all stakeholders – including the corporate sector, the wider public and governments.

Part of the process of engaging all stakeholders will be to ensure the use of terms and concepts which are familiar and meaningful to different audiences but are also definitionally precise enough to avoid confusion and misunderstanding.

This section has highlighted the utility of the concept of dependability, which focuses upon the attributes of Availability, Reliability, Safety & Security. For the purposes of policy-making, dependability is sufficiently similar a concept to trustworthiness that the concepts can be used interchangeably. This section has also noted that a dependable system must be survivable and that the concept of survivability has particular resonance when applied to open systems operating in a hostile environment, as is increasingly the case with systems such as the Internet.

Security is an important functionality of a dependable system. It is important enough that its elements (confidentiality, integrity, availability, authentication & non-repudiation) are the subject of particular social and policy interest under the rubric of network and information security.

In order to promote an understanding of information security and dependability in the Information Society amongst suppliers, users, owners and operators of information systems, it may be advisable to adopt the concept of information assurance and to embed this in the broader concepts of business assurance, underpinned by contemporary approaches to information risk management.

³³ Daniel E Geer, Jr, “Risk Management is where the Money is,” paper delivered to *the Digital Commerce Society of Boston*, 3 November 1998, available at <http://www.sans.org/geer98.txt>

³⁴ Marjory S. Blumenthal, “The Politics and Policies of Enhancing Trustworthiness,” in *Trustworthiness: Evolution of Concept and Policy*, (Draft September 1998), pp.1-2.

³⁵ *Ibid.*, p. 1.

2 European Information Infrastructures

This section provides an overview of what is meant by European information infrastructures.

The goal of this section is to emphasise the pivotal role for the socio-political and economic development of Europe of its information infrastructures. Particular attention is devoted to the implications of new technologies, market convergence and the impact of new regulatory developments. The section also provides an overview of the place of European information infrastructures within the global information infrastructure and of the interdependencies between information infrastructures and other infrastructures.

2.1 Defining the Information Infrastructure

The information infrastructure³⁶ has traditionally been defined as “that system of advanced computer systems, databases and telecommunications networks ... that make electronic information widely available and accessible. This includes the Internet, the public switched network and cable, wireless and satellite communications.”³⁷

This definition was expanded upon in a European Commission workshop, which found that:

“The convergence of computer and communications technologies has created a global infrastructure for the transmission and processing of information. This new infrastructure is based on the ability of diverse networks to be interconnected and provide global coverage for the transmission of data. The defining characteristic of this global infrastructure is the absence of central monitoring and control in contrast to conventional computer communications systems.

Communications networks and services are increasingly moving towards a layered model, consisting of interconnected communications networks with data services and applications operating on top. The layering of services implies that lower layers details are hidden from higher layers and that the dependability (availability, security) of upper-layer applications rely in large part on performance of lower layer services and networks.”³⁸

However, the emerging information infrastructure is in fact a much broader concept, captured in the notion of “pervasive computing.” As the European Commission recognises with its concept of “ambient intelligence,” the future European information infrastructure will involve the convergence of networked

³⁶ The Joint Research Centre’s term “communications infrastructure” is parallel as it is defined as: “the collection of hardware equipment and procedures (software, management) for transporting data needed by an application to deliver specified services to the users.” Nicholas Kyriakopoulos and Marc Wilikens, Dependability and Complexity: Exploring Ideas for Studying Open Systems-Full Report, 15 December 2000.

³⁷ Adapted from definition of NII in: US Senate Permanent Subcommittee on Investigations, Hearings on “Security in Cyberspace,” 5 June 1996. The Information Assurance Advisory Council defines the information infrastructure as: “The information, the information channels, information processes and the information channel bearers that are needed to support the infrastructure. Infrastructure Protection is concerned with threats to both the functioning of such infrastructures and to the information carried on such infrastructures.” www.iaac.org.uk

³⁸ EC IST programme consultation meeting on “Infrastructure Adaptability and Survivability for Dependable and Reliable Services”. Report of the workshop held in Brussels on 23 May 2000. Report available also on <http://www.cordis.lu/ist/fpd/wpconsult.htm>

embedded and hybrid systems that will immerse citizens in an information environment and in which physical control systems will increasingly migrate online.

For policy-making purposes, though, it is important not to limit attention to information systems and networks, as was done in the June 2001 Communication which concentrated upon: "Networks [which] are systems on which data are stored, processed and through which they circulate."³⁹ For European citizens and Information Society stakeholders, the dependability and security of information networks and systems is not an end in itself. There are two ways of characterising this higher level. One approach is that which has come to be adopted in the US Critical Infrastructure Protection programme which focuses upon assuring delivery of critical services such as power and transportation, regardless of whether threats are physical or digital.

Another approach is to focus upon information assurance, in other words assuring the societal "digital (or information) environment."⁴⁰ This approach points to information as the asset of concern and starts from the perspective that it is assurance of the business and societal processes supported and enabled by information networks that is of concern ; i.e. Information Society service delivery. In a society in which information is the key asset, information assurance translates into business assurance at the highest levels.

When it comes to defining the actual European information infrastructure, problems are caused by the constantly changing nature of technology and of services. In light of the emergence of new technologies and services, the actual elements and structures are in a permanent state of flux. Data and information can now be transmitted through diverse channels such as, for example, fixed and wireless lines or through satellites.⁴¹ These may require different transfer and transport protocols. More importantly, information and data can be processed through a large variety of instruments including, for example, from servers, personal computers, digital TVs, digital assistant, mobile phones and many others. Policy therefore needs to be cognisant of this rapid pace of change and needs to remain technology neutral so as not to hinder market developments.

2.2 European Information Infrastructures: Regulatory, Technological & Commercial Developments

Europe has developed a complex and pervasive information infrastructure, which is now a critical and essential part of its socio-political and economic well-being. This becomes evident when examining quantitative data on Internet access and use in Europe. According to the European Commission, Internet home penetration has been showing signs of steady growth. In the period between March and October 2000, penetration rates increased an average of 20% in each Member State. At the moment, almost half of the European population might be considered Internet users. Although the large majority of them access it either by dial-up at home or in the office, a growing percentage are exploiting the potential of accessing through more advanced means such as ISDN lines, cable modems or TV set-top boxes.

³⁹ Commission of the European Communities, "Network and Information Security: Proposal for a European Policy Approach"

⁴⁰ DERA, An Analysis of the Military and Policy Context of Information Warfare, June 1997, (DERA/CIS3/58/8/5).

⁴¹ Concerning Internet in space, it might be interesting to look at the activities and prospects of Teledesic. For more information see <http://www.teledesic.com> (visited on 24 August 2001)

According to a survey conducted by the Organisation for Economic Cooperation and Development (OECD), between March and September 2000, access costs declined by more than eight percent.⁴²

Together with individuals, public and private organisations are increasingly exploiting the potentials of the information infrastructure. A growing number of European governments are providing their services online. According to the European Commission, about 25% of Internet users have accessed government websites, although only 10% have filled out forms or completed financial transactions online. Meanwhile, European businesses are becoming more active, especially in the area of business-to-business e-commerce activities, which are often an extension of past electronic data interchanges (EDI).⁴³

The expansion of these novel information capabilities and services can be related to a combination of regulatory, business and technology trends, which are set to continue in the future. A first major development has been the overall trend toward the liberalisation of European market sectors. Particular attention should be given to the telecommunications sector. In this area, the liberalisation process began during the 1980s and led to the rapid introduction of competition for the provision of telecommunication and information services. The so-called "national telecommunication champions" have started to face strong competition inside their markets as new players have begun to offer services. This competitive environment is being further encouraged as a more advanced European telecommunication regulatory framework is put in place.⁴⁴ A visible example of this competitive environment is the wireless industry.⁴⁵ For example, in the United Kingdom, one of the leading operators of mobile phones, Orange, is controlled by France Telecom. Meanwhile, Italy's Omnitel is led by the Vodafone Group, the global leader in mobile telephony.⁴⁶

Globalisation is another main factor explaining the expansion of the European information infrastructure. The European infrastructure is just part of the global information and network infrastructure. This is most evident in the case of packet-switched networks, such as those forming the Internet, where data may reach its destination by crossing the borders of many different countries, without the need of any pre-programmed routing. By being part of a global infrastructure, European users benefit from the worldwide growth of ICT. This can be easily explained through the concept of "positive network externalities".

The term "externalities" refers to a situation where the value of a particular good or instrument is assessed not only according to its features and qualities, but also by the number of its users. A network, such as the European information infrastructure, experiences "positive externalities" when its value increases

⁴² Commission of the European Communities, "E-Europe 2002: Impact and Priorities", COM (2001), 140 Final, 13 March, 2001.

⁴³ Commission of the European Communities, "E-Europe 2002: Impact and Priorities", COM (2001), 140 Final, 13 March, 2001.

⁴⁴ An overview of the overall contents of the European regulatory framework is available at http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm (visited on August 24). For a set of interesting set of proposed courses of action for the future of telecommunication regulatory initiatives see W. Russel Neumann, Lee McKnight and Richard Jay Solomon, The Gordian Knot: Political Gridlock on the Information Highway, (London, UK: The MIT Press, 1998)

⁴⁵ For a general overview see Squire Sanders and Dempsey, Final Report of the Study for the Development of Competition for Electronic Networks and Services and Inventory of EU Must Carry Regulations, Report on behalf of the DG Information Society, April 2001 available at http://europa.eu.int/information_society/topics/telecoms/regulatory/studies/new_rf/index_en.htm (visited on 24 August, 2001)

⁴⁶ For more information see the websites <http://www.orange.co.uk>, <http://www.vodafone.co.uk>, and <http://www.omnitel.it>

exponentially as more users connect and transact over it.⁴⁷ The following micro-level example provides a better understanding of this state of affairs. When an individual decides to use the same spreadsheet package as that of one or two other actors, he or she benefits from the fact that his or her documents can be read immediately by two other individuals. However, the two actors also profit from this choice since they have another potential user of their files and, consequently, services and products. Due to network externalities, it is clear that the more the global information infrastructure expands, the better it is for Europeans as individual and business users since they have a larger set of potential recipients for their services and goods.

2.2.1 Convergence

These positive network externalities and the overall value of the European and global information infrastructures are facilitated by convergence between different services. At the micro-level, this is typified, for example, by the growing success of digital TV services, where users can access the Internet and other services through their TV set.⁴⁸ This convergence is also evident at the macro-level where information and telecommunication services are delivered by non-traditional providers. This situation becomes evident when looking at the increasing number of European utilities companies (water, electricity, etc.) offering information and telecommunication services. In France, Vivendi, formerly known as Generale des Eaux, is now involved in the provision of Internet and broadband services.⁴⁹ In the United Kingdom, the gas provider CENTRICA is offering telecommunication services. In Italy, local utility companies, such as Rome's ACEA and Milan's AEM, have teamed with national and international companies to provide broadband services, Internet and advanced telecommunication services.⁵⁰

This convergence is also becoming more evident in the overall e-business environment. A growing set of financial companies are in the process of teaming up with Internet and telecommunications providers, as well as utilities, to provide their clients with one single general account through "aggregation services".⁵¹ Business and individual users will soon be able to have on one screen all of their accounts while requesting all their major services from a single "multiple source" company.

2.2.2 The Wireless Era

Networking, especially in small environments like homes and offices, has been associated primarily with cables and other physical links. This situation is poised to change due to the growing success of wireless

⁴⁷ For more information on the notion of "network externalities" see Michael Katz and Carl Schapiro, 'Network Externalities, Competition and Compatibility', *American Economic Review*, vol.73 no.3 (April 1985), pp.424-440, *ibid.* "Systems Competition and Network Effects", *Journal of Economic Perspectives*, vol.8 no.2, (1994), pp.93-114; Niko Economides, 'The Economics of Networks', *International Journal of Industrial Organisation*, vol. 14 no.6, (April 1996), pp. 673-693 and Carl Shapiro and Hal Varian, *Information Rules*, (Cambridge, Mass, Harvard Business School Press).

⁴⁸ An overview of the development of digital TV in Europe see IDATE, "Development of Digital Television: Report on Behalf of the DG Information Society" February 2001, available at http://europa.eu.int/information_society/topics/telecoms.regulatory/studies/index_en.htm (visited on 24 August 2001)

⁴⁹ For more information see <http://www.vivendi.fr>

⁵⁰ For more information see <http://www.acea.it> and <http://www.aem.it>

⁵¹ An interesting example is the case of MyWellsFargo, a service provided by the US financial institution Wells Fargo, through which account holders can have a view of all their financial dealings by combining data from other institutions. See <http://www.wellsfargo.com>.

networking technologies and products. Offices, airports and many other public places, both in Europe and the United States, are fielding “access points” so that individuals can move freely.⁵² Individuals and organisations can now move away from committing large financial resources to laying cables to fit office premises or even homes. The penetration of wireless networks has been fostered by the technical flexibility of wireless networking protocols, such as IEEE 802.11b and Bluetooth, whose implementation does not require advanced technological knowledge.⁵³

The success of wireless networking, nevertheless, has not come without risks and dangers. Researchers and journalists have already warned about the vulnerabilities of the protocols.⁵⁴ During a recent information security workshop organised by the OECD, Vint Cerf, vice president of WorldCom, warned industry and governments about the need to raise awareness among individuals about the risks of exchanging information and data over the air.⁵⁵

2.3 Global Information Infrastructure Dependencies

Whilst the globalisation of information infrastructures brings economic and social benefits it also means that the European information infrastructure is no more an independent, self-reliant entity than is the information infrastructure of any one Member State. All are inextricably linked into the global information infrastructure. Indeed, as the JRC notes: “by its nature, the ... Internet, renders national borders almost irrelevant with respect to the transmission of information. In some cases, even the constituent sub-networks may span more than one States.”⁵⁶

These global interdependencies are evident at all levels of the information infrastructure, from the physical and logical elements of the network, through the transport and middle layers to the application layer. One widely publicised element of this interdependency, for instance, is the global reliance on a handful of Domain Name Servers (DNS) which can constitute single points of failure. Another is the development of a software “monoculture” that has facilitated the spread, for instance, of MS Outlook viruses and worms.

2.4 Wider Societal Dependencies

In addition to the development of the information infrastructure itself, it is important to emphasise the extent to which other societal infrastructures have become intertwined with the information

⁵² For more information about wireless networks in airports, see the activities of the US based organisation, Wireless Airport Association at <http://www.wirelessairport.org> (visited 3 October 2001)

⁵³ For an general overview of IEEE 802.11b see <http://krypton.mnsu.edu/~kawatra/ieee80211.htm>. The activities of IEEE 802.11b are available at <http://www.ieee802.org>. (visited on 3 October, 2001). For an overview of Bluetooth, see the Official Bluetooth website at <http://www.bluetooth.com> (visited 3 October, 2001)

⁵⁴ For an interesting overview, see Sultan Weatherspoon, “Overview of IEEE 802.11B Security”, *Intel Technology Journal*, 2nd Quarter 2000, available at http://developer.intel.com/technology/itj/q22000/articles/art_5.htm (visited on 3 October, 2001). In order to begin to tackle these security issues, IBM Research has recently launched Wireless Security Auditor. For more information about its functionalities, see http://www.research.ibm.com/resources/news/20010712_wireless.shtml (visited on 3 October, 2001) and <http://www.research.ibm.com/gsal/wsa/> (visited on 3 October, 2001)

⁵⁵ Vint Cerf, Keynote Address before the OECD Cybersecurity Workshop: Information Security in a Networked World, Tokyo, Japan, 12 September 2001.

⁵⁶ Nicholas Kyriakopoulos and Marc Wilikens, Dependability and Complexity: Exploring Ideas for Studying Open Systems-Full Report, 15 December 2000.

infrastructure. The Y2K problem brought this dependency into public focus. Y2K demonstrated that not only were information assets embedded in a wide range of other activities, such as manufacturing, but that all of modern society's other infrastructures such as transport, energy, finance, water, government and retail were dependent on the information infrastructure and also, to varying degrees, upon one another.

The growing interdependence and tight connectivity between these infrastructures means that failures in one sector can have a cascading impact on other sectors. Unfortunately, most modern infrastructures share one common element: they all use software and hardware solutions that may carry inside them a set of faults.

The problem this may pose was described by a study conducted in the Netherlands which argued that:

“market pressures and the widespread use of ICT make the risk of large-scale (multi-modal) disruptions, involving several infrastructures simultaneously, increasingly likely in the future. In terms of the availability and reliability of ICT-infrastructure, none of the parties concerned (government, infrastructure operators, the business community or society) is prepared for large-scale disturbances and disruption.”⁵⁷

Furthermore, the combination of European dependence on the global information infrastructure and the interdependencies of this infrastructure with other socially critical infrastructures should also focus attention on extra-European infrastructures aside from the information infrastructure. For instance, the European electrical power grid, upon which other infrastructures rely, depends increasingly upon extra-European energy supplies.

⁵⁷ H.A.M. Luijff & Dr. M.H.A. Klaver, In Bits and Pieces: Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society (Infodrome, 2000).

3 Risks to Information Infrastructures

This section discusses the categories of risks to the dependability of European information infrastructures and explains the processes by which faults and vulnerabilities can lead to failures.

Within the dependability community, there is a well developed approach to the analysis of faults and the process by which these faults may become system failures that impact upon the services that users' receive. The "fault-tree" approach is a very useful way in which to understand risks to information infrastructures and mitigation strategies. Recent work on dependability requirements in relation to malicious attacks has brought together the language of faults with that of vulnerabilities.⁵⁸ This is helpful for policy-makers since the language of vulnerabilities fits more easily into the widely accepted language of risk assessment in which risk is the product of vulnerability, impact and threat.

3.1 Faults & Vulnerabilities

Avizenis *et al* have defined three general classes of faults: physical, design and implementation and interaction. These categories can also be used to structure our analysis of vulnerabilities.

3.1.1 Physical Faults

These faults are primarily related to the physical components of a system. They may be the consequence of physical deterioration⁵⁹ or software ageing.⁶⁰ In addition, the external environment surrounding the system may change to such an extent that faults occur. Examples include "acts of God", such as storms or floods. Another example would be a sudden increase in access requests which a system is not able to handle.⁶¹

Another important category of physical faults or vulnerabilities are the associated infrastructures upon which information infrastructures depend, primarily power and energy but also transport and finance. The critical dependency of information infrastructures upon power supplies is evident but, as interdependency analyses during Y2K demonstrated, these infrastructures are dependent upon a wider feedback relationship to function. For instance, power supplies may depend upon transport of fuels, which may in turn be dependent upon an information system to manage distribution and ordering.⁶²

The physical behaviour of systems may also be considered as a source of faults in itself, as exemplified by the phenomenon of *Vac Eck Phreaking*.⁶³ This refers to the possibility of obtaining information on signals and data inside equipment when electro-magnetic radiation is picked up and signals are decoded.⁶⁴

⁵⁸ MAFTIA Conceptual Model and Architecture, pp. 16-17; Bob Anderson, et al., Securing the US Defense Information Infrastructure: A Proposed Approach (1999), available at: <http://www.rand.org/publications/MR/MR993>.

⁵⁹ E.g. deterioration of cabling, metal fatigue in components.

⁶⁰ Progressively accrued error conditions resulting in performance degradation or activation of faults.

⁶¹ Laura Unger, Online Brokerage: Keeping Apace of Cyberspace, Final Report of a Special Studies for the US Stock and Exchanges Commission, November 1999 available at <http://www.sec.gov/news/studies.shtml> (visited on 2 August 2001)

⁶² Edward E. Balkovich & Robert H. Anderson, Critical Infrastructures Will Remain Vulnerable: Neighborhoods Must Fend for Themselves (RAND: 2001).

⁶³ Information from <http://www.sans.org/infosecFAQ/encryption/TEMPEST.htm> (visited 3 October 2001).

3.1.2 Design and implementation faults

The core elements of an information infrastructure may be software (protocols, operating systems and applications) and hardware (routers, NAP, exchanges, cables, etc.). Faults in the design and development of each of these elements may impact on the functionalities of the overall infrastructure. It is difficult to assess the number of design faults inside software and hardware solutions. The Computer Emergency Response Team - Coordination Centre (CERT-CC) has reported almost 4,000 worldwide vulnerabilities since 1995. CERT-CC also issued over 300 security alerts and over 200 security notes and handled over 370,000 email messages concerning faults and similar topics.⁶⁵ These figures by no means represent the totality of design and implementation faults as faults are not always reported.

Bev Littlewood and Lorenzo Stringini from the Centre for Software Reliability at City University, London have proposed four factors explaining the high number of design faults in today's software and hardware applications: novelty; difficulty; complexity; and assurance.⁶⁶

In the contemporary commercial and socio-political environment, individuals and organisations are looking to software-based applications and tools as solutions to a wide range of problems. This *novelty* pushes software developers to create tools and solutions based on minimal previous experience. The implications of novelty are magnified by the increasing *difficulty* in coding and integrating software solutions. Clearly, "the more difficult and novel the task, the more likely that mistakes will be made, resulting in the introduction of faults which cause system failure when triggered by appropriate input conditions".⁶⁷ An example of the consequence of these two factors is the rising number of faults in wireless networks and infrastructures.⁶⁸

The *complexity* of today's software and hardware solutions is the third possible explanation of the increasing number of system faults. The need for complex hardware and software solutions to cater for the ever-changing requests of today's users can lead developers to lose sight of the overall functionalities of the system or infrastructure. This contradicts, argue Littlewood and Stringini, one of the covenants of software engineering: "a system should not be more complex than it need be to deliver the needed functionality".⁶⁹ In conjunction with novelty and difficulty, complexity has undermined the capacity to assess the *assurance* of the overall functionalities of a system since the testing environment is often different from the real one.

⁶⁴ Van Eck Phreaking is often confused with the term TEMPEST, which indicates the technical and logistical processes and procedures to protect organisations from the information security risks associated with the diffusion of electro-magnetic radiations. TEMPEST is an acronym for Telecommunications Electronics Material Protected from Emanating Spurious Transmissions. For more information see the US NSA Endorsement Programme at <http://www.nsa.gov/isso/bao/tep.htm> (visited 3 October 2001). For an historical overview of TEMPEST-related initiatives see <http://www.eskimo.com/~joelm/tempestintro.html> (visited 3 October 2001)

⁶⁵ CERT/CC Statistics 1988-2001 available at http://www.cert.org/stats/cert_stats.html (visited on 27 July, 2001)

⁶⁶ Bev Littlewood and Lorenzo Stringini, "Software Reliability and Dependability: A Roadmap", in *ibid.*, Future of Software Engineering (New York: ACM Press, 2000), pp.177-188.

⁶⁷ *ibid.* p. 178

⁶⁸ Sue Marek, "Not 'Old Reliable' Quite Yet; Wireless Networks Still Experience Delays In SMS Delivery", WirelessWeek, June 18, 2001, p.18, "Verizon Web Service Returns to Business in Seattle after Three Days Outage", Seattle Times, March 16 2001. For an historical overview of system faults see Peter Neumann, Computer-Related Risks, (Cupertino, CA: Addison Wesley), 1995

⁶⁹ *ibid.*, p.179

This analysis has focused so far on faults originating during the design phase. Many faults occur when systems enter the implementation stage and become networked. One problem is that software and hardware solutions are regularly updated to satisfy users' needs. These updates can lead to new faults and vulnerabilities. Further, new faults may arise when different systems become integrated with other networks. In both cases, novelty, difficulty, complexity and lack of assurance provide plausible explanations for the origin of these faults. As exemplified by the European information infrastructure, network environments are in a dynamic flux related to ever-changing user needs. Different systems and technologies are often rapidly coupled together and integrated without a full appreciation of possible faults and vulnerabilities.⁷⁰

3.1.3 Malicious Logic

This consists of malicious internal faults, including developmental faults such as logic bombs and Trojan horses and operational faults such as viruses and worms.

3.1.4 Intrusions and Attacks

Research into intrusion tolerance techniques aims to design systems that “tolerate the fact that vulnerabilities have been successfully exploited by an attacker.”⁷¹ An intrusion can be defined as “a malicious, externally-induced, operational fault.”⁷² This can encompass a fault perpetrated by an insider since “the intent is to carry out an operation on some resource that is unwanted by the owner of that resource.” There is a distinction between an “intrusion” and an “attack” since “an attack is an *intrusion attempt* and an intrusion results from an attack that has been (at least partially) successful.” There are therefore two causes of any intrusion:

- An *attack* that attempts to exploit a weakness in the system
- At least one weakness, flaw or *vulnerability* (i.e. an accidental or intentional fault)

Typical examples of intrusions are:

- An outsider penetrating a system by guessing a user password
- An insider abusing his authority
- An outsider using “social engineering” to cause an insider to carry out a misfeasance on his behalf
- A denial-of-service attack by request overload

Interdependent Faults

The faults outlined above may be independent but can also be interdependent, for instance if attackers intrude into a system by exploiting a design fault. For example, a programming bug inside a transmission protocol or an operating system may be viewed as an accidental fault created by a programmer during its design phase. Conversely, a logic bomb or Trojan horse could be an intentional design fault. The malicious software could be placed inside a system during either the development or the operational phase

⁷⁰ This problem is highlighted by the fact that certification processes such as Common Criteria often fail to keep up with the market demand for system implementations other than those verified during the testing process.

⁷¹ MAFTIA Conceptual Model and Architecture, pp. 24-25.

⁷² Discussion below adapted from: MAFTIA Conceptual Model and Architecture, pp. 24-25.

by an insider (*a disgruntled programmer*)⁷³ or an outsider (*a malicious hacker*).⁷⁴ It can then be exploited by an attacker at some point during the implementation phase.

3.2 Errors and Failures

Faults and vulnerabilities by themselves do not undermine the dependability of a system or of an information infrastructure. It is only when *faults* turn to *errors* that in turn lead to *failures* that undermine the user-defined functionalities of a system, that dependability is undermined.

An *error* is the external manifestation of a fault. Not every fault becomes an error. Systems may have built in a set of mechanisms to prevent this progression. Indeed, a major area of research today is into fault tolerant systems. Nevertheless, even if a fault manifests itself in an error, it does not mean that the system experiences a *failure*. As argued by Laprie, a failure "occurs when an error reaches the service interface and alters the service".⁷⁵ *Failures*, therefore, are processes affecting the service that a user expects to receive from a system or an infrastructure.

Failures may be classified according to three categories: Domain (value and timing); Perception (consistent and inconsistent); Severity (benign and catastrophic).⁷⁶

The *domain* category considers failures according to their impact on the overall value and timing of a system. The former describes failures impacting on the overall value of the system itself and/or activities based upon it. The latter depicts failures which undermine the timing specifications of a system. The e-commerce world can provide examples of both failure types. One of the advantages of shopping online is the ability to buy goods at any time of the day and night and have them delivered directly to the home or the office. Failures of the e-retailer's systems, therefore, produce both effects. They do not allow customers to order the goods (*value failure*) or to do so at their convenience (*timing failure*).

Failures can also be classified according to the *perception* that they create for the users of a system. These failures can be *consistent* and *inconsistent*. In the first case, all system users are aware of the failure, which is not the case in the second scenario. The distinguishing factor is the pervasiveness of the service provided by a system.

Finally, the *severity* of failures can be classified as *benign* or *catastrophic* in light of their overall impact and implications. Benign failures do not impair the overall value of the system as losses may be recouped through other means. Catastrophic failures have economic and socio-political consequences which are difficult or impossible to reverse. Examples can be the breakdown of a large health information system,

⁷³ For an overview of the threat to systems caused by authorised users, see Peter Neumann, Research and Development Initiatives Focused on Preventing, Detecting and Responding to Insider Misuse of Critical Defence Information Systems: Results of a Three-Day Workshop, available at <http://www2.csl.sri.com/insider-misuse/ins.html> (visited on 17 November 2000)

⁷⁴ Under the Council of Europe cyber-crime convention, the former may be seen as *data interference*, defined as the unauthorised and intentional damaging, deletion, deterioration, alteration or suppression of computer data. The latter may be defined as *system interference*, i.e., the hindering of a computer system through the insertion, transmission, damaging, deleting, deteriorating, altering or suppressing computer data. Council of Europe-European Committee on Crime Problems, Draft Convention on Cybercrime and Explanatory Memorandum Related Thereto, Docn. n. CDPC 2001 (2 rv), Strasbourg 25 May 2001, pp. 9-10.

⁷⁵ J.C. Laprie, "Dependability: A Unifying Concept for Reliable Computing and Fault Tolerance" in T. Anderson (ed.), Dependability of Resilient Computers, (Oxford: BSP Professional Books, 1989), pp.10

⁷⁶ A. Avizienis, J.C. Laprie and Brian Randell, Fundamental Concepts of Dependability, p.11

which impact on the well-being of patients and medical personnel or the failure of an air-traffic transport system leading to collisions between aircraft.

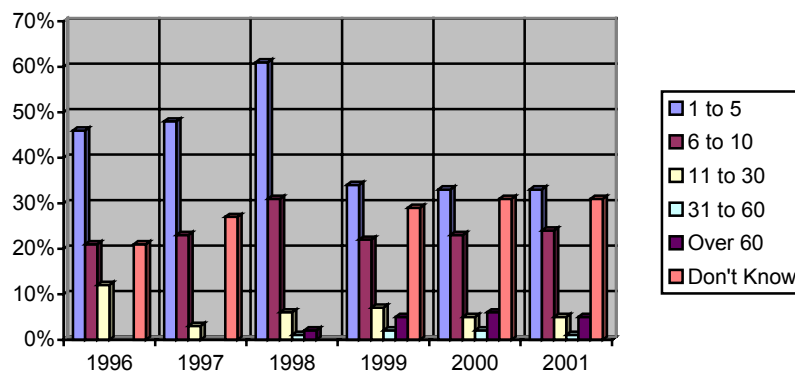
3.3 Threats

Threats to information systems may come from a range of sources, including design or implementation problems, human error or natural disasters. A growing challenge is the class of malicious attacks. This class of threats has been characterised by the G-8 as: “threats to computer infrastructures, which concern operations to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computer and networks themselves.” In the language of dependability, these are “uncontained interaction faults” in which attackers exploit vulnerabilities to intentionally cause errors and failures.

Malicious threats may arise from a range of actors including recreational hackers, criminals, terrorists and states.⁷⁷ A reliable quantitative assessment of the extent of these activities is extremely difficult. It remains a significant problem for policy-makers that data on such threats is partial, fragmented and unreliable. Better “metrology,” including statistics and trend analysis are important prerequisites for improved risk assessment and policy-making.

The statistics offered by the San Francisco-based Computer Security Institute (CSI) provide some background. In 2001, the number of organisations surveyed by the CSI that had detected intrusions or security breaches rose over ninety per cent from the previous year. Sixty four per cent of respondents acknowledged financial losses due to online malicious activities.⁷⁸ The table below shows the number of incidents that the organisations surveyed by the CSI reported. The last three years are remarkably consistent in the percentage of incidents reported.

Number of incidents



Source: **2001 CSI/FBI Computer Crime and Security Survey**⁷⁹

Although the large majority of these incidents are caused by internal authorised human actors, the Computer Security Institute (CSI) found that, for the fourth year running, more respondents cited their Internet connection as a principal point of malicious intrusions (70%). Indeed, organisations indicated that

⁷⁷ Concerning an overview of hacking activities, see Paul Taylor, *Hackers: Crime in the Sublime*, (London: Routledge, 1999)

⁷⁸ 2001 CSI/FBI Computer Crime and Security Survey p.4

⁷⁹ 2001 CSI/FBI Computer Crime and Security Survey p.7

hackers were more likely to be the cause of intrusions and other malicious activities than authorised individuals. (81% vs. 76%).⁸⁰

Similar data has emerged in the United Kingdom. According to the annual Information Security Breaches Survey 2000 sponsored by the Department of Trade and Industry (DTI), over sixty percent of organisations had suffered an intentional malicious intrusion in the preceding two years.⁸¹ This becomes more evident in relation to the case of failures brought about by malicious software like the infamous MELISSA or ILOVEYOU. The Labs Computer Virus Prevalence Survey 2000, an annual survey conducted by the US-based International Computer Security Association, noted that the likelihood of a virus hitting an Internet-connected organisation has doubled each year between 1996 and 2000.⁸²

3.4 Conclusion

This section has pointed out that failures are the consequence of a progression starting with faults and vulnerabilities. This process is not automatic as faults may remain dormant without leading to errors and failures. The error process may start *accidentally* or be triggered *intentionally* by a malicious actor. Failures are the final point of this process and may themselves create new faults.

Threats to information systems arise from multiple sources, including design faults, human error, natural disaster and malicious acts. Malicious threats may arise from recreational hackers, criminals, terrorists and states. Assessing the extent of these malicious activities is difficult due to a paucity of reliable and consistent data.

To mitigate these risks, the overall aims of dependability policies should involve:

- a) Limiting the initial development of faults and vulnerabilities that can be exploited
- b) Controlling the process connecting faults to errors and failures
- c) Managing failures to mitigate their consequences for users
- d) Understanding the risks from, and extent of, malicious acts
- e) Limiting attacks that exploit faults and vulnerabilities

⁸⁰ The rising threat from external attackers was also noted in a survey by the UK's Confederation of British Industry in 2001.

⁸¹ http://www.dti.government.uk/cii/datasecurity/infosecuritybreachsurvey2000/headline_news.shtml (visited on 15 August 2001)

⁸² <http://www.trusecure.com/html/tspub/pdf/vps20001.pdf> p.10 (visited on 17 August 2001)

4 Dependability Requirements for Trust and Confidence

This section discusses the broader societal implications of information infrastructure failures and the reasons why a public policy response is required.

The success of the Internet and other information infrastructures has been primarily due to the fact that individuals, public institutions and private organisations recognise the benefits of transferring some of their activities from the physical to the digital domain. Successful Internet-based business-to-business (B2B) and business-to-consumer (B2C) activities involve "relational exchanges" that allow commercial and government organisations, as well as individuals, to buy and sell products and services more efficiently over the Internet and other networks.⁸³

Relational exchanges do not originate in a vacuum. In the physical world, they build upon trust and confidence between different actors, which is enhanced by instruments such as brands, location and legal norms and rules.⁸⁴ In online environments, trust involves instruments such as computer and network systems and large information infrastructures. These instruments are expected to be able to deliver a set of functionalities and services that sustain trust and confidence among distant actors and thus support relational exchanges.⁸⁵ Trust and confidence arise when users view these communication and information mechanisms as dependable.⁸⁶ This perception can be undermined by failures.⁸⁷

That the lack of dependability is having an impact on trust and confidence is demonstrated by numerous surveys in the USA and Europe. These surveys indicate that users have not developed sufficient trust and confidence in information infrastructures.

4.1 The Lack of Trust in Online Activities: A Perspective from the United States

Donna Hoffman and Thomas Novak from the Owen Business School at Vanderbilt University have quantified the impact of concerns about privacy and security violations in terms of user perceptions of system dependability. According to their analysis of the results of the 1997 CommerceNet/Nielsen Internet Demographic Survey, around 50% of US Internet users refrain from engaging in online relational exchanges due to their lack of confidence in the security and reliability of their systems.⁸⁸ Similar results

⁸³ For more information on the notion of relational exchanges, see John George, "Do Norms Matter in Marketing Relationship?", *Journal of Marketing*, vol.55 (April 1992), pp.32-44, Gregory Gundlancy and Patrick Murphy, "Ethical and Legal Foundations for Relationship Marketing Exchanges", *Journal of Marketing*, vol.56 no.3 (October 1993), pp.35-46, Christine Norman and Gemral Zaltman, "Factors Affecting Trust in Marketing Research Relationships", *Journal of Marketing Research*, vol.29 no.2 (August 1992), pp.314-329.

⁸⁴ Concerning the impact of legal norms and rules on trust and confidence, see Fernando Flores and Robert Solomon, "Creating Trust", *Business Quarterly*, vol.8 no.2 (April 1998) and Robert Morgan and Shelby Hunt, "The Commitment-Trust Theory of Relationship Marketing", *Journal of Marketing*, vol.58 no.3 (July-September 1994), pp.23-34.

⁸⁵ An interesting overview is provided by Peter Keen, Craig Balance, Sally Chan and Steve Schrupp, *Electronic Commerce Relationships: Trust By Design* (London: Prentice Hall, 2000)

⁸⁶ John Butler, "Towards Understanding and Measuring Conditions of Trust: An Inventory", *Journal of Management*, vol.17 no.4 (April 1991), pp.643-663.

⁸⁷ Kriistina Karvonen, "Creating Trust" in *Proceedings of the Fourth Nordic Workshop on Secure IT Systems (NORDSEC 99)*, held in Krista, Sweden, 1-2 November 1999

⁸⁸ Donna Hoffman, Thomas Novak and Marcos Peralta, 'Building Consumer Trust Online', *Communications of the ACM*, vol.42 no.2 (April 1999), pp.81-84.

emerged from an AT&T survey, which found that 87% of Internet users were concerned about their personal online privacy. Similarly, the Pew Internet American Life Project, which was released in August 2000, concluded that US Internet's users have an overall distrust towards this communication and information medium. This is due to fears about misuse of personal data, illegal disclosure of financial details and general cyber-crimes.⁸⁹

More recently, pollsters from Gallup reported that more than three quarters of US Email users are concerned about the security of their credit card details. The same survey concluded that *only* 5% of US Internet users were significantly comfortable with giving financial details to online institutions. The data emphasises that US individuals are deeply concerned for the privacy and security of their online information and transactional activities. These fears have been magnified by the rising number of online frauds which often involve the exploitation of software faults by the fraudster. According to data from Internet Fraud Watch, in the period between January and September 2000, credit card and securities frauds and online identity thefts accounted for almost a quarter of online scams in the United States.

US Internet users, moreover, seem to have difficulty in trusting their government's information systems. A survey conducted in September 2000 by the Information Technology Association of America revealed that 63% of respondents were not likely to engage in electronic transactions with government institutions due to their perceived incapacity to protect online activities from malicious attacks and system outages.⁹⁰ These fears were given justification by the US General Accounting Office which, between September 1998 and July 2000, released several reports highlighting the poor status of information security controls and management procedures in several Federal departments.⁹¹

4.2 European Perceptions of Trust

Like their American counterparts, European Internet users are wary of online interactions. Commissioner David Byrne has emphasised this state of affairs by arguing that:

“While Internet penetration is growing rapidly, all the evidence shows that consumer confidence in the e-commerce medium itself and in cross-border transactions remains low. E-commerce, therefore, is an insignificant part of the final consumption within the European Union - significantly below 1% of total retail sales...We are confronted with what I certainly call the e-confidence barrier.”⁹²

⁸⁹ Susannah Fox (ed.), *The Internet Life Report: Trust and Privacy Online-Why Americans Want to Rewrite the Rules*. Final Findings, August 2000, available at <http://www.pewinternet.org> (visited 20 August 2000). The relationship between trust, confidence and privacy has been already highlighted by various authors. See Esther Dyson, *Release 2.1: A Design for Living in the Digital Age*, (London: Penguin Books, 1998), Tim Berners Lee, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*, (London: HarpersCollins, 1999) and Philip Agre and Marc Rotenberg, *Technology and Privacy: The New Landscape* (London, UK: The MIT Press, 2000)

⁹⁰ Bob Cohen, "New Poll Finds Americans Concerned About Security of Government Computers", *Infosec Outlook*, vol.1 n.7 (September 2000) available at <http://www.ita.org> (visited on 1 February 2001)

⁹¹ US General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets At Risk* (GAO/AIMD-98-92 23 September 1998), *ibid.*, *DOD Information Security: Serious Weaknesses Continue to Plaque Defence Operations At Risks* (GAO/99-107, 26 August 1999) and *ibid.*, *Information Security: Serious and Widespread Weaknesses Persist At Federal Agencies*, (GAO/AIMD-00-295)

⁹² Speech by David Byrne, European Commissioner for Health and Consumer Protection, *The E-Confidence Barrier-New Regulatory Models-Conference on the E-Economy in Europe*, European Parliament, Brussels, 2

This e-confidence barrier seems to be confirmed by the fact that one quarter of regular European Internet users have encountered security problems while transacting online. In certain countries, the percentage has reached 30-35%. Among these users, 15% have been hit by spamming and viruses. An average of 3% have experienced credit card fraud while buying online.⁹³

In certain European countries, the issue of trust and confidence in online environments has been examined in detail. In the UK, the National Consumer Council (NCC) has found that British Internet users are very worried about the possibility of hackers accessing their personal and financial details. Such worries have been sufficient to deter Internet users from engaging in online activities.⁹⁴ In fact, according to data collected by the NCC, only 1 percent of UK consumers believe that the Internet is the safest method of shopping. In contrast, 35% believe that it is the riskiest method to conduct commercial transactions. Meanwhile, in 1999 researchers from the University of Freiburg released the findings of a survey assessing the security and trust concerns of over one thousand German companies. They concluded that online risks were significant for the vast majority of these firms and that:

“the decision whether the Web will be used for electronic commerce is very dependent on adequate levels of technical security especially for integrity and documentation (for verification) of transactions combined with an adequate legal framework.”⁹⁵

4.3 Critical Infrastructures

Trust and confidence are vital if European information infrastructures and the Internet are to be used for online relational exchanges. Trust and confidence are even more important when they involve critical societal functions. One example is telemedicine. The medical profession requires the information infrastructure to be fully functional if they are going to consult with other colleagues online to jointly help patients. This situation becomes especially crucial when diagnostic tests or even surgery are carried out remotely. Dependable systems are essential since uncontained failures may lead to catastrophic consequences such as wrong diagnoses or even deaths.⁹⁶ Similarly, the provision of emergency services, e.g. the dispatch of ambulances, is dependent on information and network technologies. Faults in these areas can have significant safety implications.

Similar concerns have emerged in relation to other socially critical infrastructures such as power and water distribution and financial services. As the European Commission has noted, “there are growing concerns about **national security** as information systems and communication networks have become a critical

March 2001 available at: http://europa.eu.int/comm/dgs/health_consumer/library/speeches/speeches86_en.html (visited on 30 July 2001)

⁹³ E-Europe Eurobarometer, Flash 71, February 2001. Data available at http://www.europe.eu.int/information_society/eeurope/ (visited 30 July 2001)

⁹⁴ National Consumer Council, *E-Commerce and Consumer Protection*, London, August 2000 available at <http://www.ncc.org.uk> (visited on 29 August 2000)

⁹⁵ Detlef Schoder, "Perception of Risk Factors in Electronic Commerce: Empirical Evidence From Germany", in Gunter Muller and Kai Rannenber, *Multilateral Security in Communications: Technology, Infrastructure and Economy* (London: Addison Wesley, 1999), pp.451-459. For an more international overview, see Sirkaa Jarvenpaa and Noam Tractinsky, "Consumer Trust in an Internet Store: A Cross-Cultural Validation", *Journal of Computer Mediated Communication*, vol.5 n.2 (December 1999), available at <http://www.ascusc.org/jcmc/issue2/jarvenpaa.html> (visited on 31 January 2000)

⁹⁶ Marc Wilikens, Tom Jackson, Alberto Sanna, Work Package x: A case study from the Health Care sector (Ispra: JRC, 1999), Issue 2, Draft 4.

factor for other infrastructures (e.g. water and electricity supply) and other markets (e.g. the global finance market).⁹⁷

These concerns have been forcefully expressed by UK Ministers. In February 2001, the Home Secretary told the BBC that “the results of cyber-terrorism, by which people could hack into the control systems of, say, the water supply, the electricity supply, those operating a hospital could be worse even than those caused directly by explosion.”⁹⁸ In March 2001, the Foreign Secretary warned Parliament that “a computer-based attack on the national infrastructure could cripple the nation more quickly than a military strike.”⁹⁹

4.4 The Need for Public Policy

Given the growth in faults, vulnerabilities and threats and the need to ensure trust and confidence if the Information Society is to fulfil its potential, the European Commission has argued that solutions to dependability cannot be left to the market alone:

“there are reasons why actions by governments are required in response to imperfections in the market. Market prices do not always accurately reflect the costs and benefits of investment in improved network security and neither the providers nor users always bear all the consequences of their behaviour....

when operators, suppliers, or service providers improve the security of their products a good deal of the benefits of this investment accrues not only to their customer but to all those directly or indirectly affected by electronic communication-basically the whole economy.”¹⁰⁰

This analysis is supported by a knowledgeable observer from HP Labs who pointed out that:

“The majority of good practice adoption can be expected to occur through economic incentives, as traders find it difficult to attract customers and get business insurance if they do not adopt such practices.

Public policy cannot, however, be left to market pressures alone: some imbalances of market power have serious social consequences if left unchecked. The role of governments ... in establishing minimum legal standards, in recognising and encouraging responsible self- and co-regulation, and in providing the framework for commercial and social acts, extends as far into the "e-world" as it does in the normal one.”¹⁰¹

An insight into the nature of the market failure is provided by Ross Anderson from Cambridge University who uses the principles of network economics to address the reason why design faults and hence security vulnerabilities continue to plague the software industry.¹⁰² Information Technology markets, he argues, embody the following features. First, the value of an IT product or a system is related to how many other

⁹⁷ European Commission, “Network and Information Security: Proposal for a European Policy Approach”

⁹⁸ 25 Feb 2001, BBC News

⁹⁹ Hansard, 29 March 2001

¹⁰⁰ Commission of the European Communities, "Network and Information Security: Proposal for a European Policy Approach" Text released on 6 June 2001 available at http://www.europe.eu.int/information_society/

¹⁰¹ Stefek Zaba, *Confidence in e-commerce: issues and possible resolutions* (Bristol: Hewlett-Packard Laboratories, 2001).

¹⁰² Ross Anderson, "Why Information Security is Hard-An Economic Perspective". Paper available at <http://www.cl.cam.ac.uk/users/rja14/> (visited on 19 July 2001), pp.1-10

users adopt it and/or interact through it. Second, IT systems have very high development and initial costs but very low marginal costs. Consequently, it is necessary to recoup the investment and development costs before such systems become commodities. At the same time, users often face high operational and implementation costs when deciding to switch from one product to another. Therefore, they may refrain from switching unless they are given incentives whose costs are borne by the system developers.

All of these factors lead to a situation of "first winners take all", in a sense that for developers and service providers "it is extremely important to get into markets quickly".¹⁰³ This pressure creates a situation where novelty, difficulty, complexity and lack of assurance are amplified by the need to get systems out as fast as possible to create immediate revenue streams. These demands become even more forceful in times of economic slowdown when competition becomes fiercer.¹⁰⁴ All of these factors may lead to the entry into the market of software and hardware solutions which are not properly tested and evaluated and which contain faults.

Anderson's analysis is echoed by that of Eugene Spafford from Purdue University who argues that there is:

“a myth that is often repeated, namely that industry will find incentives to solve our security problems. To the contrary, it is largely because of industry practices that we currently face such security problems! Industry is concerned with getting products to market as quickly as possible, at the lowest cost. The result is often software with extraneous, poorly designed and poorly tested features. To spend extra time or money on better security is to put the companies at a disadvantage in the marketplace. Instead, many software companies have disclaimed all liability in their licenses, and sought to insulate themselves from adverse reactions and scrutiny of their software... , In the current market that does not offer consumers significant choices, and where there is no liability for faulty products, there is little likelihood that industry players will invest in fundamental research to improve products.”¹⁰⁵

It is also clear that the operators and end-users of information systems are often lax in enforcing security management policies. An important reason for this was highlighted by an October 2000 survey from Cap Gemini Ernst & Young which found that 4% of UK financial services companies cite security as their greatest priority. Some 40% cited competition in the marketplace as their greatest worry.

The poor state of information security management is reflected in survey after survey. In August 1999 the CERT-CC estimated that 99% of all reported intrusions “result through exploitation of known vulnerabilities or configuration errors, [for which] countermeasures were available.”¹⁰⁶

4.5 Conclusion

This section has emphasised how dependable systems and information infrastructures are vital elements for enhancing trust and confidence in online environments. Dependability is essential for establishing

¹⁰³ *ibid.* p. 3

¹⁰⁴ Philippe Collier, "The Astronomical Debt", *Connectis-The Financial Times*, issue 14, August 2001, pp.12-21.

¹⁰⁵ Statement of Eugene H. Spafford, Professor of Computer Science and Director of Purdue University's Center For Education and Research in Information Assurance and Security, House of Representatives Science Committee, 10 October 2001.

¹⁰⁶ <http://www.cert.org/present/cert-overview-trends/index.htm>

relational exchanges over the Internet and other online infrastructures. Dependability is even more crucial to support critical infrastructure services.

Given an evident market failure to provide sufficient levels of dependability, there is therefore a clear societal need to approach dependability-related issues from a public policy perspective. This section has emphasised the importance of using public policy to address both the economic and commercial factors that lead to the development of faults and vulnerabilities and to deal with situations where these faults can lead to failures.

5 Towards European Dependability Policy

This section introduces the global and European policy environment and situates the development of dependability policy within the broader context of the development of the European Information Society.

The need to ensure “trust in cyberspace” and to provide security for networked information systems through enhancing the dependability of information infrastructures has been rising up the global public policy agenda since the 1990s. In the USA, information security has been framed as a national security question since the mid-1990s and the Administration has led efforts to protect critical infrastructures, including information infrastructures, against attack. In Europe, policy-makers became aware in the late 1990s that the development of an Information Society and knowledge economy required dependable information infrastructures. At an international level, governments and businesses have in recent years worked through fora such as the G-8, OECD and Council of Europe to promote cyber-security, counter cyber-crime and promote trust and dependability.

The transformation of this topic from the relatively narrow and specialist field of “information security” into a broad public policy issue during the 1990s was the result of two trends. First, the increased reliance by governments, businesses and citizens on networked information and communication technologies (ICT), notably the Internet. As the business and societal benefits of the exploitation of these technologies became evident, so society became more dependent upon an expected level of service. Second, the parallel growth in “cyber-abuse,” ranging from criminality and vandalism to more serious attacks, and in system outages.

Once it became evident to policy-makers that society could not rely on networked ICT to deliver the expected benefits unless the risks were managed, efforts began to address dependability and Critical Infrastructure Protection as cross-cutting public policy issues. It is in this context that the European Union has initiated efforts to address information security and dependability.

5.1 The European Policy Context

Since the beginning of the 1990s, the European Commission has viewed information and network technologies as essential tools for Europe's economic and social development and growth. In 1993, the Commission's White Paper on *Growth, Competitiveness and Employment* emphasised the need to create a European-wide information infrastructure to sustain economic and commercial growth. The Commission also called for the appropriate regulatory and policy environment to sustain the needs of the Single European market and address the interests of all major stake-holders. In 1997, the Commission introduced the *European Initiative in Electronic Commerce* which was followed by a ministerial conference on Global Information Networks held in Bonn during Germany's presidency of the European Union.

Discussions surrounding these events confirmed the need for a common European regulatory framework but also emphasised the need to enhance overall trust and confidence in information infrastructures.¹⁰⁷ It started to become evident that users' perceptions of trust and confidence in the online environment could be undermined by the increasing number of faults and malicious activities involving the Internet and other

¹⁰⁷ Commission of the European Communities, *A European Initiative in Electronic Commerce*, Comm (97) 157, 15 April, 1997. Information about the ministerial conference can be found at <http://www2.echo.lu/bonn/final.htm> (visited on 14 June 2000).

information and communication media. Stakeholders began to recognise that online malicious activities, system faults and outages risked undermining not only the overall dependability of Europe's information infrastructures but also the growth of the Information Society as a whole.¹⁰⁸

This recognition led to three separate but related activities. First, the Commission started to address the implications of the rising number of cyber-crimes. It first completed a major comparative legal study, *ComCrime*, whose findings were discussed during the European Council summit held in Tampere in October 1999.¹⁰⁹ Here, EU leaders concluded that only common international definitions and sanctions would allow for an effective fight against cyber-crime. Meanwhile, the European Parliament also called for initiatives, with specific attention to aspects of substantive and procedural criminal law. In December 1999, the European Council decided to support the drafting of an international convention by the Council of Europe dealing with substantive and procedural responses to cyber-crime.

At the end of January 2001, the Commission released a communication outlining its overall thinking concerning present and future activities in the areas of cyber-crime. In particular, this document proposed:

“a comprehensive policy initiative in the context of broader Information Society and Freedom, Security and Justice objectives for improving security of information infrastructures and combating cyber-crimes, in accordance with the commitment of the European Union to respect human rights.”¹¹⁰

Second, the Commission has been encouraging research and development activities in the field of information and network security. A number of research projects were sponsored as part of the TEDIS programme, beginning in 1988. The European Trust Service research programme was also initiated, as part of the Fourth Research and Development Framework. Building on these efforts, the Fifth Research and Development Framework considers dependability as a pivotal subject to be investigated through the Information Society Technology (IST) plan. Dependability initiatives were focused in the late 1990s through the Dependability Initiative, discussed below.

The third strand, and the most significant high level effort to implement a coordinated policy, arose from the Lisbon Summit of March 2000, when EU leaders called upon the Commission to draft a comprehensive action plan aimed at making Europe the most competitive and advanced knowledge-based economic area in the world. The eEurope 2002 Action Plan was subsequently introduced. This recognised the importance of promoting trust and confidence. It called, *inter alia*, for actions aimed at

¹⁰⁸ In October 1997, the Commission emphasised this point in its communication discussing the provision of cryptographic services. See: Commission of the European Communities, Ensuring Security and Trust in Electronic Communication: Towards a European Framework for Digital Signatures and Encryption, Com. (97) 503, 8 October 1997. This process eventually led to changes in the circulation and exports of encryption technologies and the provision of digital signature services. See "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures" in Official Journal of the European Communities, vol. 43 no. L13, 19 January, 2000.

¹⁰⁹ The full name of the COMCRIME Study is Legal Aspect of Computer-Related Crimes in the Information Society. Report prepared by Prof. Ulrich Sieber, version 1.1998, available at <http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html> (visited on 24 August 2001). The Conclusion of this European Council are available at http://europa.eu.int/council/off/conclu/oct99/oct99_en.htm (visited on 24 August 2001)

¹¹⁰ Commission of the European Communities, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Cybercrime*, Comm (2000) 890 Final, 26 January 2001.

fostering network and information security, enhancing early warning and information sharing capabilities and improving public-private partnerships. Overall, the Action Plan emphasised the need to ensure the dependability of Europe's information infrastructures to safeguard its socio-political and economic well-being.¹¹¹

In June 2001, the European Commission issued a Communication on Network and Information Security outlining a proposed European policy approach.¹¹² This was revised and on 6 December 2001, the European Council adopted a Resolution on Network and Information Security. This resolution provides the mandate and context for a more comprehensive and overarching approach to dependability policy. The Resolution urges a number of actions on Member States, such as improved user education, and mandates the Commission to examine and propose further initiatives at European level.

The June 2002 Seville Summit reaffirmed the recommendations of this Resolution. The Summit supported proposals for an eEurope 2005 Action Plan, including measures to build a “secure information infrastructure”. Member States approved three actions in particular:¹¹³

- Creation of a Cyber Security Task Force. The aim is for this to become a centre of competence on security questions, to facilitate cross-pillar discussion and to improve trans-border cooperation, possibly including helping to develop a “concept for a European computer attack alert system.”
- Promotion of a “culture of security” in the design and implementation of information and communication products; including actions to raise awareness of security risks.
- To examine the possibilities of establishing a secure communications environment for the exchange of classified government information.

It is important to note that, unlike in the USA, information infrastructure dependability has been treated as an Information Society and, in part, criminal issue. Since the European Union does not have competence in areas affecting national security and defence, Critical Infrastructure Protection has remained a Member State responsibility. Nonetheless, a combination of the growing competencies of European institutions in relation to both Pillar Two (Common Foreign and Security Policy) and Pillar Three (Justice and Home Affairs) activities and the increased European policy focus on large scale terrorist attacks on infrastructures since the 11 September 2001 attacks on New York and Washington, may lead to a realignment of priorities and focus. It is noticeable that the Council Framework decision on combating serious attacks on information systems identifies: “increasing concern at the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States.”¹¹⁴ This language reflects increasing cross-pillar coordination in the context of EU efforts to combat terrorism.

The Dependability Initiative

¹¹¹ The text of the E-Europe Action Plan is available at http://www.europa.eu.int/information_society/eeurope/action_plan/actionplantext/index_en.htm (visited on 24 August 2001).

¹¹² European Commission, “Communication: Network and Information Security: A Proposal for a European Policy Approach”, June 2001

¹¹³ eEurope Action Plan 2005.

¹¹⁴ European Commission, Proposal for a COUNCIL FRAMEWORK DECISION on combating serious attacks against information systems COM (2001), version of 5.10.01

EU activities in the area of dependability have been focused in recent years through the Dependability Initiative (DEPPY).¹¹⁵ As part of the Information Society Technologies research programme, the principal objective of DEPPY is: “to contribute towards raising and assuring trust and confidence in heavily connected systems and services and promoting dependability enabling technologies.”

In order to achieve these objectives, DEPPY has supported three strands of initiatives. First, it has backed fundamental research and development aimed at assessing and managing vulnerabilities within complex and large-scale information and communication infrastructures. It has also examined the implications of embedded systems in critical applications and the requirements for scalability and for diverse operating environments. Second, it has supported industrial research and piloting activities. The goal has been to identify opportunities for new technological solutions, to fill technology gaps and to encourage technology take-up.

Third, DEPPY has fostered international cooperation with non-member states, in particular with the United States. These initiatives result from a recognition that dependability necessitates a global approach. In April 1999, a joint US-EU Workshop of Experts was organised in Venice to prepare an agenda for collaboration between research centres and academic institutions. Several bilateral programmes were introduced such as the Joint Task force on Critical Infrastructure Protection. During IST1999, IST2000 and IST2001, the annual conferences where findings of IST-funded research projects are presented to the general public, representatives from leading US and EU research institutions agreed to enhance cooperation on existing dependability project plans and to improve the interaction among dependability-related research communities.

5.2 The Future Technology and Policy Environment

DDSI's objective is to assist the European Commission to devise policies to enhance the dependability of Europe's information infrastructures. Any such policies need to be set in the context of developments in technology, markets and public policies, both as related to ICT and to the European policy environment as a whole.

5.2.1 Technology & Market Trends

Whilst long-term prediction of the future of ICT and of the market are fraught with uncertainty, there is a degree of consensus around some of the main characteristics of the future ICT environment for which policy-makers must now prepare. Sources include EU IST visions of the FP6 research programme, the Global Internet Project,¹¹⁶ the US National Intelligence Council's conferences on the Information Revolution,¹¹⁷ discussions held at Purdue University's Centre for Education and Research in Information Assurance and Security (CERIAS)¹¹⁸ and forecasting exercises carried out by the Information Assurance Advisory Council.¹¹⁹

¹¹⁵ An inventory of these projects is available at http://deppy.jrc.it/default/show.gx?Object.object_id=KM-----000000000000134 (visited 24 August 2001)

¹¹⁶ Global Internet Project, A Primer On The Security, Privacy and Reliability of the Next Generation Internet (6 November 2000).

¹¹⁷ NIC/RAND, The Global Course of the Information Revolution: Technological Trends (Santa Monica: 2000).

¹¹⁸ Accenture and CERIAS "Security Call for Action" Paper available at http://www.cerias.purdue.edu/previous.php?ndx_ID=4 (visited on 24 August 2001)

¹¹⁹ www.iaac.org.uk

The central factor to take account of is the fact that the “Next Generation Internet” that will form the backbone of the future information environment will provide always on connection through multiple devices embedded in all aspects of business, public and personal life. This will mean that businesses, consumers and governments will depend upon the Internet even more than they do today. The Internet will become as ubiquitous as electricity and will have to be as reliable.¹²⁰

Aspects of this future environment that are of particular significance include: pervasive computing;¹²¹ the emergence of a highly connected Global Information Infrastructure (GII) with converged broadband computing, media, telecommunications capabilities; and greater interconnectivity between traditionally separate infrastructures.

Ubiquity and interconnectivity point to the fact that information and network technologies are becoming more inter-connected, pervasive and more integrated into every aspect of the overall infrastructure and of citizens’ lives. One example is the rapid convergence between telephony services and Internet-related technologies as exemplified by Internet-based telephony, Wireless Application Protocol (WAP)-based services and digital TV. This pervasiveness is only set to increase with the IPv6 protocol, which will provide enough IP numbers to interconnect even household appliances. Organisations will be able to use this increased ubiquity to improve control or monitoring and to reduce costs.

This ubiquity is enhanced by *growing performance capacity* in terms of bandwidth, processing power and storage. Fibre-optic networks and/or satellite transmission are set to bring new and more advanced personal and business services through small devices, such as PDAs, which presently have processing power and storage capabilities matching those of PCs.¹²² Organisations can benefit from this performance increase to improve their operations and foster knowledge management, while getting closer to the needs and requirements of their customers and clients. Organisations can also exploit the potential to increase *mobility* since data and information can be accessed from multiple instruments and sources.

Systems and tools are not only becoming more ubiquitous, powerful and mobile but also increasingly “intelligent” thanks to improved artificial intelligence capabilities. In the near future, these instruments are set to become more independent as they develop their own appreciation of their owners’ needs and requirements. Transactional intelligent agents are an interesting case; this is software that trawls information networks performing actions, i.e. buying a book from an online bookstore, without the direct control of a human actor.

However, these new technologies and the services they make possible carry with them a set of vulnerabilities which may undermine their functionality and the dependability of the other infrastructures dependent upon them. In general, these developments will lead to an increase in dependencies, potential vulnerabilities and potential threats.

¹²⁰ “Computing Power on Tap”, *The Economist*, 23 June 2001

¹²¹ Or, to be more precise, extensive, networked embedded systems.

¹²² Donald Norman, *The Invisible Computer: Why Good Products Can Fail, The Personal Computer is So Complex, and Information Appliances are the Solution* (London, England: The MIT Press, 1998) pp.247-262

5.2.2 European Policy Developments

Since the 1980s, the European Commission has worked to liberalise the European telecommunication market to increase competition. After years of debate, this liberalisation has begun to bring results.¹²³ At the present time, a set of new pan-European information and communication providers are competing to cater for the increasingly sophisticated and demanding European market. More importantly, they are also increasingly becoming the underpinning infrastructures for other elements of Europe's infrastructures, which rely on new information and telecommunication services to provide their services. These other sectors (banking, health care, utilities) are also undergoing significant liberalisation, encouraged by the European Union.

In this phase of technological, business and legislative dynamism, the challenge is to devise policies and regulations to satisfy the interests and concerns of all involved stakeholders. In the EU, this process is complicated by the institutional and geographic development of the Union itself, notably as a result of the establishment of a single market and currency and the admission of further Member States.

Overall, though, it does appear that EU institutions have increasingly moved away from mandatory regulation as a means to influence market and technological developments. Whilst the Commission wishes to intervene to promote economic and social wellbeing, there is increasing use of co-regulation, where all stakeholders have a direct input into the preparation and content of any policy initiatives.¹²⁴

5.3 The Global Context

It is also vital that European policies are developed in the global context. As discussed in the global overview, a number of national governments and international organisations are developing policies, standards, regulations and procedures to promote dependability, network security and counter cyber-crime. European policy needs to be congruent with these approaches so that it can both influence global trends and help to ensure the harmonisation of global approaches at all levels from the technical to the regulatory, legal and policy.

In addition to harmonisation with international governmental approaches, European policies need to take into account the perspectives of the globalised business community and of citizens' movements. Globalised businesses, operating through associations such as the Global Business Dialogue on e-Commerce, and in dependability-related sectors are setting global standards and best practices. Citizen groups, meanwhile, are active in debates over regulation of cyberspace and the appropriate balances between liberty and security. European policy needs to both shape and be shaped by these forces.

¹²³ The provision of telecommunication and information services is presently undergoing changes at the EU level. For more information see <http://www.europe.eu.int/telecommunication>

¹²⁴ The need for co-regulation involving all the stakeholders for online activities has been strongly argued in Brian Kahin and James Keller, *Coordinating the Internet*, (Cambridge, Mass: MIT Press, 1997) and Klaus Grewlich, *Governance in Cyberspace: Access and Public Interest in Global Communications*, (London, Kluwer International Law, 1999)

6 Policy Options

This section discusses means for enhancing dependability and translates these into policy options that could contribute to a roadmap for European policy-makers.

Dependable systems are central to the fostering of online trust and confidence, especially relational exchanges. Dependable systems also permit the migration of critical infrastructure functions into online environments. The dependability of systems and information infrastructures is affected by failures which originate from faults and vulnerabilities and their exploitation by malicious actors. These faults and vulnerabilities are in part a result of market failures.

Dependability-enhancing policies at the European level need to take a comprehensive approach that draws upon the multi-disciplinary understanding of dependability and information assurance developed in multiple research disciplines and different industrial sectors. It is helpful to first review how the dependability and the information assurance communities categorise approaches to enhancing dependability and assurance.

6.1 Approaches to Enhancing Dependability

Dependability can be enhanced through four approaches:

Fault prevention aims at avoiding the presence of faults inside systems and infrastructures. This includes attack prevention, vulnerability prevention and intrusion prevention.¹²⁵ Attack prevention involves social and legal measures. Vulnerability prevention involves system design and specification along with access control and system management, including security management and password policies.¹²⁶ Intrusion prevention involves socio-technical measures such as firewalls and authentication procedures.

Fault tolerance approaches allow systems and infrastructures to withstand the impact of faults and to recover from errors. Contemporary approaches to fault tolerance recognise that many systems in an open environment will be “permanently intruded upon” and therefore have adopted the concept of *intrusion tolerance* which seeks to ensure that a “system provides security guarantees in spite of partially successful attacks.”¹²⁷

When discovered, faults need to be removed. (*Fault removal*). This concept is relevant to vulnerability removal and will include steps such as “verification procedures such as formal proof, model-checking and testing Flaws may then be removed by correcting the code, applying a security patch, withdrawing a given service, changing a password, etc.”¹²⁸

It is also important to forecast faults throughout the life-stages of a system (*Fault forecasting*). In relation to malicious activities, this can be broken down into: **attack forecasting** which involves estimating the “presence, creation and consequences of attacks. This includes intelligence gathering, threat assessment and attack warning.” **Vulnerability forecasting** involves estimating the presence, creation and consequences of vulnerabilities. This includes the gathering of statistics about the current state of

¹²⁵ MAFTIA Conceptual Model and Architecture, pp. 30-31.

¹²⁶ A. Avizienis, J.C. Laprie and Brian Randell, Fundamental Concepts of Dependability, p.7

¹²⁷ MAFTIA Conceptual Model and Architecture, p. 31.

¹²⁸ *Ibid*, p. 34.

knowledge regarding system flaws, and the difficulties that an attacker would have to take advantage of them.”¹²⁹

A useful counterpart to this four stage model is the five stage model commonly used by the information security and assurance community. This comprises:

- Deterrence of threats
- Protection against exploitations
- Detection of attacks
- Reaction to attacks
- Recovery from attacks and failures

6.2 Dependability Policy Development

The threats, vulnerabilities and interdependencies that face Europe are transnational and global. Indeed, in the words of Brian Randell from Newcastle University, the emerging information infrastructure can be seen as a global socio-technological system. Policy responses and governance mechanisms therefore need to be as multi-disciplinary and as transnational as the challenges.

The first requirement, one that DDSI serves, is to provide European policy makers and information infrastructure stakeholders with the opportunity to collaborate in the development of forward-looking and inclusive policies that address the dependability requirements outlined above. Policy makers, users and developers need to be engaged in designing dependability into Europe’s information infrastructures in order to prevent, tolerate, remove and forecast faults.

Given the importance of engaging all stakeholders in policy development, it is not the goal of DDSI to prejudge the most appropriate public policy solutions to the challenge of dependability. As both technology and the market are changing rapidly, it is important not to become locked into one approach. For instance, the current structure of the Internet requires a high degree of user knowledge and responsibility; the policy implication is a need for user education and awareness raising. However, an emerging trend is towards Application Service Providers and Managed Service Providers – the thin client model. This could remove much responsibility for security from the end-user and thereby shift responsibility onto service providers.

Therefore, the aim of DDSI is to provide baseline knowledge and a platform for concerted action. In an information age, which features a liberalised and globalised economy, this approach is the only way to effectively address concerns about dependability since society "is fast changing, less predictable and with a wider set of more actively engaged stakeholders". Mandatory and top-down regulations will not be able to match this dynamic environment. Market-only voluntary regulations are also not producing the desired results.

6.3 The Content of Public Policy

Public policy should be designed to “engineer in” dependability to Europe’s information infrastructures. Public policy needs to deploy a range of instruments ranging from legislation and regulation, through

¹²⁹ Ibid., p. 32.

direct intervention to stimulating further R&D and technology take-up as well as good practice stimulation.

In order to understand the stages at which public policy can assist in promoting dependability, it may be helpful to categorise options according to the following schema. These categories draw on established practice in the dependability and information assurance communities.

6.3.1 Policy Making Mechanisms

Taking into account the principles for policy-making outlined above and having examined good practice on a global basis, the following requirements for policy-making mechanisms emerge:

- *The need for a central policy lead.* Since dependability is a cross-pillar challenge, it may be helpful to adopt the practice of a number of national governments and invest the policy lead in a central office with the ability to coordinate policy across pillars.
- *The need for a strategic approach.* Dependability R&D, cyber-crime and information security are only elements of the systemic risks in question. An integrating strategy could add value to these discrete elements. The EU has experience of adopting integrated, strategic approaches to manage the upside risks of ICT-related socio-technological developments, in the form of the eEurope Action Plan. It may be appropriate to adopt a similarly strategic approach to managing the downside risks of the ICT revolution. Any such strategy should be designed to maximise opportunities for synergy with similar efforts in partners such as the USA, Canada, Australia and Japan and Intergovernmental Organisations.
- *Partnerships among all stakeholders,* but in particular spanning the private and public sectors, are vital to develop appropriate co-regulation and to implement operational solutions across infrastructures which are “joint products”.¹³⁰ Since this is a priority theme of DDSI, this requirement is discussed in more detail at 6.4 below.

6.3.2 Deterrence

This category focuses upon discouraging potential malicious actors from exploiting vulnerabilities (“attack prevention”). Options include:

- *Development of criminal justice mechanisms* to deter cyber-abuse. This involves building on the work of the Council of Europe which has focused upon harmonising substantive criminal law and ensuring effective national and transnational law enforcement and procedural law harmonisation. It also includes exploring options for market-based deterrent solutions such as active defence.
- *Development of educational programmes* to prevent cyber-abuse. Whilst criminal justice focuses upon deterring criminality, educational programmes focus upon forestalling the emergence of criminal tendencies by encouraging ethical and responsible behaviour.
- *Strengthening of deterrent and investigative measures* to counter “high-end” cyber-threats in the context of the struggle against terrorism.

¹³⁰ Marcelo Masera, “European Working Group on Interdependencies and Vulnerabilities in Information Infrastructures” Final Report of a Workshop held in Brussels on March 22-23 2001 available at http://deppy.jrc.it/default/show.gx?Object.object_id=KM-----000000000000002 (visited on 2 August 2001)

- These activities need to be informed by a robust research-based understanding of the motives, intentions and value systems of threat actors in order to craft cost-effective deterrent policies.

6.3.3 Protection

This category focuses upon the protection of systems. It encompasses the concepts of vulnerability prevention and intrusion prevention.¹³¹ The aim of policies in this category should be to prevent vulnerabilities from being injected into information systems, whether at the design or implementation stage, whether by human error or malicious action.

Underpinning policy responses in this category must be a rigorous analysis of the economic and commercial drivers of dependability and insecurity. It would be advisable for policies to be developed that encourage the market to develop solutions to market failures rather than relying on administrative controls. As a starting point, analysis of the market problems identified earlier in this paper would be of assistance. Such analysis could deal with: first, the features of the IT market that permit faults and vulnerabilities to be designed into systems; second, the incentives and disincentives for adoption of good practice in information risk governance by end-users; third, the market forces that are leading critical infrastructures to design out resiliency and “buffering” in the quest for competitive advantage and supply-chain integration.

Based upon this analysis, European policy-makers will want to examine the range of policy instruments available to them to ensure the following:

- *Promotion of more dependable software & system design and implementation.* Efforts are already underway in this area, ranging from research activities to develop more rigorous software engineering processes to the use and improvement of technical standards such as Common Criteria, to the Open Source movement. These activities need to be encouraged and complemented by examination of the policy options for dealing with market challenges such as software liability and the “shrink wrap” license issue.
- *Promotion of corporate and information governance & security management good practice.* European policy is already encouraging adoption of good practice such as ISO17799 but there is considerably more that could be done at European level to promote and implement such standards and to incentivise the adoption of good practice, notably amongst SMEs. Tools that can be used include regulatory, civil & corporate law and insurance-based incentives.
- *Updated and appropriate standards.* Developing standards that keep up with the fast pace of market and technological change is a challenge. Europe needs to engage with international efforts to enhance guidelines and standards to ensure they remain appropriate for new market and technological circumstances. An example is the revision of OECD Information Security Guidelines.
- *Promotion of dependability aware cultures & education encouraging ethical and responsible user behaviour.* The Safer Internet programme has touched on this area but there would be considerable benefit in European action to raise awareness of dependability issues in key communities and to build an ethical foundation amongst the population at large that would prevent intrusions.
- Promotion and exploration of technical and organisational solutions to priority issues, such as authentication and access control. Considerable research has been conducted into, for example, smart cards, but most EU Member States and industry sectors remain uncertain how or whether to

¹³¹ As well as vulnerability removal.

implement comprehensive schemes such as Public Key Infrastructures. At the same time, solutions need to be found to civil liberties and privacy concerns with such technological solutions.

6.3.4 Detection

Detection of faults, failures and malicious activities is a prerequisite for policy-making, operational response and research-based solutions. This category encompasses attack and vulnerability forecasting and metrology as well as information sharing and warning. The key point here is the requirement, expressed in EU policy and by most governmental, inter-governmental and private sector organisations that have engaged in this debate for more and better information on security incidents, vulnerabilities and threats. European-wide action can add considerable value since the challenges are common to all Member States and all industry sectors; many of the solutions will require structures, methods and legal actions that are inherently transnational. There are two priorities:

- *Promotion of warning, alerting & information sharing initiatives.* As a priority theme within DDSI, this requirement is discussed in more detail at 6.5 below.
- *Development of reliable statistical indicators for trend analysis.* This need has been identified by the EU since 1999. Current indicators of threats, vulnerabilities, information risks and the state of dependability, trust and confidence are partial in coverage, often incompatible and suffer from weaknesses in definitions, data collection and presentation.

6.3.5 Risk Management

A risk management approach needs to underpin all efforts to promote dependability. This approach is inherent in the dependability concept of fault and intrusion tolerance and in the information assurance concepts of reaction and recovery. The assumption must be that, even with deterrence, protection and detection in place, faults will occur and failures will result, whether from malicious attack, human error or natural causes. These risks need to be effectively and proportionately managed at all levels from the European-wide to that of the individual citizen. The tools and infrastructures for undertaking this risk management need to be developed, adopted and implemented. Areas in which European action could add particular value include:

- *Encouragement of good practice in business continuity & risk management.* As with information risk governance, this could involve facilitation of the development of appropriate tools in areas not well served by the market, e.g. SMEs and citizens, and employment of a range of policies to encourage take-up. These policies could range from legal mandate to stimulation of consumer demand.
- *Integration of intrusion tolerant architectures into corporate governance & risk management processes.* Emerging intrusion tolerant network architectures provide the technical underpinnings for effective risk management that meet the requirements of senior management for good corporate governance.
- *Development of scaleable risk management methods across interdependent infrastructures.* As Europe's converging infrastructures become more complex, more interdependent and more tightly coupled, it becomes harder for any one sector or Member State to develop the tools, acquire the data or build the constituencies required to undertake effective risk management across these socio-technological systems. Community building efforts such as the EU Working Group on Interdependencies have an important role to play, as do modelling and simulation activities. The goal should be to develop and deploy risk management tools that will ensure all sectors adequately govern their exposure to information risks.

- *Development of uniform criminal codes and law-enforcement procedures* to ensure that individuals or groups who interfere with information systems have a high likelihood of being caught and appropriately punished. Punishment of attackers is a vital element in the reactive process and is currently a weak spot in many jurisdictions.
- *Provision of emergency and consequence management capabilities able to deal with systemic risks on a European-wide basis.* The aim of European policy should be to ensure sufficient measures are in place that any failures of information infrastructures will be of limited societal impact. At the same time however, growing vulnerabilities of interdependent infrastructures and growing threats means that it would be prudent to make provision for recovery and reconstitution activities on a European-wide basis in the event of major failures that cannot be handled by the private sector or Member States. Initiatives such as a European-wide approach to consequence management should therefore be explored.

6.4 Cross-Sectoral Partnerships

As noted above, an important mechanism for policy-making and implementation are partnerships. Partnerships should provide all stakeholders with fora in which to exchange policy and regulatory concerns about dependability and to find solutions to vulnerabilities and threats. These partnerships recognise that modern infrastructures are “joint products” and need novel governance mechanisms. These platforms should foster exchange of information about the nature and complexity of faults, errors and failures. They should also collect and share individual experiences, best practices, management procedures and technical solutions.

The rationale behind the focus upon public-private partnerships is that, just as strategic alliances are now a central feature of the “new economy,” so innovative new partnership arrangements need to be devised to develop and implement dependability policy that bring together states, businesses and other stakeholders. No single model of partnership will be appropriate for every function and for every community.

Several national public-private initiatives have been already launched to deal specifically with issues related to dependability. In some cases, governments have created public structures or offices staffed with civil servants. A second option has been government-owned public-private partnerships, jointly established by private and public sector organisations.¹³²

Several private organisations have also launched initiatives. The leading international examples of high-level public-private partnerships are the Information Assurance Advisory Council in the UK, the Partnership for Critical Infrastructure Security in the USA and Infosurance in Switzerland. In some instances, such as a number of ISACs, the organisation guides the activities of an outsourced service provider.¹³³ In other cases, these private partnerships have been mainly the results of extensions of certain services, which were already part of a company portfolio.¹³⁴

One area of specific interest for public-private collaboration should be to promote, update or even devise dependability-enhancing *standards*. These should be flexible enough to adjust to changing technical and

¹³² An interesting example is ACTION 2000 (A2K), a private company set up by the UK Department of Trade and Industry (DTI). This role of this organisation was to deliver on the Prime Minister Tony Blair's pledge that the UK would suffer “no material disruption” as a result of the Millennium Bug. The authors would like to thank Michael Knights for providing this information.

¹³³ Such as the IT-ISAC in the USA.

¹³⁴ An example is in this regard is the AGORA Group, which is supported by the US company Regence Blue Shield, where members meet to discuss and exchange information and data about dependability-related issues.

business demands. More importantly, they need to reflect the interests and objectives of all stakeholders in order to avoid the emergence of "dead" standards.

6.5 Warning and Information Sharing

In order to enhance dependability, it is necessary to develop European-wide processes and procedures that provide warning and information sharing of vulnerabilities and threats (attacks). Due to the growing interdependence between the information infrastructures and physical infrastructures, this data needs to be shared widely, but in accordance with legal and regulatory rules.

Two major models for information sharing and warning are presently available. First, several industries and countries have established Computer Emergency Response Teams (CERT)/Computer Security Incident Response Teams (CSIRT), which collaborate loosely through fora such as FIRST.¹³⁵ Another model is embodied by Information Sharing and Analysis Centres (ISACs). Encouraged by the United States Government, these are independent institutions to whom private organisations provide, as well as receive, sanitised information about threats and vulnerabilities.¹³⁶ Unlike CERTs, ISACs are based on a subscription business model, which may limit the sharing of information outside paying members. Both models have positive and negative elements, which need to be evaluated.

Importantly, all models of information sharing and warning involve some form of partnership. One of the functions of European policy should be to overcome organisational, sectoral and national "stovepipes" and encourage European-wide information-sharing partnerships. This could be pursued through the activities of the a European Warning and Information System.

6.6 Research & Development

Underpinning all of the above policy areas will be effective and targeted investment in research and development that is multi-disciplinary and combines "blue-skies" research with market-oriented technology take-up activities. The European Commission has already made a strong initial commitment as part of its e-Europe Initiative and the Fifth Research and Development Programme.¹³⁷ The increasing importance of dependability to European and global information infrastructures means that there is a need for R&D to address new sources of faults, vulnerabilities and threats. These R&D investments need to anticipate future technical developments and users' interests and objectives.

R&D policy needs to parallel overall European regulatory and legal developments. It is also important to coordinate these activities with non-member states, in particular the United States and Japan. As part of the EU-USA dialogue, the European Commission has already established cooperation links with the US

¹³⁵ European Commission, "Network and Information Security: Proposal for a European Policy Approach" Draft, 6 June 2001 available at http://www.europa.eu.int/information_society/

¹³⁶ Examples of active ISACs are: FS-ISAC for the US financial sector or the forthcoming IT-ISAC aimed at the US information technology industry.

¹³⁷ For an overview of the past and present dependability research activities sponsored by the European Commission see information in note 6.. For more information about the future R&D directions of the European Commission in the overall area of information society see the ad-hoc website of the DG Information Society at http://europa.eu.int/information_society/programmes/research/index_en.htm (visited in 2 August 2001)

Office of Science & Technology Policy and other leading US academic and research institutions.¹³⁸ Similar activities are being developed with Japanese government agencies and research bodies.

Considerable effort has already been put into generating a vibrant and focused dependability research community in the European Union. It is important to complement this technical work with analysis of the wider policy and societal context. In particular, attention will need to be paid to the utility of a range of policy instruments that can affect market, societal and threat behaviours.

6.7 Conclusion

The December 2001 Council Resolution and the eEurope Action Plan 2005 provide starting points for a strategic approach to information infrastructure dependability.

A logical outcome of the current process would be the development of a policy Roadmap that provides a strategic overview of EU objectives, lays out the structures by which policy should be made and implemented, identifies the steps that are required to enhance dependability and the policy levers that can be used to stimulate market, technical and governmental solutions to these challenges.

This paper has provided a starting point for discussion of such a Roadmap. The intent has been to facilitate further discussion of possible solutions to the pressing challenge of dependability for the Information Society.

¹³⁸ For more information see Marc Wilikens, "US-EU Working Workshop on Dependability held in Helsinki on 21 November, 1999", published on 5 December 1999, available at <http://deppy.jrc.it/> (visited on August 2, 2001). For more information on the dependability research activities of DARPA see <http://www.darpa.mil/ito/research/ftn/index.html> (visited 2 August 2001)

7 Selected Glossary

Attack	A malicious interaction <i>fault</i> aiming to intentionally violate one or more security properties
Authentication	Ability of users to identify their transactional counterparts
Availability	Readiness for use
CERT	Computer Emergency Response Team
CIP/A	Critical Infrastructure Protection/Assurance
Confidentiality	Non-occurrence of unauthorised disclosure of information
CSIRT	Computer Security Incident Response Team
Dependability	That property of a computer system such that reliance can justifiably be placed on the service it delivers
Error	That part of a system state that may lead to a failure
Fault	The cause of an error
Failure	When the delivered service deviates from implementing the system function
IAAC	Information Assurance Advisory Council
Information Assurance	Operations undertaken to protect and defend information and information systems
Integrity	Prevention of unauthorised modification or deletion of data
Intrusion	A malicious, externally-induced, operational fault.
ISAC	Information Sharing & Analysis Centre
Maintainability	The ability to conduct repairs and to introduce evolutions
Non-repudiation	Non-occurrence of the refutation of actions of authenticated users
PCIS	Partnership for Critical Infrastructure Security
Reliability	Service continuity
Risk	The probability of a threat exploiting a vulnerability that could cause harm to an asset resulting in a negative impact.
Safety	Non-occurrence of catastrophic consequences for the environment
Security	Confidentiality, integrity, availability (& authentication and non-repudiation) relative to authorised users
Survivability	The ability of a computer-communication system to satisfy certain critical requirements in the face of adverse conditions.
Trustworthiness	Correctness, reliability, privacy, safety, and survivability

8 Bibliography

Official Documents, Final Project Reports and Speeches

Commission of the European Community (chronological order)

Marc Wilikens-Joint Research Centre, "US-EU Working Workshop on Dependability held in Helsinki on 21 November, 1999", published on 5 December 1999, available at

http://deppy.jrc.it/default/page.gx?_app.page=entity.html&_app.action=entity&_entity.object=KM-----000000000000142&_entity.name=EU-US-WSHelsinki.pdf (visited on August 2, 2001)

Andrea Servida-Joint Research Centre, "European Dependability Initiative: Inventory of EC Funded Projects in the Area of Dependability" Report published on 11 January 2000 and available at

http://deppy.jrc.it/default/page.gx?_app.page=entity.html&_app.action=entity&_entity.object=KM-----000000000000134&_entity.name=Dep-Prj-Inv022.pdf (visited on 2 August 2001)

E-Europe Eurobarometer, Flash 71, February 2001. Data available at

http://www.europa.eu.int/information_society/eeurope/ (visited 30 July 2001)

IDATE, Reference Report 2000 on the Study "Development of Digital Television, Report on behalf of the DG Information Society, February 2001 available at

http://europa.eu.int/information_society/topics/telecoms/regulatory/studies/index_en.htm (visited on 2 August 2001)

"Communication: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime", COM (2000), 890 Final

Speech by David Byrne, European Commission for Health and Consumer Protection, The E-Confidence Barrier-New Regulatory Models-Conference on the E-Economy in Europe, European Parliament, Brussels, 2 March 2001 available at

http://europa.eu.int/comm/dgs/health_consumer/library/speeches/speeches86_en.html (visited on 30 July 2001)

Marcelo Masera, "European Working Group on Interdependencies and Vulnerabilities in Information Infrastructures" Final Report of a Workshop held in Brussels on March 22-23 2001 available at http://deppy.jrc.it/default/show.gx?Object.object_id=KM-----000000000000002 (visited on 2 August 2001)

Squire Sanders and Dempsey, Final Report of the Study for the Development of Competition for Electronic Networks and Services and Inventory of EU Must Carry Regulations, Report on behalf of DG Information Society, April 2001 available at

http://europa.eu.int/information_society/topics/telecoms/regulatory/studies/index_en.htm (visited on 2 August 2001)

"Communication: Network and Information Security: A Proposal for European Policy Approach" (draft), 6 June 2001, available at http://www.europa.eu.int/information_society/

United States

Laura Unger, Online Brokerage: Keeping Apace of Cyberspace, Final Report of a Special Study for the US Stock and Exchanges Commission, November 1999 available at <http://www.sec.gov/news/studies.shtml> (visited on 2 August 2001)

US General Accounting Office, DOD Information Security: Serious Weaknesses Continue to Place Defence Operations At Risks (GAO/99-107, 26 August 1999)

US General Accounting Office, Information Security: Serious and Widespread Weaknesses Persist At Federal Agencies, (GAO/AIMD-00-295)

US General Accounting Office, Information Security: Serious Weaknesses Place Critical Federal Operations and Assets At Risk (GAO/AIMD-98-92 23 September 1998)

Books

Esther Dyson, Release 2.1: A Design for Living in the Digital Age, (London: Penguin Books, 1998)

Tim Berners Lee, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web, (London: HarpersCollins, 1999)

Concerning Privacy: Philip Agre and Marc Rotenberg: Technology and Privacy: The New Landscape (London, UK: The MIT Press, 2000)

Philip Agre and Marc Rotenberg: Technology and Privacy: The New Landscape (London, UK: The MIT Press, 2000)

Ross Anderson, Security Engineering (Chichester, UK: Wiley Computing Publishing, 2001)

Tim Berners Lee, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web, (London: HarpersCollins, 1999)

Withfield Diffie and Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption, (London, The MIT Press, 1999)

Esther Dyson, Release 2.1: A Design for Living in the Digital Age, (London: Penguin Books, 1998)

Peter Keen, Craig Balance, Sally Chan and Steve Schrupp, Electronic Commerce Relationships: Trust By Design (London: Prentice Hall, 2000)

J.C. Laprie (ed.), Dependability: Basic Concepts and Terminology (New York: Springer-Verlag, 1992)

National Research Council, Trust in Cyberspace, (Washington, DC, USA: National Academy Press, 1999)

Peter Neumann, Computer-Related Risks, (Cupertino, CA: Addison Wesley, 1995)

W. Russel Neumann, Lee McKnight and Richard Jay Solomon, The Gordian Knot: Political Gridlock on the Information Highway, (London, UK: The MIT Press, 1998)

Donald Norman, The Invisible Computer: Why Good Products Can Fail, The Personal Computer is So Complex, and Information Appliances are the Solution (London, England: The MIT Press, 1998)

Charles Pfleger, Security in Computing (New Jersey: Addison and Wesley, 1996)

Bruce Schneier, Secrets and Lies: Digital Security in a Networked World, (New York: Wesley Computing Publishing, 2000), pp.220-221

Neil Storey, Safety-Critical Computer Systems, (Harlow, UK: Addison-Wesley, 1996)

Paul Taylor, Hackers: Crime in the Sublime, (London: Routledge, 1999)

Articles, Book Chapters, Papers and Conference Proceedings

Ross Anderson, "Why Information Security is Hard-An Economic Perspective". Paper available at <http://www.cl.cam.ac.uk/users/rja14/> (visited on 19 July 2001)

Ross Anderson and Markus Kuhl, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations" <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf> (visited on 3 October 2001)

John Butler, "Towards Understanding and Measuring Conditions of Trust: An Inventory", Journal of Management, vol.17 no.4 (April 1991)

Christine Norman and Gemral Zaltman, "Factors Affecting Trust in Marketing Research Relationships", Journal of Marketing Research, vol.29 no.2 (August 1992)

Robert Ellison *et alia*, " An Approach to Survivable Systems" Paper available at <http://www.cert.org/research>. (visited on 19 July 2001)

John George, "Do Norms Matter in Marketing Relationship?", Journal of Marketing, vol.55 (April 1992)

Gregory Gundlancy and Patrick Murphy, "Ethical and Legal Foundations for Relationship Marketing Exchanges", Journal of Marketing, vol.56 no.3 (October 1993)

Donna Hoffman, Thomas Novak and Marcos Peralta, 'Building Consumer Trust Online', Communications of the ACM, vol,42 no.2 (April 1999)

Sirkaa Jarvenpaa and Noam Tractinsky, "Consumer Trust in an Internet Store: A Cross-Cultural Validation", Journal of Computer Mediated Communication, vol.5 n.2 (December 1999), available at <http://www.ascuusc.org/jcmc/issue2/jarvenpaa.html> (visited on 31 January 2000)

Erland Jonsson, "An Integrated Framework for Security and Dependability" in Proceedings of the 1998 New Security Paradigm Workshop (New York , ACM Press, 1999)

Kriistina Karvonen, "Creating Trust" in Proceedings of the Fourth Nordic Workshop on Secure IT Systems (NORDSEC 99), held in Krista, Sweden, 1-2 November 1999

J.C. Laprie, "Dependability: A Unifying Concept for Reliable Computing and Fault Tolerance" in T. Anderson (ed.), Dependability of Resilient Computers,(Oxford: BSP Professional Books, 1989)

Ibid., "Dependable Computing and Fault Tolerance: Concept and Terminology", in Proceedings of the 15 IEEE International Symposium on Fault Tolerant Computing, Ann Harbour, MI, USA, June 1985 (IEEE Press, 1986)

Howard Lipson and David Fisher, "Survivability: A New Technical and Business Perspective on Security" in Proceedings of the 1999 New Security Paradigms Workshop, 22-24 September 1999 available at <http://www.cert.org/research/> (visited on 19 July 2001).

Bev Littlewood and Lorenzo Stringini, "Software Reliability and Dependability: A Roadmap", in *ibid.*, Future of Software Engineering (New York: ACM Press, 2000), pp.177-188 (year and published to be confirmed)

H.A.M Luijff et al, "The Vulnerable Internet :A Study of the Critical Infrastructure of (the Dutch Portion) of the Internet", Paper presented at 5th International Conference of Technology Policy and Innovation-DELFT 2001, 26-29 June, 2001, available at <http://www.delft2001.tudelft.nl> (visited on 19 July 2001)

A. Holmagre, "Vulnerability of Complex Infrastructure: Power Systems and Supporting Digital Communication Systems", Paper presented at *ibid*

Robert Morgan and Shelby Hunt, "The Commitment-Trust Theory of Relationship Marketing", Journal of Marketing, vol.58 no.3 (July-September 1994)

David Powell and Robert Stroud (Eds), MAFTIA Conceptual Model and Architecture (November 20 2001), MAFTIA deliverable D2

Magnus Ramage and Keith Bennett, "Maintaining Maintainability" Paper presented at the International Conference on Software Maintenance (ICSM 1998), Washington, DC, USA, 16-20 November 1998

Brian Randell, "Dependability-A Unifying Concept", Paper presented at the workshop Computer Security, Fault Tolerance and Software Assurances: From Needs to Solutions, 1998 available at <http://www.ise.gmu.edu/~csis/conf/fns98/> (visited on 20 July 2001)

Detlef Schoder, "Perception of Risk Factors in Electronic Commerce: Empirical Evidence From Germany", in Gunter Muller and Kai Rannenber, Multilateral Security in Communications: Technology, Infrastructure and Economy (London: Addison Wesley, 1999)

Technical Reports and Surveys

A. Avizienis, J.C. Laprie and Brian Randell, Fundamental Concepts of Dependability, LAAS Technical Report n. 01145, April 2001

Computer Emergency Response Teams/Coordination Centre, CERT/CC Statistics 1988-2001 available at http://www.cert.org/stats/cert_stats.html (visited on 27 July, 2001)

Computer Security Institute, "Financial Losses due to Internet Intrusions, Trade Secret and Other Cyber-crimes soar", March 12, 2001 available at http://www.gocsi.com/prelea_00321.htm (visited on 28 July 2001)

Susannah Fox (ed.), The Internet Life Report: Trust and Privacy Online-Why Americans Want to Rewrite the Rules. Final Findings, August 2000, available at <http://www.pewinternet.org> (visited 20 August 2000)

Nicholas Kyriakopoulos and Mac Wilikens, Dependability and Complexity: Exploring Ideas for Studying Open Systems-Full Report, 15 December, 2000 available at <http://deppy.jrc.it> (visited on 19 July 2001)

Thomas Longstaff, Survivable Network Systems: An Emerging Discipline, Technical Report CMU/SEI-97-TR-013 and ESC-TR-97-013, November 1997 and May 1999

Peter Neuman, Research and Development Initiatives Focused on Preventing, Detecting and Responding to Insider Misuse of Critical Defence Information Systems: Results of a Three-Day Workshop, available at <http://www2.csl.sri.com/insider-misuse/ins.html> (visited on 17 November 2000)

ibid, Practical Architecture for Survivable Systems and Networks-Phase II: Final Report, ARL DAKF 11-97-C-0020, 30 June 2000, available at <http://www.csl.sri.com/neuman/survivability.pdf> (visited on 19 July 2001)

Symantec Antivirus Research Centre, SirCam, _____ Worm, available at <http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html> (visited on 28 July 2001)

Win Van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", Computer and Security, vol. 4 (1985), pp. 269-286

Sultan Weatherspoon, "Overview of IEEE 802.11B Security", Intel Technology Journal, 2nd Quarter 2000 available at http://developer.intel.com/technology/itj/q22000/articles/art_5.htm (visited on 3 October 2001)

Newspapers/Weekly Reports

Bob Cohen, "New Poll Finds Americans Concerned About Security of Government Computers", Infosec Outlook, vol.1 n.7 (September 2000) available at <http://www.itaa.org> (visited on 1 February 2001)

Philippe Collier, "The Astronomical Debt", Connectis-The Financial Times, no. 14, August 2001

Rob Lemos, "Virulent worm calls into doubt our ability to protect the Net" in CNET News Special Report, 27 July 2001, available at http://news.cnet.com/news/0-1003-201-6658647-0.html?tag=tp_pr (visited on 28 July 2001)

Sue Marek, "Not 'Old Reliable' Quite Yet; Wireless Networks Still Experience Delays In SMS Delivery", WirelessWeek, June 18, 2001

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.

