欧州における情報セキュリティ関連調査報告書

2023年 0月

独立行政法人 情報処理推進機構
Study on the Evaluation of IT Security Information Analysis Function in the EU Region

European Initiatives and Programs
European Organizations and Services
National Organizations and Activities

Final Report

January 30th, 2008

Customer:
IT Security Center
IPA/ISEC JAPAN

Contact Persons:
Akira Yamada a-yamada@ipa.go.jp
Wolfgang Schneider wolfgang.schneider@sit.fraunhofer.de
Status of Document

This document is the Final Report of the “Study on the Evaluation of IT Security Information Analysis Function in the EU Region”.

Editors:

Thomas Schroeder  thomas.schroeder@sit.fraunhofer.de
Management Summary

This report presents the results of the “Study on the Evaluation of IT Security Information Analysis Function in the EU Region” performed by SIT on behalf of IPA. The report gives an overview of the current status of IT security measures, strategies, programs and initiatives, and a summary of responsible organizations in the EU region. The description of organizations and activities of various European countries focuses primarily on Germany, and provides some examples from France and the United Kingdom.

This report lists institutions (research or otherwise) of the European Union (EU) and its member states dealing with information technology security and security in general. For each institution structure, area of work, work programme, major projects, and tangible results will be given. In addition, special funding programmes by the EU and its member states will also be listed.

The current situation and required further initiatives regarding IT security information analysis function in the EU region can be summarized and classified by the following aspects:

- EU initiatives and programs,
- EU organizations and activities,
- Specific, national governmental organizations and activities.

Governance and policing are problems immanent in any telecommunication network. However, with the Internet, these problems have become more prevalent for a variety of reasons, such as the ease of cross-border traffic and a false feeling of safety it gives to the user. Dealing with these issues, it is most important that subscribers are properly identified and authenticated by the network provider and that all their actions are thoroughly recorded for eventual future investigations. Network providers in turn are generally considered trustworthy, while some actually may be not, the latter being more likely the case in countries with shady governments.

Especially, the relationship between information security measures taken by the Japanese government (the Ministry of Internal Affairs and Communication) and the National Information Security Center (NISC) compared to those taken by the European Union will be investigated. Attention is paid to what sometimes is called “social engineering”, an electronic version of the confidence man, i.e. “phishing”. (The spelling is deliberate.) By phishing, people are made to give away secrets unintentionally, such as computer passwords, “spear phishing”, like the name would suggest, being a highly targeted way of phishing. Another area of concern,
especially in on-line banking, is called “pharming”, meaning the fraudulent diversion of data packets.

Information Security Management Systems (ISMS) assist enterprises and organisations in handling classified information, be it in a data processing environment or in general. In this context, the British Standards Institution (BSI) developed BS7799. Part 1 gives the guidelines, Part 2 a certification framework. Compliance requires among others that the necessary risk assessment has been undertaken. Part 1 in turn became ISO17799; Part 2 did not make it into the ISO series, which means that there is no certification according to ISO17799. ISO17799 is likely to be revised and published under the ISO/IEC 2700x suite.

Another important area is the security awareness of the public. Political activities akin to “Secure Japan” will be investigated regarding the EU and its members. The management method of “Best Practice” could be applied to IT security. Best Practice is a general idea, which asserts that there is a technique, which tops any other in some crucial aspect. In order to make Best Practice more than a buzzword, one has to investigate what can be done, not what is somebody else doing. Another management method that could be applied to IT security is the PDCA cycle, PDCA standing for plan, do, check, act. PDCA may be looked upon as related to the Japanese “kaizen”.

Education and formal qualification of IT-security personnel will also be touched briefly. Certification is an important aspect in that regard. Literacy in Information and Communication Technology (ICT) should be achieved already at school, be it primary or secondary. ICT-literacy does not only mean knowing how to put things into use, but also means understanding, last not least, the security aspects of ICT. In addition, the broad public has to be informed about security issues induced by computers and the internet in an adequate way, e.g. via the mass media.
# Table of Contents

Table of Contents

List of Tables

Abbreviations and Acronyms

## 1 Introduction

## 2 Terms and Definitions

### 2.1 Introductory Remarks

### 2.2 Information Analysis

### 2.3 Artificial intelligence

### 2.4 Data mining

### 2.5 Metadata

### 2.6 Information Assurance

### 2.7 Information Exchange

## 3 EU Legislation and Policy

### 3.1 History

### 3.2 Strategy for a Secure Information Society in Europe

## 4 EU Initiatives and Programs

### 4.1 Old Initiatives and Programs

### 4.2 Seventh Framework Program

### 4.3 EUREKA Program
5 European Organizations and Services

5.1 European Network Information Security Agency 27
5.2 European Research Area Network 31
5.3 European Commission Joint Research Centre (IPSC, Institute for the Protection and Security of the Citizen) 33
5.4 EU ECRYPT Network 35
5.5 EU-Projects NESSIE and eSTREAM 39
5.6 ESRAB (European Security Research Advisory Board) 40
5.7 Related Publications 48

6 National Organizations and Activities

6.1 France 50
6.1.1 Direction générale de la sécurité extérieure (DGSE, General Directorate for External Security) 50
6.1.2 Direction de la surveillance du territoire 53
6.1.3 Direction centrale des renseignements généraux 54
6.1.4 Business Centers 55
6.2 Germany 56
6.2.1 BSI 56
6.2.2 Bundesnachrichtendienst 58
6.2.3 Militärische Abschirmdienst 59
6.2.4 The Bundesamt für Verfassungsschutz 60
6.2.5 Bundeskriminalamt (BKA, Federal Police Office) 61
6.2.6 Civil Security Research 62
6.2.7 IT Security Activities in the Commercial Sector 63
6.3 United Kingdom 68
6.3.1 MI5 68
6.3.2 Secret Intelligence Service 69
6.3.3 CPNI 70
6.3.4 Dstl Defence Science and Technology Laboratory 78
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.5</td>
<td>CESG</td>
<td>80</td>
</tr>
<tr>
<td>7</td>
<td>Appendix</td>
<td>83</td>
</tr>
<tr>
<td>7.1</td>
<td>Evaluation of EU-projects NESSIE and eSTREAM</td>
<td>83</td>
</tr>
<tr>
<td>8</td>
<td>References</td>
<td>89</td>
</tr>
<tr>
<td>9</td>
<td>Contact Information and Links</td>
<td>91</td>
</tr>
</tbody>
</table>
List of Tables

Table 1: Documents of European Community Legislation 19
Table 2: Documents of European Community Programs and Initiatives 25
Table 3: Further ENISA Related Documents 30
Table 4: Overview of Related Publications 48
Table 5: International Links 91
Table 6: European Links 91
Table 7: Contact Information about European Organizations 94
Table 8: Japanese Links 94
Table 9: French Links 95
Table 10: Contact Information about French Organizations 96
Table 11: German Links 96
Table 12: Contact Information about German Organizations 98
Table 13: United Kingdom Links 99
Table 14: Contact Information about Organizations in the United Kingdom 100
# Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFNOR</td>
<td>Association Française de Normalisation, French Standardization Body</td>
</tr>
<tr>
<td>AIF</td>
<td>Arbeitsgemeinschaft industrieller Forschungsvereinigungen, Federation of Industrial Research Associations, GER</td>
</tr>
<tr>
<td>ARIST</td>
<td>Agences Régionales d'Information Stratégique et Technologique, Regional Agencies for Strategic and Technology Information, FRA</td>
</tr>
<tr>
<td>Beep</td>
<td>Better eEurope Practices</td>
</tr>
<tr>
<td>BITKOM</td>
<td>Bundesverband Informationswirtschaft, Telekommunikation und neue Medien, Association for Information Technology, Telecommunications and New Media, GER</td>
</tr>
<tr>
<td>BMBF</td>
<td>Bundesministerium für Bildung und Forschung, Federal Ministry of Education and Research, GER</td>
</tr>
<tr>
<td>BMI</td>
<td>Bundesministerium des Innern, Federal Ministry of the Interior, GER</td>
</tr>
<tr>
<td>BMWA</td>
<td>Bundesministerium für Wirtschaft und Arbeit, Federal Ministry for Economics and Labor, GER</td>
</tr>
<tr>
<td>BMWi</td>
<td>Bundesministerium für Wirtschaft und Technologie, Federal Ministry of Economics and Technology, GER</td>
</tr>
<tr>
<td>BSI</td>
<td>British Standards Institute, UK</td>
</tr>
<tr>
<td>BSI</td>
<td>Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security, GER</td>
</tr>
<tr>
<td>CA</td>
<td>Certification Authority</td>
</tr>
<tr>
<td>CEISNE</td>
<td>Co-operative European Information Security Network of Expertise</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>CERTA</td>
<td>Centre d'Expertise gouvernemental de Réponse et de Traitemet des Attaquas informatiques, Governmental Expert Center for Responding to and Handling of IT Attacks, FRA</td>
</tr>
<tr>
<td>CESG</td>
<td>Communications Electronics Security Group, UK</td>
</tr>
<tr>
<td>CNI</td>
<td>Critical National Infrastructure, UK</td>
</tr>
<tr>
<td>CNRS</td>
<td>Centre National de la Recherche Scientifique, National Center for Scientific Research, FRA</td>
</tr>
<tr>
<td>CORDIS</td>
<td>Community Research and Development Information Service, EU</td>
</tr>
<tr>
<td>CORNET</td>
<td>Collective Research Network, EU</td>
</tr>
<tr>
<td>CPNI</td>
<td>Centre for the Protection of National Infrastructure, UK</td>
</tr>
<tr>
<td>CSIRT</td>
<td>Computer Security Incident Response Team</td>
</tr>
<tr>
<td>CSR</td>
<td>Corporate Social Responsibility, EU</td>
</tr>
<tr>
<td>DCSSI</td>
<td>Direction Centrale de la Sécurité des Systèmes d'Information, Central Directorate for Information Systems Security, FRA</td>
</tr>
<tr>
<td>DG</td>
<td>Directorate General, EU</td>
</tr>
<tr>
<td>eCIRT</td>
<td>European CIRTs</td>
</tr>
<tr>
<td>EGC</td>
<td>European Government CSIRTs Group</td>
</tr>
<tr>
<td>EIC</td>
<td>Euro Info Centers</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EISPP</td>
<td>European Information Security Promotion Programme</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Network Information Security Agency</td>
</tr>
<tr>
<td>EPC</td>
<td>European Policy Centre</td>
</tr>
<tr>
<td>ESRAB</td>
<td>European Security Research Advisory Board</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EURAB</td>
<td>European Research Advisory Board</td>
</tr>
<tr>
<td>EWS</td>
<td>European Warning and Information System Forum</td>
</tr>
<tr>
<td>FIRST</td>
<td>Forum of Incident Response and Security Teams</td>
</tr>
<tr>
<td>FP7</td>
<td>7th Framework Program, EU</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>IDDEF</td>
<td>Intrusion Detection DEF</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>INRIA</td>
<td>Institut National de Recherche en Informatique et en Automatique, National</td>
</tr>
<tr>
<td>IO SH</td>
<td>Institution of Occupational Safety and Health, UK</td>
</tr>
<tr>
<td>IPA</td>
<td>Information-Technology Promotion Agency, JAP</td>
</tr>
<tr>
<td>IPM</td>
<td>Interactive Policy Making, EU initiative</td>
</tr>
<tr>
<td>IPR</td>
<td>Intellectual Property Rights</td>
</tr>
<tr>
<td>IST</td>
<td>Information Society Technologies, EU</td>
</tr>
<tr>
<td>JPCERT/CC</td>
<td>Japan Computer Emergency Response Team Coordination Center</td>
</tr>
<tr>
<td>JRC</td>
<td>Joint Research Centre, EU</td>
</tr>
<tr>
<td>KA-IT-SI</td>
<td>IT Security Initiative of the Karlsruhe Region (KA-IT-SI)</td>
</tr>
<tr>
<td>LEXSI</td>
<td>Laboratoire d'Expertise en Sécurité Informatique, Laboratory of IT Security Expertise, FRA</td>
</tr>
<tr>
<td>MIN E FI</td>
<td>Ministère de l'Économie, des finances et de l'industrie, Ministry of Economics, Finance and Industry, FRA</td>
</tr>
<tr>
<td>MOD CERT</td>
<td>Ministry of Defense CERT, UK</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Security, EU</td>
</tr>
<tr>
<td>NISCC</td>
<td>National Infrastructure Security Co-ordination Centre, UK</td>
</tr>
<tr>
<td>NSAC</td>
<td>National Security Advice Centre, UK</td>
</tr>
<tr>
<td>NSE</td>
<td>Network Security Information Exchange, UK</td>
</tr>
<tr>
<td>NSSF</td>
<td>National Standardization Strategic Framework, UK</td>
</tr>
<tr>
<td>OJ EU</td>
<td>Official Journal of the European Union</td>
</tr>
<tr>
<td>OSVDB</td>
<td>Open Source Vulnerability Data Base</td>
</tr>
<tr>
<td>PSG</td>
<td>Permanent Stakeholders Group, EU</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>Research &amp; Development, EU</td>
</tr>
<tr>
<td>RTD</td>
<td>Research &amp; Technology Development, EU</td>
</tr>
<tr>
<td>RTIR</td>
<td>Request Tracker for Incident Response, EU</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCSIE</td>
<td>SCADA and Control Systems Information Exchange, UK</td>
</tr>
<tr>
<td>SDN</td>
<td>Secrétariat Général de la Défense Nationale, General Secretary for National Defense, FRA</td>
</tr>
<tr>
<td>SIRIOS</td>
<td>System for Incident Response in Operational Security</td>
</tr>
<tr>
<td>SIT</td>
<td>Fraunhofer Institute for Secure Information Technology</td>
</tr>
<tr>
<td>STD R</td>
<td>Standards and Technical Regulations Directorate, UK</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>TERENA</td>
<td>Trans-European Research and Education Networking Association</td>
</tr>
<tr>
<td>TESTA</td>
<td>Trans-European Services for Telematics between Administrations</td>
</tr>
<tr>
<td>TF-CSIRT</td>
<td>Task Force CSIRT, EU</td>
</tr>
<tr>
<td>TI</td>
<td>Trusted Introducer, EU</td>
</tr>
<tr>
<td>TISP</td>
<td>TeleTrusT Information Security Professional Certificate, GER</td>
</tr>
<tr>
<td>TRANSITS</td>
<td>Training of Network Security Incident Teams Staff</td>
</tr>
<tr>
<td>TSIE</td>
<td>Transport Services Information Exchange, UK</td>
</tr>
<tr>
<td>W ARP</td>
<td>Warning Advise and Reporting Point</td>
</tr>
<tr>
<td>W G-CS</td>
<td>Working Group CERT Services, EU</td>
</tr>
</tbody>
</table>
1 Introduction

This report presents the results of the “Study on the Evaluation of IT Security Information Analysis Function in the EU Region” performed by SIT on behalf of IPA. The report gives an overview of the current status of IT security measures, strategies, programs and initiatives, and a summary of responsible organizations in the EU region. The description of the responsible organizations and activities of various European countries focuses primarily on Germany, and provides some examples from France and the United Kingdom.

This report lists institutions (research or otherwise) of the European Union (EU) and its member states dealing with information technology security and security in general. For each institution, structure, area of work, work programme, major projects, and tangible results will be given. In addition, special funding programmes by the EU and its member states will also be listed.

The current situation and required further initiatives regarding IT security information analysis function in the EU region can be summarized and classified by the following aspects:

- EU initiatives and programs,
- EU organizations and activities,
- Specific national governmental organizations and activities.

CERTs (Computer Emergency Response Teams) play an outstanding role in the field of information security. Their primary field of responsibility is the collection, evaluation, and timely dissemination of information about security breaches that have been brought to their attention by state authorities or other users of information technology. In the beginning, CERTs have been established within universities or research institutions, since the Internet has its roots in the ARPANET, an early research network initiated by the US government (Department of Defence). More recently, CERTs have been established by private industry or as government agencies, although they may have been named more generically “(computer security) incident response teams” (CSIRT). In the US, examples are the CERT/CC (CC for Coordination Centre) of Carnegie Mellon University as opposed to the US-CERT (Computer Emergency Readiness Team) which is part of the National Cyber Security Division of the DHS (Department of Homeland Security). It must not be confused with the CERT (Community Emergency Response Team) attached to FEMA (Federal Emergency Management Agency), also of the DHS. In Japan, there is e.g. JPCERT/CC of the Japanese Internet Community. FIRST (Forum of Incident Response and Security Teams) is an umbrella organisation of all kinds
of CERTs, established in 1990 and now having about 180 members. CSIRTs begin more and more to provide direct services to their customers, like configuration of firewalls and update of virus scan software.

Governance and policing are problems immanent in any telecommunication network. However, with the Internet these, problems have become more prevalent for a variety of reasons, such as the ease of cross-boarder traffic and a false feeling of safety it gives to the user. Dealing with these issues, it is most important that subscribers are properly identified and authenticated by the network provider and that all their actions are thoroughly recorded for eventual future investigations. Network providers in turn are generally considered trustworthy, while some actually may be not, the latter being more likely the case in countries with shady governments.

Pseudonymity, in the Internet, is the possibility to notice whether different transactions have been made by the same user, although every transaction does not contain any personal identity information of the user. Anonymity, in the Internet, is the (practical) impossibility to identify the person that is behind a pseudonym, e.g. an IP-address. Internet anonymity has become a controversial issue, for reasons that anonymity plays an important role in every day life. For instance, we normally do not reveal our identity to shop-keepers (and maybe do not want to) when buying necessaries, provided we pay cash. However, many feel that the one who seeks anonymity has to hide something.

The Information-technology Promotion Agency (IPA) of Japan is interested in the state of information technology security in the European Union as well as in its member and associated states. There are close similarities between the problems of general security and those of information technology security. For the purpose of this report, focus is put on information gathering and analysis in regard to security. This can be done manually, but in light of the sheer amount of information, mostly automated methods will be used in the future. This information, e.g. gained by monitoring of WEB-servers, Internet traffic, or other facilities, is usually set in relation to external risk assessment and a priori threat knowledge. In security parlance, such procedure is often called “data fusion”. Within the ISO Reference Model, these activities are related to the Application Layer. Apparently, Artificial Intelligence (AI), Pattern Recognition, and Data Base techniques are used to some extent in order to detect threats and security breaches. Analysis may be active in the sense that systems under investigation may be put into certain states of interest. In addition to the general importance of IT security, IT security has become a commercial market of its own.

Especially, the relationship between information security measures taken by the Japanese government (the Ministry of the Internal and Communication) and the National Information Security Center (NISC) compared to those taken by the European Union will be investigated. Attention is paid to what is called “social engineering”, an electronic version of the confidence man, i.e. “phishing”. (The
spelling is deliberate.) By phishing, people are made to give away secrets unintentionally, such as computer passwords, "spear phishing", like the name would suggest, being a highly targeted way of phishing. Another area of concern, especially in on-line banking, is called "pharming", meaning the fraudulent diversion of data packets.

Some light will be shed on peer-to-peer networks (P2P) and file-sharing. They are widely used to distribute copyrighted material without authorisation, and are for that reason considered illegal per se by many countries. They also open security breaches, partly because of the use of software from dubious sources, partly because of practical anonymity of the participants in some nets, partly because of false labelling of files. (In the past, this has been made surprisingly obvious by the Japanese network Winny, where the use of private computers by employees for their work played an important role.) The discussion is complicated by the fact that the mere existence of a P2P net can be totally obscured by steganographic techniques (sometimes called “dark nets”). By cryptographic techniques, some security can be added to P2P nets, but misgivings regarding their security remain.

Information Security Management Systems (ISMS) assist enterprises and organisations in handling classified information, be it in a data processing environment or in general. In this context, the British Standards Institution (BSI) developed BS7799. Part 1 gives the guidelines, Part 2 a certification framework. Compliance requires among others that the necessary risk assessment has been undertaken. Part 1 in turn became ISO17799; Part 2 did not make it into the ISO series, which means that there is no certification according to ISO17799. ISO17799 has been revised and published under the ISO/IEC 2700x suite.

What does industry do on its own, to foster security of computer and communication products? In this context, activities of industry associations will also be listed. Last not least, security is also a focus of lobbying activities. Industry may try to stay ahead from activities by politicians and law-makers. In this context, there is some hope that future operating systems will have fewer security problems, when security is considered from the very beginning of the design process on. However, it is obvious that complete security cannot be achieved with a system being of any meaningful use; it even may be theoretically impossible. Another approach is the secure Virtual Machine (secure VM), also known as “sandboxing”. However, the achievable security depends on the restrictiveness, with which the underlying operating system is used and which may not be acceptable to users.

Another important area is the security awareness of the public. Political activities akin to “Secure Japan” will be investigated regarding the EU and its members. The management method of “Best Practice” could be applied to IT security. Best Practice is a general idea, which asserts that there is a technique, which tops any other in some crucial aspect. In order to make Best Practice more than a buzzword, you have to investigate what can be done, not what is somebody else doing. Another management method that could be applied to IT security is the
PDCA cycle, PDCA standing for plan, do, check, act. PDCA may be looked upon as related to the Japanese “KAIZEN”.

The military also relies heavily on information processing and transmission. So, its IT facilities are likely to be targeted by the enemy, and actually have been so in the past. This may be even more the case, if the military uses, for reasons of cost effectiveness, standard equipment and the general Internet.

Digital forensics will play a growing role in the future. Policemen with a solid IT-knowledge become more and more important. The reality of cybercrime, the modus operandi of the cybercriminal, has to be recorded and investigated.

Education and formal qualification of IT-security personnel will also be touched briefly. Certification is an important aspect in that regard. Literacy in Information and Communication Technology (ICT) should be achieved already at school, be it primary or secondary. ICT-literacy does not only mean knowing how to put things into use, but also means understanding, last not least, the security aspects of ICT. In addition, the broad public has to be informed about security issues induced by computers and the Internet in an adequate way, e.g. via the mass media.

The document is structured into chapters on

- initiatives and programs,
- EU organizations and activities, and
- Specific national organizations and activities.

The chapter on “European initiatives and programs” provides an overview of main European support related to and including IT security measures.

The chapter on “European organizations and services” summarizes the main objectives, roles, schemes, and special services of European organizations.

The chapter on “National organizations and activities” provides examples of national organizations in France, Germany, and the United Kingdom, concerned with IT Security Information Analysis.
2 Terms and Definitions

2.1 Introductory Remarks

This is not a complete list of terminology used in this report. Instead, some definitions are given, which the authors think are beneficial to the reader.

2.2 Information Analysis

The Department of Homeland Security of the US was most likely the first to use the term “information analysis” in the context of computer security, making reference to artificial intelligence and database technologies. The Department of Homeland Security, working together with enhanced capabilities in other agencies such as the Federal Bureau of Investigation would make America safer by pulling together information and intelligence from a variety of sources. The Department would fuse and analyze legally accessible information from multiple available sources pertaining to threats to the homeland to provide early warning of potential attacks. This information includes foreign intelligence, law enforcement information, and publicly available information. The Department of Homeland Security would merge the capability to identify and assess current and future threats to the homeland under one roof, map those threats against our current vulnerabilities, issue timely warnings, and immediately take or effect appropriate preventive and protective action. The Department and the Bureau would ensure cooperation by instituting standard operating procedures to ensure the free and secure flow of information and exchanging personnel as appropriate. Because of the central importance of this mission, the Department would build excellence in its threat analysis and warning function, not only in terms of personnel, but also in terms of technological capabilities. The Department would develop and harness the best modeling, simulation, and analytic tools.

The nation’s information and telecommunications systems are directly connected to many other critical infrastructure sectors, including banking and finance, energy, and transportation. The consequences of an attack on the cyber infrastructure can cascade across many sectors, causing widespread disruption of essential services, damaging our economy, and imperiling public safety. The speed, virulence, and maliciousness of cyber attacks have increased dramatically in recent years. Accordingly, the Department of Homeland Security would place an especially high priority on protecting our cyber infrastructure from attack by unifying and focusing the key cyber security activities performed by the Critical Infrastructure Assurance Office (currently part of the Department of Commerce) and the National Infrastructure Protection Center (FBI). The Department would augment
those capabilities with the response functions of the Federal Computer Incident Response Center (General Services Administration). Because our information and telecommunications sectors are increasingly interconnected, the Department would also assume the functions and assets of the National Communications System (Department of Defense), which coordinates emergency preparedness for the telecommunications sector.

2.3 Artificial Intelligence

Traditionally, the term is defined as "the science and engineering of making intelligent machines". The more modern definition is "the study and design of intelligent agents" where an intelligent agent is a system that perceives its environment and takes actions which maximizes its chances of success. Artificial Intelligence (AI) has been adopted throughout the technology industry, e.g. logistics, data mining, medical diagnosis and many other areas.

Expert systems were one of the earliest types of AI system. They are built around automated inference engines including forward reasoning and backwards reasoning. Many expert systems are organized collections of if-then such statements, called productions. These can include stochastic elements, producing intrinsic variation, or rely on variation produced in response to a dynamic environment. Based on certain conditions ("if"), the system infers certain consequences ("then").

Classifiers make use of pattern recognition for condition matching. In many cases, this does not imply absolute, but rather the closest match. The most widely used classifiers are the neural network, support vector machine, k-nearest neighbour algorithm, Gaussian mixture model, naive Bayes classifier, and decision tree.

Epistemology, the study of knowledge, also makes contact with AI, as engineers find themselves debating similar questions to philosophers about how best to represent and use knowledge and information (e.g., semantic networks).

2.4 Data mining

Data mining is the principle of sorting through large amounts of data and picking out relevant information. It can be defined as "the nontrivial extraction of implicit, previously unknown, and potentially useful information from data" or as "the science of extracting useful information from large data sets or databases". It is widely used by business intelligence organizations, and financial analysts, but it is increasingly used in the sciences to extract information from the enormous data
sets generated by modern experimental and observational methods. It has been suggested that both the Central Intelligence Agency and their Canadian counterparts, Canadian Security Intelligence Service, have put this method of interpreting data to work for them as well, although they have not said how.

Metadata, or data about a given data set, are often expressed in a condensed data mine-able format, or one that facilitates the practice of data mining. Common examples include executive summaries and scientific abstracts.

Data mining identifies trends within data that go beyond simple analysis. Through the use of sophisticated algorithms, users have the ability to identify key attributes of business processes and target opportunities.

The term data mining is often used to apply to the two separate processes of knowledge discovery and prediction. Knowledge discovery provides explicit information that has a readable form and can be understood by a user. Forecasting, or predictive modelling, provides predictions of future events and may be transparent and readable in some approaches (e.g. rule based systems) and opaque in others such as neural networks. Moreover, some data mining systems such as neural networks are inherently geared towards prediction and pattern recognition, rather than knowledge discovery.

A key defining factor for true data mining is that the application itself is performing some real analysis. In almost all cases, this analysis is guided by some degree of user interaction, but it must provide the user some insights that are not readily apparent through simple slicing and dicing. Applications that are not to some degree self-guiding are performing data analysis not data mining.

Although the term “data mining” is usually used in relation to analysis of data, like artificial intelligence, it is an umbrella term with varied meanings in a wide range of contexts. Unlike data analysis, data mining is not based or focused on an existing model which is to be tested or whose parameters are to be optimized.

In statistical analysis where there is no underlying theoretical model, data mining is often approximated via stepwise regression. With the advent of parallel computing, it became possible (when the number of variables is less than approximately 40) to examine all models. This procedure is called all subsets or exhaustive regression. Essentially, data mining gives information that would not be available otherwise. It must be properly interpreted to be useful. When the data collected involves individual people, there are many questions concerning privacy, legality, and ethics.
2.5 Metadata

Metadata is data about data. An item of metadata may describe an individual datum, or content item, or a collection of data including multiple content items. Metadata is used to facilitate the understanding, use and management of data. The metadata required for effective data management varies with the type of data and context of use. In the context of a camera, where the data is the photographic image, metadata would typically include the date the photograph was taken and details of the camera settings. In the context of an information system, where the data is the content of the computer files, metadata about an individual data item would typically include the name of the field and its length. Metadata about a collection of data items, a computer file, might typically include the name of the file, the type of file and the name of the data administrator. The hierarchy of data, metadata, meta-metadata etc. can go on forever. Metadata is a set of optional structured descriptions that are publicly available to explicitly assist in locating objects. The focal purpose of metadata is to find ‘objects", "entities" or ‘resources'. When structured into a hierarchical arrangement, metadata is more properly called an ontology or schema. Metadata helps to bridge the semantic gap. By telling a computer how data items are related and how these relations can be evaluated automatically, it becomes possible to process even more complex filter and search operations. Application and file system metadata derived from electronic documents and files can be important evidence. Metadata is subjective and depends on context. All of this metadata can be interesting to one party or another — such as the spectators, sponsors or a counterterrorist unit of the police — and even for a simple resource the amount of possible metadata can be gigantic.

2.6 Information Assurance

There is little information that exists that will not at one time or another be stored or transmitted electronically. Information on paper, as soon as it is faxed or input into a computer, enters the electronic world. From here the information can be changed, deleted or broadcast to the world. Electronic information must be readily available when needed and trusted to be accurate. Sometimes there are confidentiality concerns. Ensuring the confidentiality, availability and integrity of all electronically held information is the goal. "Information Assurance" is the term used to describe this goal.

2.7 Information Exchange

In the context of Information Assurance, the mechanism, called Information Exchange, is based upon the personal trust of representatives, sharing information in a confidential meeting, which may be a virtual one. Trust is built up slowly; representatives at Information Exchanges are expected to attend all meetings,
which are held every two months. Meeting face-to-face, we are building up a trusted, relatively small community with a common interest. Each organisation can put forward a maximum of two representatives, and cannot send substitutes to attend; a stranger turning up at a meeting would inhibit the sharing of sensitive information.
3 EU Legislation and Policy

This chapter provides an overview of European legislation and policy initiatives.

3.1 History

The European Union (EU) is a political body made up of 27 (at the time of writing) member states, all of which are located in Europe. The institutions of the EU are primarily the European Commission, the Council of the European Union (not to be confused with the European Council and the Council of Europe), and the European Parliament. For short, the Commission is the executive government; the Council and the Parliament form the legislature. As far as we are concerned here, the Commission controls most of the research agencies attached to the EU; the Council is responsible for the monitory funding aspects of research programmes of the EU. The legal instruments of the EU are, in the order of decreasing obligation to the member states: regulations, directives, decisions, recommendations, and opinions.

The EU strives for unison in foreign and security policy. Most of the military aspects have been transferred to NATO, although the European Defence Agency (EDA) located in Brussels has been established in 2004. Co-ordination between the two is in the responsibility of the High Representative for the Common Foreign and Security Policy (CFSP). Among the members of the EU, there is an effective police and judicial co-operation in criminal matters and home affairs. Between the EU and its member states, the share of responsibility is ruled by the principle of subsidiarity; meaning that the member states act on their own whenever appropriate (Treaty of Maastricht). Standardisation of devices and procedures throughout the EU is also of prime concern. It has been laid in the hands of CEN (Comité Européen de Normalisation) and CENELEC (Comité Européen de Normalisation Electrotechnique).

3.2 Strategy for a Secure Information Society in Europe

In its resolution on a "Strategy for a Secure Information Society in Europe [ER 2007/C68/01]" the Council of the EU has explicitly mentioned the importance of IT security. Although a number of awareness raising campaigns have already been taken place both at national and EU-level, there is still much work to be done in this field, especially concerning the end-users. Particular consideration should be given to users that have special needs or have low awareness of network and information security issues. All stakeholders should be aware that
they are part of the global security chain and should be empowered to act as such; network and information security issues should be taken into account in all education and training relating to Information and Communication Technologies (ICT). A European wide awareness raising day called “Information and Network Security DayQ has been planned for 2008 to be conducted on an annual and voluntary basis in each member state.

The Communication “i2010 – A European Information Society for growth and employment”, highlighted the importance of network and information security for the creation of a single European information space. The purpose of the present Communication is to revitalise the European Commission strategy set out in 2001 in the Communication “Network and Information Security: proposal for a European Policy approach”. It reviews the current state of threats to the security of the Information Society and determines what additional steps should be taken to improve network and information security (NIS).

Drawing on the experience acquired by Member States and at European Community level, the ambition is to further develop a dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnership and empowerment. In tackling security challenges for the Information Society, the European Community has developed a three-pronged approach embracing: specific network and information security measures, the regulatory framework for electronic communications (which includes privacy and data protection issues), and the fight against cybercrime. Although these three aspects can, to a certain extent, be developed separately, the numerous interdependencies call for a coordinated strategy. This Communication sets out the strategy and provides the framework to carry forward and refine a coherent approach to NIS.

The 2001 Communication defines NIS 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”. Over recent years, the European Community has implemented a number of actions to improve NIS. The regulatory framework for electronic communications, the review of which is underway, includes security-related provisions. In particular, the Directive on Privacy and Electronic Communications contains an obligation for providers of publicly available electronic communications services to safeguard the security of their services. Provisions against spam and spyware are laid down.

Trust and security also play an important part in the European Community programmes devoted to research and development. The 6th Research Framework Programme addresses these issues through a wide range of projects. Security-related research is to be reinforced in the 7th Framework Programme with the establishment of a European Security Research Programme (ESRP).
Furthermore, the “Safer Internet Plus” programme supports networking projects and the exchange of best practices to combat harmful content circulating on information networks. As a part of its response to security threats, the European Community decided in 2004 to create the European Network and Information Security Agency (ENISA). ENISA contributes to the development of a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations throughout the European Union (EU). The EU also plays an active role in the international forums addressing these topics, such as the OECD, the Council of Europe or the UN. At the World Summit on the Information Society in Tunis, the EU strongly supported the discussions on the availability, reliability and security of networks and information. The Tunis Agenda, which together with the Tunis Commitment sets out further steps for the policy debate on the global Information Society as endorsed by the world’s leaders, highlights the need to continue the fight against cybercrime and spam while ensuring the protection of privacy and freedom of expression. It identifies the need for a common understanding of the issues of Internet security and for further cooperation to facilitate the collection and dissemination of security-related information and the exchange of good practice among all stakeholders on measures to combat security threats.

Despite the efforts at international, European and national level, security continues to pose challenging problems. Firstly, attacks on information systems are increasingly motivated by profit rather than by the desire to create disruption for its own sake. Data are illegally mined, increasingly without the user’s knowledge, while the number of variants (and the rate of evolution) of malware is increasing rapidly. Spam is a good example of this evolution: it is becoming a vehicle for viruses and fraudulent and criminal activities, such as spyware, phishing and other forms of malware. Its widespread distribution increasingly relies on botnets, i.e. compromised servers and PCs used as relays without the knowledge of their owners. The increasing deployment of mobile devices (including 3G mobile phones, portable videogames, etc.) and mobile-based network services will pose new challenges, as IP-based services develop rapidly. These could eventually prove to be a more common route for attacks than via personal computers since the latter ones already deploy a significant level of security. Indeed, all new forms of communication platforms and information systems inevitably provide new windows of opportunity for malicious attacks.

Another significant development is the advent of “ambient intelligence”, in which intelligent devices supported by computing and networking technology will become ubiquitous (e.g. through RFID, IPv6 and sensor networks). A totally interconnected and networked everyday life promises significant opportunities. However, it will also create additional security and privacy-related risks. While common platforms and applications contribute positively to interoperability and the take-up of Information and Communication Technologies (ICTs), they can also increase risks. For example, the greater the use of “off-the-shelf” software, the
greater the impact when vulnerabilities are exploited or failures occur. The emergence of certain “monocultures” in software platforms and applications can greatly facilitate the growth and spread of security threats such as malware and viruses. Diversity, openness and interoperability are integral components of security and should be promoted.

The relevance of the ICT sector for the European economy and for European society as a whole is incontestable. ICT is a critical component of innovation and is responsible for nearly 40% of productivity growth. In addition, this highly innovative sector is responsible for more than a quarter of the total European R&D effort and plays a key role in the creation of economic growth and jobs throughout the economy. More and more Europeans live in a truly information-based society where the use of ICT has rapidly accelerated as a core function of human social and economic interaction. According to Eurostat, in 2004 89% of EU enterprises actively used the Internet and around 50% of consumers had recently used the Internet.

A breach in NIS can generate an impact that transcends the economic dimension. Indeed, there is a general concern that security problems may lead to user discouragement and lower take-up of ICT, whereas availability, reliability and security are a prerequisite for guaranteeing fundamental rights on-line. In addition, because of increased connectivity between networks, other critical infrastructures (like transport, energy, etc.) are also becoming more and more dependent on the integrity of their respective information systems.

Both business and citizens in Europe still underestimate the risks. This is for various reasons, but the most important seems to be, in the case of enterprises, the poor visibility of the return on investment in security and, in the case of citizens, the fact that they are not aware of their responsibility in the global security chain. Indeed, given the ubiquity of ICT and information systems, network and information security is a challenge for everybody:

- Public administrations need to address the security of their systems, not just to protect public sector information, but also to serve as an example of best practice for other players;
- Enterprises need to address NIS more as an asset and an element of competitive advantage than as a “negative cost”;
- Individual users need to understand that their home systems are critical for the overall “security chain”.

In order to successfully tackle the problems described above, all stakeholders need reliable data on information security incidents and trends. However, reliable and comprehensive data on such incidents are difficult to obtain for many reasons,
ranging from the rapidity with which security events can happen to the unwillingness of some organisations to disclose and publicise security breaches. Nonetheless, one of the cornerstones in developing a culture of security is improving our knowledge of the problem.

It is important that awareness programmes, designed to highlight security threats, do not undermine the trust and confidence of consumers and users by focusing only on negative aspects of security. Wherever possible, therefore, NIS should be presented as a virtue and an opportunity rather than as a liability and a cost. It needs to be viewed as an asset in building trust and consumer confidence, a competitive advantage for enterprises operating information systems, and a service quality issue for both public and private sector service providers.

The key challenge for policy makers is to achieve a holistic approach. This approach must recognise the respective roles of the various stakeholders. It must ensure proper coordination of the range of public policy and regulatory provisions that impact either directly or indirectly on NIS. The processes of liberalisation, deregulation and convergence have produced multiplicity of players among the various stakeholder groups, which does not make this task easier. The contribution of ENISA to this goal can be important. ENISA could serve as a centre for information sharing, cooperation amongst all stakeholders, and the exchange of commendable practices, both within Europe and with the rest of the world, in order to contribute to the competitiveness of our ICT industries and a well-functioning internal market.

A secure information society must be based on enhanced NIS and a widespread culture of security. To this end, the European Commission proposes a dynamic and integrated approach that involves all stakeholders and is based on dialogue, partnership and empowerment. Given the complementary roles of public and private sectors in creating a culture of security, policy initiatives in this field must be based on an open and inclusive multi-stakeholder dialogue.

This approach, and its associated actions, will complement and enrich the Commission’s plan to continue the development of a comprehensive and dynamic policy framework through a number of initiatives in 2006:

(1) Addressing the evolution of spam and threats, like spyware and other forms of malware, in a Communication on these specific issues.

(2) Making proposals for improving cooperation between law enforcement authorities and addressing new forms of criminal activity that exploit the Internet and undermine the operation of critical infrastructures. This will be the subject of a specific Communication on cybercrime.
These policy initiatives also complement the activity being planned to achieve the goals of the Commission’s Green Paper on the European Programme for Critical Infrastructure Protection (EPCIP), developed in response to a request by the December 2004 Council. The Green Paper process is likely to lead to an action plan combining an overall “umbrella” approach to critical infrastructure protection with the necessary sector-specific policies, including one for the ICT sector. The sector-specific policy for the ICT sector would examine, via a multistakeholder dialogue, the relevant economic, business and societal drivers with a view to enhancing the security and the resilience of networks and information systems.

Moreover, the 2006 review of the regulatory framework for electronic communications will also consider elements to improve NIS, such as technical and organisational measures to be taken by service providers, provisions dealing with the notification of security breaches, and specific remedies and penalties regarding breaches of obligations. It is largely up to the private sector to deliver solutions, services and security products to end-users. It is therefore of strategic importance that European industry be both a demanding user of security products and services as well as a competitive supplier of NIS products and services.

National governments need to be able to identify and implement best practice in policymaking, as well as demonstrate commitment to these policy objectives by managing their own information systems in a secure manner. Public authorities, in Member States and at EU level, have a key role to play in properly informing users to enable them to contribute to their own security and safety. Raising awareness on NIS issues and providing appropriate and timely information via dedicated e-security web portals on threats, risks and alerts as well as on best practices should be priorities. To this end, examining the feasibility of creating a European multilingual information sharing and alert system, which would build upon and link together existing or planned national public and private initiatives, could be a major goal for ENISA.

The global dimension of network and information security challenges the Commission, both at international level and in coordination with Member States, to increase its efforts to promote global cooperation on NIS, notably in implementing the agenda adopted at the World Summit on the Information Society (WSIS) in November 2005. Lastly, research and development, notably at EU level, will help develop new and innovative partnerships to boost the growth of the European ICT industry at large, and the European ICT security industry in particular. The Commission will therefore seek to ensure that appropriate financial resources are allocated to research on NIS and dependability technologies under the 7th EU Framework Programmes.

As a first step to enhancing dialogue between public authorities, the Commission proposes initiating an exercise to benchmark national NIS-related policies,
including specific security policies for the public sector. This exercise will help identify the most effective practices, so that they can then be deployed wherever possible on a broader basis throughout the EU and help make public administrations a driver of best practice in security. The work on electronic identification, for example as part of the recent eGovernment Action Plan, could play an important role in that respect.

A structured multi-stakeholder debate on how best to exploit existing tools and regulatory instruments to attain an appropriate societal balance between security and the protection of fundamental rights, including privacy, is needed. The planned Conference “i2010 – Towards a Ubiquitous European Information Society” being organised by the forthcoming Finnish Presidency, and the consultation on the security and privacy implications of RFID, which is part of the broader consultation recently launched by the Commission, will contribute to this debate. In addition, the Commission will organise:

- A business event to stimulate industry commitment to adopting effective approaches to implement a culture of security in industry.
- A seminar reflecting on ways to raise security awareness and strengthen the trust of end-users in the use of electronic networks and information systems.

Effective policy making needs a clear understanding of the nature and extent of the challenges. This calls for not only reliable and up-to-date statistical and economic data both on information security incidents and levels of consumer and user confidence, but also up-to-date data on the size and trends of the ICT security industry in Europe. The Commission intends to ask ENISA to develop a trusted partnership with Member States and stakeholders to develop an appropriate data collection framework, including the procedures and mechanisms to collect and analyse EU-wide data on security incidents and consumer confidence. In parallel, because of the highly fragmented market in the EU and its rather specific nature, the Commission will invite Member States, the private sector and the research community to establish a strategic partnership to ensure the availability of data on the ICT security industry and on the evolving market trends for products and services in the EU.

In order to improve the European capability to respond to network security threats, the Commission will ask ENISA to examine the feasibility of a European information sharing and alert system to facilitate effective responses to existing and emerging threats to electronic networks. A requirement of such system will be a multilingual EU portal to provide tailored information on threats, risks and alerts.

The empowerment of each stakeholder group is a prerequisite to foster awareness of security needs and risks in order to promote NIS.
In this respect the Commission invites Member States to:

- Proactively participate in the proposed benchmarking exercise of national NIS policies;
- Promote, in close cooperation with ENISA, awareness campaigns on the virtues, benefits and rewards of adopting effective security technologies, practices and behaviour;
- Leverage the roll-out of e-government services to communicate and promote good security practices that could then be extended to other sectors;
- Stimulate the development of network and information security programmes as part of higher education curricula.

The Commission also invites private sector stakeholders to take initiatives to develop an appropriate definition of responsibilities for software producers and Internet service providers in relation to the provision of adequate and auditable levels of security. Here, support for standardised processes that would meet commonly agreed security standards and best practice rules is needed.

- Promote diversity, openness, interoperability, usability and competition as key drivers for security as well as stimulate the deployment of security-enhancing products, processes and services to prevent and fight ID theft and other privacy intrusive attacks.
- Disseminate good security practices for network operators and service providers as baseline levels for security and business continuity.
- Promote training programmes in the business sector to provide employees with the knowledge and skills necessary to effectively implement security practices.
- Work towards affordable security certification schemes for products, processes and services that will address EU-specific needs (in particular with respect to privacy).
- Involve the insurance sector in developing appropriate risk management tools and methods to tackle ICT-related risks and foster a culture of risk management in organisations and business.

Identifying and meeting security challenges in relation to information systems and networks in the EU requires the full commitment of all stakeholders. The policy approach outlined in this Communication seeks to achieve this by reinforcing a
multi-stakeholder approach. This would build on mutual interests, identify respective roles and develop a dynamic framework to promote effective public policy-making and private sector initiatives. The Commission will report to Council and Parliament in the middle of 2007 on launched activities, the initial findings and the state of play of individual initiatives, including those of ENISA and those taken at Member State level and in the private sector. If appropriate, the Commission will propose a Recommendation on network and information security (NIS).
Table 1: Documents of European Community Legislation

<table>
<thead>
<tr>
<th>DOCUMENT ID/TYPE</th>
<th>DATE</th>
<th>PURPOSE OF DOCUMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference</td>
<td>2007-05-03</td>
<td>Responsible Entrepreneurship Exchange, Brussels</td>
</tr>
<tr>
<td>News</td>
<td>2007-04-02</td>
<td>Enterprise and Industry Directorate-General: European Innovation</td>
</tr>
<tr>
<td>News</td>
<td>2007-03-30</td>
<td>Education - Promoting entrepreneurial mindsets</td>
</tr>
<tr>
<td>News</td>
<td>2007-03-15</td>
<td>Policy makers focus on craft and small enterprises</td>
</tr>
<tr>
<td>Speech</td>
<td>2007-03-15</td>
<td>José Manuel Durão Barroso, President of the European Commission: Reform to perform: how to boost business in Europe</td>
</tr>
<tr>
<td>Speech</td>
<td>2007-03-15</td>
<td>Vice-President, Commissioner G. Verheugen: Corporate Social Responsibility, Innovation and Competitiveness</td>
</tr>
<tr>
<td>Publication</td>
<td>2007-01-01</td>
<td>Summaries of European Legislation Related to Information Society</td>
</tr>
<tr>
<td>Opinion</td>
<td>2006/2138</td>
<td>Committee on Culture and Education for the Committee on Industry, Research and Energy on Time to move up a gear - Creating a Europe of entrepreneurship and growth</td>
</tr>
<tr>
<td>Speech</td>
<td>2006-06-07</td>
<td>Vice-President, Commissioner G. Verheugen: Launch of the ICT Task Force</td>
</tr>
<tr>
<td>Communication</td>
<td>COM/2006/251</td>
<td>From Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: A Strategy for a Secure Information Society - &quot;Dialogue, Partnership and Empowerment&quot;</td>
</tr>
<tr>
<td>DOCUMENT ID/TYPE</td>
<td>DATE</td>
<td>PURPOSE OF DOCUMENT</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Communication</td>
<td>2005-06-01</td>
<td>Communication from the Commission of 1 June 2005 to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - “i2010 - A European Information Society for growth and employment”</td>
</tr>
<tr>
<td>EC Communication</td>
<td>2003</td>
<td>“Green Paper on Entrepreneurship in Europe”</td>
</tr>
<tr>
<td>96/280/EC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4 EU Initiatives and Programs

This chapter provides an overview of European initiatives and programs related to IT security measures. Implementing research programmes is an obligation of the EU (Amsterdam Treaty). In order to co-ordinate its activities and make its long-term strategies, also in monetary regard, known to the scientific public, the EU issues research framework programmes in regular time intervals. The following issues and main programs are covered:

- enhanced competitiveness and co-operation through ICT,
- Go Digital program,
- sixth framework program,
- Beep program,
- seventh framework program,
- aeronautics research program,
- capacities program,
- competitiveness and innovation program,
- grants program,
- EURO STARS-EUREKA program,
- EU gateway to Japan program.

4.1 Old Initiatives and Programs


EISPP has already been discussed in section 3.2 of the study on “Current Status of Software Vulnerability Handling Scheme in the EU Region” [IPA 07-2].

The Sixth Framework Programme (FP6) lasted from 2002 to 2006. The main goal of FP6 was to have a structuring effect on research and technological development in Europe, and to make a significant contribution to the establishment of the European Research Area and innovation.

The “Better eEurope Practices” (Beep) project has been funded within the IST Programme (see link: http://www.cordis.lu/ist/). Within Beep, different services have been realized that are provided by the Beep knowledge system (see link: http://www.beepknowledgesystem.org). Beep provides free access to a good practice knowledge system of cases for guidance or for research purposes and to
learning resources describing the use of Information and Communication Technology (ICT). At its web page, Beep provides public deliverables, a research glossary, details of partners, etc. The Beep project has been completed under FP6 (2001-2003).

4.2 Seventh Framework Program

Within the Seventh Framework Programme for Research and Technology Development, which covers the time period from 2007 to 2013 (FP7 is the first framework programme to run for seven years), the thematic area ICT (Information and Communication Technologies) is organized in seven so-called challenges; one of those is titled “Pervasive and Trusted Network and Service Infrastructure”. The European Union believes that within the next ten years, a converged communication and service infrastructure will replace the current Internet, mobile, fixed, and audiovisual networks, serving a large variety of nomadic devices. In spite of its envisaged tenfold complexity and an overall design not fully known from the beginning, system security must not be compromised, although some of the system components (devices, software components) may initially be insecure. In consequence, strategies and technologies enabling mastery of complexity, dependability, and behavioural stability have to be provided. Once a year, calls for proposal are issued for each thematic area. The calls follow so-called objectives, which are subdivisions of the challenges. There are also “joint calls” where more than one thematic area is involved, like ICT and SEC (Security); the latter will be shortly described in the following paragraph.

The European Parliament has made a decision concerning the FP7 of the EU for research, technological development and demonstration activities under which some part of FP6 will also be further funded. FP7 is based on the following four main programs:

- **COOPERATION**: 60% of total budget with the strong ambition to promote the European science and technology areas by research activities carried out jointly between research organizations and enterprises in trans-national cooperation. Within FP7 the industry will play a strong role in defining industry-relevant topics for EU research support. The EC is working closely with industry through technology platforms, which bring together all stakeholders in a specific sector under the leadership of industry.
- **IDEAS**: 14% of total budget to foster competition and excellence in frontier or fundamental research,
- **PEOPLE**: 9% of total budget to enhance the mobility and career development of researchers together with industry by provision of support for longer term cooperation programs between academia and industrial organizations, and
- **CAPACITIES**: 8% of total budget to ensure scientific and technological capacity-building, e.g. in the area of infrastructures or in helping new member states to gear up their scientific potential. An average increase of 54% in current prices
in the budget for cooperative and collective research has been foreseen for the specific benefit.

Security research in FP7 will have a budget of 1.35 billion € for 2007-2013. FP7 will support research to protect Europeans from threats such as terrorism, natural disasters and crime. Priorities will be security of citizens; security of infrastructure and utilities; intelligent surveillance and border security; restoring security and safety in case of crisis; security systems; and social aspects. More information on the project is provided at the link: www.eu-sec.org.

The objectives of the FP7 security program (budget: 80.3 million €) include the following activities:

- development of technologies and knowledge needed to ensure the security of citizens from threats such as terrorism and crime, natural disasters and industrial accidents;
- ensuring optimal and concerted use of available and evolving technologies to the benefit of civil European security, and;
- stimulating the cooperation of providers and users for civil security solutions; improving the competitiveness of the European security industry and delivering mission-oriented results to reduce security gaps.


Within FP7 there is another Thematic Area of interest regarding this report: “Security” (No. 10). This Thematic Area is clearly of civilian nature, although it raises the issue of classification and clearance. The tasks in this Thematic Area are more of fundamental nature and oriented towards general methods and models, rather than concrete implementation and policies, which is the realm of the framework programme on “Security and Safeguarding Liberties”, which is outside FP7. Interoperability between security agencies, often an ICT issue, is on top of the agenda of Thematic Area 10. For the current Calls for Proposal, two demonstration areas have been chosen as examples of what can be accomplished in the security field by computer technology; those being “Security of Infrastructure and Utilities” and “Surveillance and Border Security”. Railway has been chosen as an exemplary field of application for the first Call. Hardening of signals against electromagnetic interference, automatic recognition of foreign items on the track, driver identification, and luggage security are sub-items of interest mentioned explicitly. The European Commission is fully aware of the fact that there is a lack of homogenization in this area among the members of the EU. The Joint Call between ICT and SEC briefly mentioned above deals with “System Integration, Interconnectivity, and Interoperability”. The focal subject of this Joint Call is the software-supported establishment of secure ad-hoc digital radio networks. The calls for proposal also state the per annum monetary frame.
The framework programme on “Security and Safeguarding Liberties” mentioned earlier deals with the more societal aspects of security. It covers the time span from 2007 to 2013, just as FP7 does. It is under the responsibility of the Directorate-General of Justice and Home Affairs. Ethical and legal problems are covered. Of prime concern is the trade-off between security on the one side, and privacy and social cohesion on the other, especially in light of prevention, preparedness, and consequence management (related to terrorism and organised crime). Thus the EU has set the conditions, also financially, to prevent, detect, investigate, and prosecute all sorts of crime effectively, especially under cross-border aspects.

The continued industrial relevance of the themes and the continued participation of industry will be ensured by relying, among other sources, on the work of the various “European Technology Platforms” (ETP). This specific program and the contributions made by the industry shall contribute to the implementation of relevant strategic research agendas established and developed by the ETP. ETP with possible participation of regional research driven clusters can facilitate and organize the participation of the industry in research projects under FP7.

4.3 EUREKA Program

EUREKA, often abbreviated as “E!” is a pan-European research and development funding and coordination organisation. EUREKA aims to coordinate efforts of governments and commercial companies. It does not partake in, for example, military research. EUREKA was established with the “Paris Declaration” of July 17, 1985, and its principles are based on the later Hannover Declaration, subscribed by Ministers on November 6, 1985.

At the time of writing (October 2007), EUREKA has 38 full members, including the European Union, represented by the European Commission. Among the 38 members, all the present 25 EU Member States are also members of EUREKA (the last EU Member State of the EU to join EUREKA was Malta, in June 2006). The Russian Federation joined in 1993.

Contrary to what many seemingly believe EUREKA is not an EU research programme, but rather an inter-governmental initiative, of which the EU is a member. However, a large cooperation and synergy is sought between EUREKA and the research activities of the EU proper, notably with the EU Framework Programme for Research and Development. It enables industry and research institutes from 37 member countries and the EU to collaborate in a bottom-up approach to develop and exploit innovative technologies. More information about EUREKA may be found at the link: http://www.eurostars-eureka.eu.
4.4 SHARE

SHARE is an EU project under the auspices of the European Commission. It has begun under the sixth framework programme. It deals with the mobile support for rescue services, integrating multiple modes of interaction. To some extent, the project covers the problems related to the robustness of the electronic support system.

An overview of further programs and initiatives of the EU is provided in Table 2.

Table 2: Documents of European Community Programs and Initiatives

<table>
<thead>
<tr>
<th>DOCUMENT ID</th>
<th>DATE</th>
<th>PURPOSE OF DOCUMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cordis News FP7</td>
<td>2007-01</td>
<td>The 7th Framework Programme <a href="http://www.cordis.lu/fp7/">http://www.cordis.lu/fp7/</a></td>
</tr>
<tr>
<td>DOCUMENT ID</td>
<td>DATE</td>
<td>PURPOSE OF DOCUMENT</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EC Observatory Report</td>
<td>2003-08</td>
<td>Highlights from the 2003 Observatory</td>
</tr>
<tr>
<td>EC Communication COM (2000) 890</td>
<td>2000-06</td>
<td>Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime <a href="http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi%21celexplus%21prod%21DociNumber&amp;lg=en&amp;type_doc=COMfinal&amp;an_doc=2000&amp;nu_doc=890">link</a></td>
</tr>
</tbody>
</table>
5 European Organizations and Services

This chapter provides an overview of European organizations and services related to IT security measures including:

- European Network Information Security Agency,
- European Research Area Network,
- European Commission Joint Research Centre,
- EU Encrypt Network
- EU-Projects NESSIE and eStream
- ESRAB.

5.1 European Network Information Security Agency (ENISA)

The agency was established in 2004 by the EU, while it is open for non-member countries for participation. It is located in Heraklion, Greece. At the time of writing, it has a staff of about 50, the annual budget being about 6 million Euros. Essential for the understanding of the work of ENISA is what they call a “culture of network and information security”. In its day to day work, ENISA assists the Commission of the EU in the preparation of “cyber law” legislation. A further field of interest is the evaluation and management of risks concerned to IT security. This work is, among others, of value for the insurance industry, in providing novel products related to IT security. Especially, wholesale insurance companies want the risks offered to them by retail insurance companies to be evaluated by independent institutions.

ENISA’s latest activities were focused on the setting-up of and cooperation between Computer Security Incident Response Teams (CSIRTs). CSIRTs are distinguished by the sector for which they provide their services. Examples of European CSIRTs are Cert-IST (France), CERT-Verbund (Germany), or Mcert (Germany) that also have been discussed in [IPA 07-2].

ENISA next steps will first analyze the need for security services of specific categories of users, home users, or governmental bodies. In this context ENISA will assess which type of service provider, e.g., CSIRT or WARP, can best offer these security services. The main objective will be to identify potential gaps and to provide recommendations in order to improve the coverage of these users by European service providers. Current and future activities of ENISA are fixed in its “Work Program 2007” including the following main tasks:

- contribution to improve the general level of electronic communication systems security,
• identification of existing technical, organizational, and cultural barriers in the area of ICT security,
• deepening the inventory of risk management methods and exploring their interrelation with business continuity and business governance based on 2006 results,
  – real life examples of the usage and implementation of a limited number of RM/RA methods,
  – extension of the inventory of risk assessment and risk management methods to include risks affecting operational continuity as a contribution to Business Continuity Planning (BCP), and
  – special attention of risk assessment and risk management methods,
• addressing of possible approaches to integrate IT-risk management with existing corporate governance frameworks and standards such as Basel II, or Sarbanes-Oxley,
• coping with the comparability of different risk management methods and the feasibility of fully integrating risk assessment and risk management processes into the overall business processes,
• production of recommendations for creating incentives for relevant ICT actors to remove any barriers,
• encouragement of the European information security community in order to realize compatible and interoperable authentication levels,
• mapping of the different national or industry-specific methods,
• establishment of an eID directory that provides an overview of actors relevant to electronic identity management in Europe,
• integration of these activities in the EC roadmap 2006-2010 for eID development handled by the e-Government group of the EC,
• continuation of support for the setting up of suitable facilities like CSIRTs or W ARPs in the member states, including facilitating trainings and identifying relevant partners based on the “Step-by-Step Approach on how to Set-up a CSIRT” that has been developed last year,
• analysis of the role of cooperation among CERT/CSIRT teams in the process of enhancing the effectiveness of combating threats, vulnerabilities and security incidents,
• collection of best practices for the quality assurance for CERTs and research of good practices for efficient and successful operation of response teams,
• assuring an adequate level of quality of service by means of advanced training for staff and for management, audits, standardization to support information sharing, evaluation by the constituency, and certification in order to enhance the general level of European CERTs performance,

Resulting from discussions between ENISA and its stakeholders, the following four main areas have been identified to structure the content of ENISA activities for the period 2006 until 2010:
• “raising awareness and building confidence” by the development of end user-oriented activities,
• “facilitating the working of the Internal Market for e-Communication”,
• “mastering emerging technologies and services”, and,
• “bridging security gaps in Europe”.

The following activities have been foreseen for the “raising awareness and building confidence” end-user-oriented area:

• identifying, gathering and promoting methods, material and procedures that increase the understanding and trust of users in electronic communication,
• performing awareness raising campaigns,
• professional and product certificates, labels, security seals and other tools that provide evidence of an adequate level of security in the use of ICT systems.

The following activities have been foreseen for the “facilitating the working of the Internal Market for e-Communication” business-oriented area:

• provision of an independent view on the barriers to the fair working and development of the internal market related to network and information security issues,
• analysis, proposal and promotion of the most appropriate solutions to reduce such obstacles in terms of methods and procedures and of incentive policies at EU and national level,
• guaranteeing the integrity and robustness of the European e-Communication systems,
• provision of best conditions of usage to European users, and the,
• discussion with the stakeholders concerning the sharing of responsibilities.

The following activities have been foreseen for the “mastering emerging technologies and services” technology-oriented area:

• assessment of the impact that emerging technologies and services may have on security and privacy and to advice on ways to control it,
• use of an interdisciplinary approach including economic and social factors, and,
• strengthening the R&D capacity in Europe and to foster its position as a competitive supplier in products and services for network and information security.

The following activities have been foreseen for the “bridging security gaps in Europe” policy-oriented area:

• development of European network and information security policies,
• set up of a wide partnership to collect and process data on threats, vulnerabilities, incidents and damages,
investigation of the best ways to close gaps between user expectation and security service providers, and the lack of interoperability between European security services,
- identification of best practices for quality assurance for security services,
- provision of methods to assess the impact of security policies,
- provision of valuable material to help responsible authorities to adequately define their specific IT security policies, justify the investment and control the evolution of the network and information security level in their environment.

The EC has recently asked ENISA to examine potential models for a European-wide warning system. In its newsletter ENISA Quarterly 03-07, ENISA states that first results will be presented to the member states under the project “European Information Sharing and Alert System (EISAS)”. The focus of this project is on monitoring and early warning systems for the Internet by examining a variety of initiatives targeted at warning network operators and users of security risks initiatives. In this context ENISA was also asked to analyze the current state of affairs in the public and private sectors and to identify possible sources of security information that can potentially contribute to EISAS. The main goal of such a system would be to raise awareness on Network and Information Security (NIS) issues. Currently the Executive Director of ENISA has launched a call for membership of a new Permanent Stakeholders’ Group (PSG) of ENISA. Recently a new website to tackle emerging risks has been launched (for details see link: www.enisa.europa.eu/rmra).

In addition, ENISA together with ITU has opened and maintains an Internet portal about security standards in the area of networking and information, using the IDABC network of the EU. ENISA also publishes a periodical, the ENISA Quarterly.

For 2008 an EU program will be defined to remove network and information security-related barriers in the internal market. This program will mainly address regulatory, technical and operational fields with required actions to be implemented at the national and local levels. It will also provide advices for a better risk management integration at the enterprise level. A list of further ENISA related documents is provided in Table 3.

Table 3: Further ENISA Related Documents

<table>
<thead>
<tr>
<th>ORGANIZATION</th>
<th>DATE</th>
<th>PURPOSE OF DOCUMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENISA</td>
<td>2007-05-24</td>
<td>Influence of cooperation on CERTs services improvement</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.enisa.europa.eu/cert_cooperation/pages/07_02.htm">http://www.enisa.europa.eu/cert_cooperation/pages/07_02.htm</a></td>
</tr>
<tr>
<td>ENISA</td>
<td>2007-02</td>
<td>Study on the “Collection and Dissemination of Information related to Emerging Risks in the area of Information Technology”</td>
</tr>
</tbody>
</table>
### European Research Area Network

The ERA-NET scheme with a budget of €148 million for the period 2003-2005 represented the principal means for FP6 to support the cooperation and coordination of research activities carried out at national or regional level. The scheme has been financed as part of the specific program "Integrating and strengthening the European Research Area". The objective of the ERA-NET scheme, in the context of the European Research Area (ERA), has been to increase the cooperation and coordination of research activities carried out at national or regional level in the member and associated states by means of the networking of research activities, and the development and implementation of joint activities. The research activities carried out at national or regional level have been full research and innovation programs. Details on the ERA-NET scheme can be found at the link: [http://cordis.europa.eu/coordination/era-net.htm](http://cordis.europa.eu/coordination/era-net.htm).

The objective of the ERA-NET scheme is to increase the cooperation and coordination of research activities carried out at national or regional level in the member states and associated states by:
• networking of research activities conducted at national or regional level, and,
• mutual opening of national and regional research programs.

Both networking and mutual opening require a progressive approach. The ERA-NET scheme therefore has a long-term perspective that must also allow for the different way that research is organized in different EU countries.

These actions will use two main tools: the ERA-NET scheme and the participation of the Community in jointly implemented national research programs (Treaty Article 169). The action will also be used to enhance the complementarily and synergy between FP7 and activities carried out under inter-governmental structures such as EUREKA and COST. A previous background document Coordination of National Research Programs on the coordination of national research programs stated the FP7 proposals will aim at consolidating these results and pushing the coordination to a higher level. ERA-NET will aim to strengthen the coordination of national and regional research in two ways:

• providing a framework for actors implementing public research programs to improve coordination through new ERA-NETs and broadening and deepening existing ERA-NETs, and,
• providing additional EU financial support to participants who create a common fund for the purpose of joint calls for proposals among national and regional programs called ERA-NET PLUS.

The DG Research of the EC is funding the EU-SEC project within the framework of the ERA-NET program. EU-SEC will actively support and improve the coordination of the research activities on security during major events of ten European countries by carrying out a networking activity among national research programs.

EU-SEC goes beyond the concept of 'platform of discussion' used by UNICRI at the global level and answers the demand of an expanded European Research Area by elaborating a common methodology for research coordination among its partners. The implementation of such a methodology will allow the partners to optimize the use of available resources and avoid duplication of efforts. The contents of the project are structured in the following main categories:

• systematic exchange of information and best practices in order to describe the state of the art of national research programs on security,
• strategic analysis of complementarities, gaps and barriers that hinder an effective cooperation in research within the European area, and the,
• development of joint activities devoted to elaborate common research strategies and methodologies.
Security research is now a thematic priority in FP7 and will have a budget of 1.35 billion € for 2007 until 2013. FP7 will support research to protect Europe from threats such as terrorism, natural disasters and crime. Priorities will be security of citizens, security of infrastructure and utilities, intelligent surveillance and border security, restoring security and safety in case of crisis; security systems; and social aspects. For more information on the project see link: www.eu-sec.org.

5.3 European Commission Joint Research Centre (IPSC, Institute for the Protection and Security of the Citizen)

IPSC is one of the seven institutes of the Joint Research Centre (JRC) of the European Commission. The JRC has the rank of a directorate-general. IPSC is located at Ispra, Italy. It provides research support to the EU so as to protect the citizen against risks (of technological kind, among others). One of the research areas of IPSC is the vulnerability of IT equipment. In this context, advanced analytical techniques are used for intelligence (information) gathering, such as web and data mining.

The Joint Research Centre is a research based policy support organisation and an integral part of the European Commission. The Joint Research Centre provides scientific advice and technical know-how to support EU policies. Its status as a Commission service, which guarantees its independence from private or national interests, is crucial for pursuing its mission. Its institutes carry out extensive research of direct concern to European citizens and industry. Over the years, the JRC has developed special skills and unique tools to provide autonomous and Europe-wide expertise to improve understanding of the links between technology, the economy and society. Its work is split between institutional research in support of Commission policymaking, direct support for specific Directorates-General (DGs) and competitive activities in strategic relationships with the scientific and business communities. Its guideline is that of ‘adding value’ where appropriate, rather than competing directly with establishments in the EU Member States. Its structure is based on seven specialised Institutes. It employs about 2700 staff (Dec 2006) and uses a budget of over 300 million Euro per year stemming from the European Commission’s research budget and from competitive income. The research programmes are decided by the Council of the European Union and funded by the EU budget with additional funding from associated countries.

The JRC multi-annual work programme, running from 2007 to 2013, focuses on clearly defined themes, reflecting a coherent approach to user needs. Five policy themes have been identified to build on JRC strengths under the EU Seventh Framework Programme (FP7) for research and technological development. Thematic concerns include:

- Food safety to ensure quality systems in the food chain;
• Biotechnology - with a focus on genetically modified organism (GMO) detection, measurements and safety concerns;
• Chemicals - particularly through the European Centre for Validation of Alternative Methods (ECVAM) and the European Chemical Bureau (ECB);
• Health - with a focus on ensuring safety, quality and reliability of medical devices and biological systems as well as the relationship between environment and health;
• Environment - including climate change, sustainability and biodiversity as well as the prediction, assessment and mitigation of natural disasters;
• Nuclear energy - including the safety of power plants and nuclear waste, nuclear safeguards and non-proliferation control techniques;
• Competitiveness and innovation and information society technologies; and,
• Internal and external security, antifraud and development aid.

Cross-sectional activities range from diverse technology foresight exercises - in particular, within an enlarged EU - and reference materials for applications such as faster BSE identification to tackling major issues in cyber security and industrial risks. The Joint Research Centre provides services directly in support of EU legislation and policy through several laboratories such as the European Laboratory for Air Pollution (ERLAP), the European Chemicals Bureau (ECB) and the Major Accident Hazards Bureau (MAHB). The JRC also has an important role to play in the establishment of the European Research Area (ERA), in particular through the ERAWATCH service. The mission of IPSC, multidisciplinary analysis of industrial, socio-technical and environmental systems, innovative application of information and communication technologies, science and technology for safety management, is to provide research-based, systems-oriented support to EU policies so as to protect the citizen against economic and technological risk. The Institute also continues to maintain and develop its expertise in information, communication, space and engineering technologies in support of its mission.

IPSC provides scientific and technical support to EU external relations and security related policies, particularly in the areas of global security & stability, border management, fight against terrorism and crime, as well as in nuclear, transport and energy security. For this purpose, IPSC applies its expertise and competencies in nuclear safeguards/non-proliferation, open source and geo-spatial intelligence and analysis, information technologies as well as systems engineering and analysis. IPSC works in support of risk prevention and management, notably in the fields of the industrial accidents (Seveso II Directive), the vulnerability assessment of buildings and IT infrastructure, the risk assessment of landslides and avalanches.

IPSC applies its expertise in space and IT technologies (including intelligence gathering and advanced analytical techniques) to enhance the EU’s capacity in compliance monitoring and to detect and monitor fraud against the EU budget in several fields including agriculture, fisheries, customs, and external assistance.
Moreover, IPSC performs quantitative econometric analysis in support to competitiveness and growth, with emphasis on financial services, macro-economic modelling, business cycles analysis, and the development and assessment of statistical indicators. IPSC provides also tools for the assurance of scientific information quality. In order to help safeguard EU citizens against damage caused by natural disasters, human activities or criminal fraud, IPSC maintains and develops expertise in technologies relating to information and communication, space, and engineering. The Institute's scientific and technical services cover the full cycle from the conception of a new policy, through support in its development and implementation, to the monitoring and evaluation of eventual results. Added benefit derives from the ability to call on the expertise of network partners and collaborating research establishments throughout the EU.

Through its strong competencies in key technologies such as satellite images analysis, web/data mining and nuclear and sensor technologies, the IPSC address the following broad research themes in support to EU policies:

- Support to external Security
- Agriculture and Fisheries
- Hazard Assessment
- European Laboratory for Structural Assessment
- Traceability and Vulnerability Assessment
- Nuclear Safeguards
- Econometric and Statistical Support to Antifraud
- Sensors, Radar technologies and Cyber security

5.4 EU ECRYPT Network

ECRYPT (European Network of Excellence for Cryptology) is a four year European research initiative, which started in 2004. It has the following areas of interest: information security, cryptology, and digital watermarking.

ECRYPT - European Network of Excellence for Cryptology is a 4-year network of excellence funded within the Information Societies Technology (IST) Programme of the European Commission's Sixth Framework Programme (FP6) under contract number IST-2002-507932. It falls under the action line towards a global dependability and security framework. ECRYPT was launched on February 1st, 2004. Its objective is to intensify the collaboration of European researchers in information security and more in particular in cryptology and digital watermarking.

Cryptology is the science that studies mathematical techniques in order to provide secrecy, authenticity and related properties for digital information. Watermarking allows embedding hidden information into the digital media, such that the watermark is imperceptible and difficult to remove. Cryptology and watermarking are interdisciplinary research areas with a high strategic impact for European
industry and for the society as a whole. They are a fundamental enabler for security, privacy and dependability in the Information Society for digital asset management. The ECRYPT research roadmap is motivated by the changing environment (evolving towards ambient intelligence) and threat models in which cryptology is deployed, by the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based, by the need of strong foundations in the watermarking area and by the requirements of new applications and cryptographic implementations. The main objective of ECRYPT is to ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas. In order to reach this goal, 32 leading players integrate their research capabilities within five virtual labs focused on the following core research areas: symmetric key algorithms (STVL), public key algorithms (AZTEC), protocols (PROVILAB), secure and efficient implementations (VAMPIRE), and watermarking (WAVILA). Essential integration activities include joint workshops, exchange of researchers and students, development of common tools and benchmarks and a website and forum which will be a focal point for the network and the wider cryptographic community. Spreading activities will include a training program, a substantial contribution towards standardization, bodies and an active publication policy. The project team has the critical mass and breadth to address the key questions in these areas.

The general objectives of the ECRYPT network of excellence are the following:

- Maintain and strengthen the excellence of European research and industry in the areas of cryptology and watermarking and obtain a durable integration which lasts beyond the funding of the NoE provided by the European Commission. This is achieved by E-integration: web portal, forum, email lists, Workshops for collecting requirements from all relevant players, building consensus on an integrated research roadmap, scientific presentations and interactions (brainstorming sessions), Exchange visits of researchers and PhD students, and Developing a joint infrastructure.

- Strengthen and integrate research in cryptology and watermarking in Europe and decrease fragmentation by creating a research infrastructure and by organising research into virtual laboratories thereby establishing a joint research agenda and executing joint research in these areas. The Virtual Labs foster joint research between the ECRYPT members; each Virtual Lab has several working groups; this substructure will be refocused or renewed on a regular basis. The network will be organised to ensure that Virtual Labs cooperate closely towards achieving common goals.

- Improve the state of the art in practice and theory of cryptology and watermarking: Improve our understanding of existing algorithms and protocols, expand the theoretical foundations of cryptology and watermarking, and develop better cryptographic algorithms, protocols...
and implementations in the following respects: high performance, low cost, high security.

- Develop a joint infrastructure which includes: tools for the evaluation of cryptographic algorithms, a benchmarking environment for cryptographic hardware and software, infrastructure for side channel analysis measurements and tools, tools for benchmarking watermarking schemes.

The activities of the ECRYPT Network of Excellence are organized into five virtual laboratories established as follows:

1. Symmetric techniques virtual lab (STVL)
2. Asymmetric techniques virtual lab (AZTEC)
3. Protocols virtual lab (PROVILAB)
4. Secure and efficient implementations virtual lab (VAMPIRE), and
5. Watermarking and perceptual hashing virtual lab (WAVILA).

Each virtual lab within the ECRYPT Network of Excellence aims to promote and facilitate cryptographic research on a pan-European level.

The primary technical objective of the STVL is to facilitate European research on both the design and analysis of symmetric cryptosystems. In this way it is hoped that the work in the STVL will address some pressing issues for academia and industry alike. Thus, three particular areas of research have been identified within the scope of the STVL and it is intended that an exchange of ideas from both academia and industry will help the cryptographic community make substantial progress in these areas. The first target for the efforts of the STVL is the development of secure and efficient stream ciphers; a task that will require considerable input from industry and academia alike. A second target for the STVL is a coordinated cryptanalytic assessment of the Advanced Encryption Standard. In fact, this task lies within a broader research area of symmetric cipher cryptanalysis, and it is anticipated that collaboration with the AZTEC virtual lab will complement the efforts within the STVL. A third goal of the STVL will be to address the development of lightweight cryptographic primitives as a fundamental foundation to ambient technology.

The main technical objective of the AZTEC lab is to allow better collaboration among European institutions on the design and analysis of asymmetric cryptographic techniques. To accomplish this goal, four main areas of study have been identified. First, it is important to study, compare and propose mechanisms for provable security, to improve and better understand the security of asymmetric schemes. A second target for the AZTEC efforts is to develop alternatives to the RSA scheme, with particular attention to lightweight solutions, a task that will require considerable efforts from industry and academia. In the Internet era, many new applications are emerging for which asymmetric primitives with some specific properties are useful; for this reason it is fundamental to include the study of such primitives as the third target area of the AZTEC lab. Finally, since there cannot be
unconditionally secure asymmetric cryptography, the fourth goal of AZTEC is to improve our knowledge on the hardness of the computational problems that are used as underlying assumptions to provide security.

PROVILAB is concerned with cryptographic protocols, where two or more agents interact in order to reach some common goal; this can be to establish a secure network connection, to realize a payment transaction securely, or to carry out a secure auction over a network. A large body of theoretical research on protocols already exists, but our basic knowledge is still far from complete. Furthermore, analyzing the security of concrete protocols is notoriously difficult, and several solutions proposed and sometimes even used in practice have later turned out to be insecure. The first objective of PROVILAB is therefore to construct practically useful protocols for a wide range of applications with well understood and provable security. The second is to expand our basic knowledge, for instance in the area of unconditional security, i.e. protocols that remain secure, no matter the resources invested in breaking them.

The VAMPIRE lab has a dual role in ECRYPT. On one hand, it will research new techniques that are related to efficient and secure implementation. On the other hand, VAMPIRE will provide a bridge between the research and the user community. In concrete terms, the technical goals of the VAMPIRE lab for the duration of ECRYPT can be summarized as: development of novel efficient implementation techniques in hardware and software; development of a solid understanding of existing and new side channel attacks and efficient counter measures; researching and understanding of crypto analytical hardware and its impact on cryptographic parameters. There are also non-technical objectives: It is hoped that the important field of cryptographic implementation grows internationally through VAMPIRE and that the interplay of secure algorithms and secure implementations becomes more prominent. It is hoped further to foster cooperation between strong engineering groups and pure crypto groups. Also, it is a major goal to bridge the existing gap between the research community and engineers in industry who need to apply implementation techniques. Another important objective is to assist the researchers in the other (more theoretical) Virtual Labs in understanding the requirements and meeting the needs of applied cryptography. The interdisciplinary structure of ECRYPT appears to be an ideal mechanism to reach these goals.

The watermarking and perceptual hashing virtual lab WAVILA intends to broaden the scope of ECRYPT beyond the classical cryptographic techniques into the domain embedded signalling and fuzzy signatures. These two techniques have recently been proposed as important ingredients in digital rights management (DRM) systems, but they have never fully been analyzed with respect to security and usage (protocols), comparable to the standard of cryptography. It is the goal of WAVILA to build tools and techniques for assessing the security aspects of watermarking and perceptual hashing, to design advanced algorithms with a well-defined security level, to design protocols, both stand-alone as well as
integrated in cryptographic protocols, and to develop methods and techniques for efficient and secure implementations. The overall and broader goal is to bring watermarking and perceptual hashing to such a level that they can be successfully integrated into future DRM systems.

5.5 EU-Projects NESSIE and eSTREAM

The following serves as an example how IT Security Information Analysis can be put into practice. The main objective of the project is to put forward a portfolio of strong cryptographic primitives that has been obtained after an open call and been evaluated using a transparent and open process. The project intends to contribute to the final phase of the AES (Advanced Encryption Standard) block cipher standardisation process (organised by NIST, US), but will also launch an independent open call for a broad set of primitives providing confidentiality, data integrity, and authentication. These primitives include block ciphers, stream ciphers, hash functions, MAC algorithms, digital signature schemes, and public-key encryption schemes. The project will develop an evaluation methodology (both for security and performance evaluation) and a software toolbox to support the evaluation. The project goal is to widely disseminate the project results and to build consensus based on these results by using the appropriate forums (a project industry board, 5th Framework programme, and various standardisation bodies). A final objective is to maintain the strong position of European research while strengthening the position of European industry in cryptography.

NESSIE was an EU project for the evaluation of cryptographic algorithms. As a follow-up, eStream has been organised under the ECRYPT network, to identify “new stream ciphers that might become suitable for widespread adoption”. NESSIE (New European Schemes for Signatures, Integrity and Encryption) was a European research project funded from 2000–2003 to identify secure cryptographic primitives. The project was comparable to the NIST AES process and the Japanese Government-sponsored CRYPTREC project, but with notable differences from both. In particular, there is both overlap and disagreement between the selections and recommendations from NESSIE and CRYPTREC (as of the August 2003 draft report). NESSIE was intended to identify and evaluate quality cryptographic designs in several categories, and to that end issued a public call for submissions in March 2000. Forty-two were received, and in February 2003 twelve of the submissions were selected. In addition, five algorithms already publicly known, but not explicitly submitted to the project, were chosen as ‘selectees’. The project has publicly announced that ‘no weaknesses were found in the selected designs’.

The selected algorithms and their submitters or developers are listed in the Appendix.
5.6 ESRAB (European Security Research Advisory Board)

ESRAB was established in 2005, although it had a more or less informal predecessor, the so-called Group of Personalities (GoP). ESRAB reports to the European Commission. Members were nominated ‘ad personam’ and no substitutes were appointed. Members served in a personal capacity and advised the Commission independently of any outside instructions.

The board has about 50 members. It consults the European Commission in questions of security, both military and police. In 2006, it has published its report “Meeting the Challenge: the European Security Research Agenda”. Concern is expressed about the differing levels of security awareness throughout the EU. This report has contributed tremendously to both the framework programme on “Security and Safeguarding Liberties” and the tenth thematic area of the Seventh Framework Programme for Research and Technology Development. The Board has ceased its activities on the 31st December 2006.

To develop the longer-term perspective in the field of Security research, a “Group of Personalities”, composed of high level industrialists, members of the European Parliament, and representatives of international organisations and research institutes, chaired by Commissioners Busquin and Liikanen, was set up in 2003 and presented a report to the Commission.

As a follow-up to this report, the Commission adopted the Communication ‘Security Research: The next Steps’ (COM(2004)590 final) on 7 September 2004 which subscribed to the main thrust of the recommendations and orientations of the Group of Personalities.

One of the actions the Commission announced was its intention to create a ‘European Security Research Advisory Board’ (ESRAB). The Board was to include high level strategists, with a responsibility relating to security research, from a broad spectrum of stakeholder groups including public and private users, industry, the European Defence Agency and research establishments. The Board was created by Commission decision (2005/516/EC) on the 22nd April 2005.

Tasks:

Specifically, but not exclusively, ESRAB shall make recommendations to the Commission in the following areas:

- the strategic missions, focus areas and priorities setting for future security research programme, on the basis of the report “Research for a Secure Europe” of the Group of Personalities while taking into account the establishment of the European Defence Agency as well as national and inter-governmental activities;
- the technological capabilities to be put in place among the European stakeholders; it shall recommend a strategy to improve the European industry's technological base, so as to improve its competitiveness;
- the strategic and operational aspects of the future security research programme taking into account the experience and results obtained from the Preparatory Action on the enhancement of the European industrial potential in the field of security research, from Commission services with an active interest in the field of Security including research covered by the EC Framework Programme for research and from other expert or advisory groups;
- the implementation issues such as the exchange of classified information and intellectual property rights;
- optimising the use of publicly owned research and evaluation infrastructures;
- a communications strategy to promote awareness of the future security research programme as well as for providing information on stakeholders' research programmes.

One of the fundamental roles of the government is to help ensure the security of its citizens. Studies show the threat of terrorism, organised crime, and natural disasters are among Europeans’ worst fears. The goal of European Security Research is making Europe more secure for its citizens while increasing its industrial competitiveness. By co-operating and coordinating efforts on a Europe-wide scale, the EU can better understand and respond to risks in a constantly changing world.

ESRAB’s findings

**Information management** systems that more efficiently and effectively provide first responders and decision-makers with improved situation awareness and interoperable command and control capabilities is a key area for investment. This includes improved surveillance capabilities with respect to coverage and quality and the fusion of real-time sensor data in order to establish a common operational picture. On occasion planning, modelling and situation analysis tools will also need to be integrated. GMES (Global Monitoring for Environment and Space), and its first wave of services, could play an integral role in this respect. Situation awareness and command and control capabilities should be supported by robust, secure and interoperable communication systems allied to significantly improved protection of supervisory control and data acquisition (SCADA) systems, widely used today for energy generation, transmission and distribution.

**Risk assessment, modelling and simulation tools** should act as support tools for decision makers in setting priorities for multiple threats and testing mitigation measures prior to incident intervention. Such tools will also benefit first responders in their efforts to improve training and exercise capabilities. Finally, the
development of intervention and neutralisation capabilities, in particular for post-crisis decontamination, is important.

The research path, system-of-systems demonstration, recognises that for large security solutions to enter into service, numerous independent but interrelated systems must be integrated and then demonstrated to prove operational effectiveness. In areas of significant European interest, it is recommended that demonstration programmes be established to act as federative frames to coalesce the required research. These European flagships would aim to ensure the coherent development of the required system building blocks, architectures and standards. As the GoP report highlighted, technology can only be part of the effective response to security threats and must be applied in combination with organisational processes and human intervention.

The implementation rules address the issue of how to cope with the specificities and sensitivities of implementing European security research. Particular governance structures, mechanisms for handling classified information, reinforcing the protection of intellectual property rights and assessing the suitability of international cooperation are recommended. Specific aspects of evaluation and co-funding levels have also been identified.

The coordination and structuring subsection outlines mechanisms to address the efficiency and effectiveness of European security research with the objective of avoiding unnecessary duplication and focusing research on high leverage customer driven requirements. All proposed mechanisms aim to deepen end-user engagement with the most ambitious mechanisms calling for the creation of a new European Security Board whose principal aim would be to ensure that all the component parts required to realise an improvement in European security (research, policies, legislation, standardisation, etc.) are synchronised and directed towards commonly agreed priorities.

The link to innovation subsection identifies mechanisms by which European security research can stimulate innovation, raise competitiveness and accelerate the pull through of research into procured products and services. ESRAB’s principal recommendation is the development of a European security innovation system. It should build upon innovative pre-commercial public procurement, the use of large-scale demonstration programmes, and the definition and use of European standards.

Europe has never been so peacefully consolidated, so prosperous and secure yet at the same time so vulnerable. Since the end of the Cold War, the threat of large-scale military aggression has subsided and been substituted by new threats, risks and vulnerabilities. These were laid out in the European security strategy, A secure Europe in a better world (2003), to include organised crime, terrorism, state failure, regional conflicts and proliferation of weapons of mass destruction. The new threats underline the fact that internal and external security is increasingly
inseparable, with the first line of defence often being abroad. European imports and exports have increased at 8% per annum over the last decade. There is a growing dependence on interconnected infrastructures in transport, energy, information and other fields increasing the vulnerability of modern societies. At the same time, the natural diffusion of technological know-how resulting from scientific and industrial development makes it easier for technological advancements to be used malevolently.

Although not yet complete, the Commission is actively engaged with a broad community of owners, operators, regulators, professional bodies, industry associations and governments to develop a European programme for critical infrastructure protection. The threats facing Europe are multifaceted, interrelated, complex and increasingly transnational in their impact. It is a simple truth that no single state can accomplish security alone — not even the United States. Implementing the European security strategy demands a comprehensive suite of instruments covering intelligence, police, judicial, economic, financial, diplomatic and technological means.

Based on 11 functional groups (listed below), it runs as a wire frame through the report:

- risk assessment, modelling and impact reduction;
- doctrine and operation;
- training and exercises;
- detection, identification and authentication;
- positioning and localisation;
- situation awareness and assessment (surveillance);
- information management;
- intervention and neutralisation;
- communication;
- command and control;
- incident response.

Situational awareness involves the capture, fusion, correlation and interpretation of disparate forms of real-time and historical data and their presentation in a clear manner, facilitating effective decision-making and performance in a complex environment. Interoperable databases will be essential to allow surveillance information to be cross-referenced against multiple heterogeneous sources.

Handling information acquired by many different sources and making it available to those with permission is an essential capability in order to improve awareness at Europe's borders. Techniques related to data and information fusion including data mining, natural language processing technologies, image/pattern recognition and expert systems are key enabling capabilities for this function. Such techniques must be investigated in parallel to intelligent knowledge based systems.
which look to develop active learning networks to identify and alert border security communities to early warning signs of possible threats. Priority, however, should be given to the development of information fusion, exchange techniques, gateways and translators, to facilitate the exchange of information between non-interoperable information systems at borders.

Due to the sensitive nature of policing Europe's external borders, particular attention should be paid to improving end-to-end secure communication in order to facilitate sharing of data within, and between, organisations and countries. To this end capabilities supporting interoperable and robust software defined radio solutions, offering the requisite flexibility to respond to dynamic situations are seen as important.

- Data fusion techniques: Design, development and application of data/information fusion techniques. Examples contain data mining, trend detection, forgetting data, optimization analysis. Information exchange: techniques to facilitate the exchange of information between non interoperable information systems.
- Semantics, topology: development of topologies and ontologies to facilitate data exchange based on semantic translations and common definitions of content.
- Secure interoperability: techniques to insure secure interoperability between current and future systems, domain different systems (i.e. civil and military) including data access control and data exchange without source availability Data fusion techniques Text-mining / data-mining Information fusion technology.
- Communication solutions for ensuring end-to-end communication availability, relying on physical and logical technologies, on diversity of hybrid systems.
- End-to-end quality of service, covering specific requirements for priority traffic and ensuring the QoS is guaranteed under all conditions.
- Interoperable and robust solutions for software defined radio Dynamic authentication in ad hoc wireless networks for emergency communication.
- Physical integration of C4 (Command, Control, Communication and Computers) equipment and interface with carrying platforms.
- Equipment of limited cost, dimensions, mass, power supply.
- Communications network management and control equipment, network supervisor.
- Authentication technologies.
- Broadband access to mobile users in dynamic situations / EM difficult scenarios.
- Secured, wireless broadband data links for secured communications.
Threat assessment models are needed to identify appropriate and targeted countermeasures. Modelling the development of terrorism and crime and the measures to prevent criminal or terrorist networks from expanding is seen as an important enabler. Decision models aimed at identifying cost effective and efficient countermeasures to protect physical structures are perceived to be a high value capability. In addition, capabilities for observation in difficult and complex environments are needed. Automated observation and monitoring should be supported.

The integration of new sensors into existing monitoring, access, control or logistic networks will improve widespread and affordable observation capabilities. Situation awareness will require a large improvement in existing command and control centres.

The prediction and correlation of events requires the development of domain and scenario-specific models to be used for advanced warning and target assessment. Mobile robust automated surveillance systems are needed to meet increasing surveillance requirements with respect to coverage and quality. Interoperability and information sharing requirements mandate the interconnection of different networks. To protect information housed in heterogeneous, decentralised and interconnected networks, new techniques are needed to guarantee their safe and secure use. The objectives are to establish a secure strategic security situation awareness system by automatically combining data from disparate high volumes data repositories and analysing the data to facilitate decision-making. The security of the infrastructure to perform this task is also a key objective.

Information management comprises data fusion techniques including mining, trend detection and optimization analysis, cultural, behavioural analysis, automated information production, monitoring and acting on digital traces, automated content analysis to track illegal content semantics, topology development to facilitate semantic data exchange, filtering technologies, natural language processing technology, and advanced behaviour modelling. Capabilities and tools for risk assessment and response modelling in critical infrastructures are needed. These tools will offer important aids for decision-makers to determine priorities among multiple risk factors, and, in some instances, to model the impact of proposed solutions. In addition, capabilities addressing the protection against cascading (‘domino’) effects are seen as key issues. In particular, specific tools to protect communication grids against cascading effect by automatic isolation in case of failure of interconnected grids are required.

The need for robust and secured communication is ubiquitous, with a special focus on capabilities for automatic authentication of people accessing terminals and networks, and the monitoring of the network traffic to detect malicious suspicious traffic and identify predefined patterns. Research into more robust encoding, not necessarily cryptography, so as to improve the protection and resilience of communication network from jamming and heavy noise signals is
also required. Integrated capabilities are required for the protection of supervisory control and data acquisition systems (SCADA) from attack. SCADA systems and networks, however, are not designed to withstand attacks. Key issues in this regard are

- monitoring of network traffic
- identification of suspicious traffic
- user authentication for terminal and network access
- physical integration of C4 equipment and interface with carrying platforms
- end-to-end interoperable secure communication infrastructure and service
- detection and identification of fraudulent control
- load balancing mechanisms (related to telecommunication networks)
- protection against heavy noise, jamming, and other harsh environment
- pattern recognition
- text and data mining
- biometrics
- security equipment
- filtering technologies

The monitoring of threats, events or critical infrastructures produces a wide range of information in the form of data which is subject, in many instances, to coding against a particular data format. Such data is carried across different networks using various technologies. There is a pressing need to define common standardised data formats to ensure information coding permits data exchange between people and systems. It is, however, impractical, and therefore unlikely, that large amounts of data would be retrospectively codified against a common standard for interoperable representation of the information (e.g. common formats, common data model) or even against a common language with the difficulties of achieving a common understanding of nomenclatures across the EU. A more practical approach would be to adopt a common interchange standard for data, either bilaterally between stakeholders or preferably for the EU as a whole.

闻言 gateways and/or translator units would be used as necessary to convert formats and protocols as required. Such translators and gateways, where information is formatted in a structured manner, require common data models in order to simplify and automate the translation process. Research into how semantic interoperability could be defined and applied would be valuable. Their definition will, however, be challenging since more than 80 % of the world's database content is in unstructured largely textual format. Commonly formatted data strongly lends itself to the application of data fusion, data mining and information processing techniques. The following technologies were identified in support of this capability:
network and protocol independent secured communications;
protocol technologies;
data and information management technology (databases, etc.);
COTS software assessment;
communications network management and control equipment, network supervisor;
infrastructure to support information management and dissemination.

In terms of interoperability, the ability to rely on interoperable communication mechanisms is a key basic enabler across all missions. The ability to exchange voice and data on demand, in real time, when needed and to command and control resources across a range of situations and departments is essential. Addressing this issue is critically important and can be achieved in two ways. First is the development of appropriate communication gateways that support the various necessary communication protocols and translate from one to another. Second is the development of new technologies that can be widely adopted in a migration phase from the current mechanisms to the new ones, over the longer term. Speed is the driving factor for authentication and information management techniques, database design and high speed communication bandwidths will all figure strongly in final solutions. Authentication speed is also affected by the chosen method of identification which varies considerably depending on the entity requesting access — be that an individual, system or application.

By way of example, biometrics is viewed today, and increasingly so, as the solution of choice for the identification and authentication for individuals. For widespread deployment of biometric-based solutions for identification and authentication interoperability between biometric data readers and their corresponding authentication databases is of critical importance. The following technologies were identified in support of this capability:

- effective and easy-to-use biometric technologies (e.g. facial recognition, iris/retina, fingerprint, etc.);
- two-factor authentication technologies for IT and network access;
- distributed trust models and technologies;
- access control models and technologies for distributed environments.

ESRAB recommends that the Commission take full advantage of the report in its preparation and implementation of the forthcoming FP7 security research work programme. In addition, ESRAB recommends the creation of a European Security Board (ESB) in order to foster greater dialogue and a shared view of European security needs with the aim of advising as to the content of a strategic security agenda. The ESB should be operational in the first half of 2007. However, at the time of writing, the ESB has not been established.
5.7 Related Publications

An overview of related publications and information is provided in Table 4.

Table 4: Overview of Related Publications

<table>
<thead>
<tr>
<th>DATE</th>
<th>ORGANIZATION</th>
<th>SUBJECT OF CONFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Organization</td>
<td>Subject of Conference</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2002</td>
<td>Enterprise DG</td>
<td>Support services for micro, small and sole proprietor businesses,</td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://europa.eu.int/comm/enterprise/entrepreneurship/craft/craft-supportserv.htm">http://europa.eu.int/comm/enterprise/entrepreneurship/craft/craft-supportserv.htm</a></td>
</tr>
<tr>
<td>2002</td>
<td>European Commission</td>
<td>Innovation Policy in Europe 2002 (European Trend Chart on Innovation),</td>
</tr>
<tr>
<td>2002</td>
<td>European Commission</td>
<td>Innovation tomorrow,</td>
</tr>
<tr>
<td>2001</td>
<td>European Commission</td>
<td>Building an innovative economy in Europe,</td>
</tr>
<tr>
<td>2001</td>
<td>European Commission</td>
<td>Innovation and enterprise creation. Statistics and indicators,</td>
</tr>
</tbody>
</table>
6 National Organizations and Activities

6.1 France

6.1.1 Direction générale de la sécurité extérieure (DGSE, General Directorate for External Security)

The Direction Générale de la Sécurité Extérieure (DGSE) or "General Directorate for External Security" is the foreign intelligence agency of France. It was formed on April 2, 1982 to replace the former Service de Documentation Extérieure et de Contre-Espionnage (External Documentation and Counter-Espionage Service, SDECE). (The SDECE was the external intelligence agency of France from November 6, 1944 to April 2, 1982.)

The DGSE was formed under the authority of the French ministry of defense, and made responsible for searching and exploiting intelligence which is relevant to the security of France, as well as detecting and finding external espionage activities directed against French interests in order prevent their consequences.

The DGSE includes the following services:

- Directorate of Administration
- Directorate of Strategy
- Directorate of Intelligence
- Technical Division - Responsible for electronic intelligence and devices
- Operations Division - Responsible for clandestine operations
- Action Division, part of the Operations Division

Action Division

The action division (Division Action) is responsible for planning and performing clandestine operations. It also fulfills other security-related operations such as testing the security of nuclear power plants (as it was revealed in Le Canard Enchaîné in 1990) and military facilities such as the submarine base of the Île
Longue, Bretagne. The division's headquarters are located at the fort of Noisy-le-Sec.

The current action division originated from the SDECE's action service (Service Action or SA. Service Action is still commonly used). The action division has a “tank” of paramilitary operatives coming mainly from the French Army, many coming from the paras and some coming from the Special Forces. Since the early 1980s, the service action is divided in three main parts: commandos, combat divers and air support.

The commandos were originally chunked in the "11e Choc" (11e Bataillon Parachutiste de Choc, 11th Shock Parachutist Battalion, later 11th Shock Parachutist Demi-Brigade), created in 1946. The 11e Choc was disbanded in 1963 because its officers were suspected to be French Algeria supporters. Consequently, its missions were partly given to military units, especially the 1st Marine Infantry Parachute Regiment and the 13th Parachute Dragoon Regiment. After the sinking of the Rainbow Warrior, the "11e Choc" was re-raised in 1985 as the 11th Shock Parachutist Regiment. The unit was disbanded in 1993 among other various changes of French armed forces following the end of the cold war. DGSE commandos are since based in three "training centers", the CPIS, the CPES and the CPEOM.

The commando Hubert originally included servicemen from both French Navy and Army. The unit soon split in two, the army soldiers being transferred to the Centre d'Instruction des Nageurs de Combat (CINC, combat divers training center, nicknamed Ajax) assigned to "11e Choc". In the aftermath of the disastrous Rainbow Warrior affair, the CINC was officially disbanded, and the DGSE combat divers were transferred in the CPEOM. The air support of DGSE operations is provided by a French Air Force unit, the Groupe Aérien Mixte 00.056 (GAM 56) 'Vaucluse'.

The DGSE headquarters, codenamed CAT (Centre Administratif des Tourelles), are located at 141 Boulevard Mortier in the XXe arrondissement in Paris, approximately 1 km northeast of the Père Lachaise Cemetery. The building is often referred to as La piscine (“the swimming pool”) because of the nearby Piscine des Tourelles of the French Swimming Federation.

A project named "Fort 2000" was supposed to allow the DGSE headquarters to be moved to the fort of Noisy-le-Sec, where the Action Division was already stationed. However, the project was often disturbed and interrupted due to lacking funds, which were not granted until the 1994 and 1995 defense budgets. The allowed budget passed from 2 billion francs to one billion, and as the local workers and inhabitants started opposing the project, it was eventually canceled in 1996. The DGSE instead received additional premises located in front of the Piscine des Tourelles.
As of 2007 the DGSE employed a total of 4620 agents. In 1999, the DGSE was known for employing a total of 2700 civilians and 1300 Officers or Under Officers in its service. It also benefits from an unknown number of voluntary correspondents both in France and abroad. These do not appear on the government's list of civil servants and are referred to with the title of "honorable correspondant" (honourable correspondent). The DGSE is directly supervised by the Ministry of Defense.

The DGSE's budget is entirely official (it is voted upon and accepted by the French parliament). It generally consists of about 270 millions Euros, in addition to which are added special funds from the Prime Minister (often used in order to finance certain operations of the Action Division). How these special funds are spent has always been kept secret.

Some known yearly budgets include:

* 1991: 0.9 billion francs
* 1992: 1 billion francs
* 1997: 1.36 billion francs
* 1998: 1.29 billion francs
* 2007: 450 million euros, plus 36 million in special funds

According to Claude Silberzahn, one of its former directors, the agency's budget is divided in the following manner:

* 25% for military intelligence
* 25% for economic intelligence
* 50% for diplomatic intelligence

Various tasks and roles are generally appointed to the DGSE:

* Intelligence gathering:
  
  o HUMINT, through formal agents and voluntary correspondents
  
  o SIGINT, through networks such as Frenchelon
  
  o Space imagery analysis
* Support for HUMINT.

Counter-intelligence on French soil is not conducted by the DGSE but by the Direction de la Surveillance du Territoire (DST).

6.1.2 Direction de la Surveillance du Territoire

The Direction de la Surveillance du Territoire (DST; Directorate of Territorial Surveillance) is a directorate of the French National Police operating as a domestic intelligence agency. Its attributions include counterespionage, counterterrorism and more generally the security of France against foreign threats and interference, including economic. It was created in 1944 with its headquarters situated at 7 rue Nélaton in Paris.

The DST Economic Security and Protection of National Assets department has units in the 22 regions to protect French technology. It has been operating for 20 years, not only on behalf of defense industry leaders, but also for pharmaceuticals, telecoms, the automobile industry, and all manufacturing and service sectors.

History of the DST

During the Algerian War (1954-62), the agency created in December 1956 the Organization of the French Algerian Resistance (ORAF), a group of counter-terrorists whose mission was to carry out false flag terrorist attacks with the aim of quashing any hopes of political compromise.

On December 3, 1973, agents of DST, disguised as plumbers, were caught trying to install a spy microphone in the offices of the Canard Enchaîné newspaper. The resulting scandal forced Interior Minister Raymond Marcellin to leave the government.

One of the greatest successes of the DST was, paradoxically, the recruitment of the Soviet KGB officer Vladimir Vetrov. Between the spring of 1981 and early 1982 he handed almost 4,000 secret documents over to the DST, including the complete official list of 250 Line X KGB officers stationed under legal cover in embassies around the world, before being arrested in February 1982 and executed in 1983.
6.1.3 Direction Centrale des Renseignements Généraux

The Direction Centrale des Renseignements Généraux (Central Direction of General Intelligence), often called Renseignements Généraux (RG), is the intelligence service of the French police, under orders of the Direction Générale de la Police Nationale (DGPN), and ultimately of the Ministry of the Interior. It is also in charge of the monitoring of gambling places and horse racing ranges.

Organisation

The RG is subdivided into four sub-directions:

* Research
* Analysis, prospective and society facts
* Resources and methods
* Games and casinos

The RG employ 3,850 public servants of the Police. Members of the RG do not have a judiciary police qualification as long as they work for this service, except for those of the "Games and casinos" sub-direction. The current chief of the RG is Pascal Mailhos.

Sub-direction of Research

The Sub-direction of Research is in charge of intelligence, prevention and repression of terrorist acts, particularly by monitoring groups and organisations likely to be linked to such activities.

Sub-direction of Analysis, Prospective and Society Facts

The Sub-direction of Analysis, Prospective and Society Facts is in charge of analysing and fusing data collected from social, financial or other institutions.

Sub-direction of Resources and Methods

The Sub-direction of Resources and Methods is in charge of recruitment, logistics, documentation and juridical matters, as well as of budget and formation of personnel.

Sub-direction of Games and Casinos

The Sub-direction of Games and Casinos monitors these places, and also has judiciary and police powers there.
History

Although police intelligence services appeared in the Ancien Régime (the time before the revolution), the term “Renseignements Généraux” dates back to 1907, with the creation by the director of the General Security, Célestin Hennion, of an intelligence department parallel to the judiciary services.

During the 30s, the activities of fascist groups, more or less manipulated by foreign powers, (like “La Cagoule”) triggered the creation of a "Direction des services de renseignements généraux et de la police administrative" (1937), followed by a "Inspection générale des services de renseignements généraux et de la police administrative" (1938).

In 1941, the Regime of Vichy created its own service, named “direction centrale des Renseignements généraux”.

After the liberation of France, the RG took back the role that they had in the 30s. With the context of the decolonisation, they were confronted to new threats, notably the emergence of modern terrorism with the OAS.

From 1973, the role of borders monitoring was detached to a dedicated service, the “Police de l’Air et des Frontières” (PAF).

From the 90s, the RG have been confronted to new events. They now particularly monitor radical Islamism, altermondialisation movements and cults.

Over the years, there have been numerous accusations that the RG has engaged in illegal spying on journalists or political opponents of the government. The suppression of the RG or their integration with some other police services, such as the DST, was suggested several times, but never implemented.

6.1.4 Business Centers

In France, currently 34 Euro Info Centers exist that provide support for the business support network structures in the country. Details on the French EIC network are provided in the document “National Network Fact Sheet” [NNF].

The national EIC website is hosted by the Ministry of Economics, Finance and Industry (MINEFI) at the link: http://www.eic.minefi.gouv.fr/.

Other community networks in France currently include 47 Innovation Relay Centers (IRCs) and 31 Business Innovation Centers (BICs).
6.2 Germany

6.2.1 BSI

BSI (Bundesamt für Sicherheit in der Informationstechnik), with a staff of about 450, is a German national institution concerned with various aspects of IT security. It is affiliated with the Ministry of the Interior. It has been founded in 1991 and is located in Bonn. It also operates the CERT-Bund for the EDP-users of the federal government. The agency informs about all important aspects of IT-security and gives consultancy to IT users. It also develops IT security applications and products on its own, such as systems for handling classified information by government agencies, and tests and certifies IT products regarding their security, especially according to the Common Criteria. Further, BSI is concerned with the security of critical infrastructures. It assists the federal government in the realisation of the National Plan for the Protection of Information Infrastructures (Nationaler Plan zum Schutz der Informationsinfrastrukturen, NPSI). Future work will include botnets and Internet telephony. BSI publishes the regular report “The Situation of IT-Security” (Lage der IT-Sicherheit) and a newsletter “Securely Informed” (Sicher Informiert). The homepage of BSI (www.bsi.bund.de) addresses the IT expert, while the Internet site (www.bsi-fuer-buerger.de) is for the general public. Product development and distribution is in general done in co-operation with the private company secunet of Essen, Germany.

VPS

VPS (Virtuelle Poststelle, virtual postal despatcher) is a general frame for secure eGovernment applications making use of client server architecture. On basis of VPS, government authorities can develop their own applications, such as trade in carbon dioxide emission allowances, the electronic town hall, or automated judicial correspondence.

SINA

SINA is a system for handling classified information by government agencies. SINA is permitted within EU and NATO for all levels of classification. It consists of the components SINA Box, SINA thin client, and SINA Virtual Workstation. SINA is based on the Linux operating system and IPsec for transmission. It uses the conceptual idea of “sandboxing”.

ElcroDat 6-2

ElcroDat 6-2 is an encryption system for use by the military and the diplomatic service. Product development was done by BSI in co-operation with the private company Rohde & Schwarz ST GmbH, which also produces and distributes the product. ElcroDat 6-2 is permitted within EU and NATO for all levels of classification. It is available for ISDN and PCM-30. Key distribution is based on a PKI.
There are components for encryption/decryption, remote management, service, and logging.

Galileo

Galileo is the future European satellite navigation system. BSI has been entrusted with its security. Galileo will ultimately consist of 30 satellites as transmitters, once it will be fully operational in 2011. Multilateration of four satellites is used for finding the exact position of the receiver. The Galileo-project has a plethora of security issues, many of which have already to be considered during the early design phase of the system. To mention, are general computer security, PKI for management and maintenance, pay system, etc.

SAR-Lupe

SAR-Lupe (Lupe German for magnifying glass) is a German reconnaissance satellite system that will consist of 5 satellites once it is fully operational (in 2008). It is operated by the military (Bundeswehr). It uses synthetic aperture radar (SAR) in the X-band (the decimetre-band), i.e. a multitude of pictures of a restricted area is taken from a varying angle to achieve a single very high resolution picture (resolution less than 1 m) by computational methods. (However, this method only works with targets nearly at rest.) The cryptographic security of the entire system is in the responsibility of BSI.

Nationaler Plan zum Schutz der Informationsinfrastrukturen

The “Nationaler Plan zum Schutz der Informationsinfrastrukturen” (NPSI, National Plan for the Protection of Information Infrastructures) has been issued by the German government (Ministry of the Interior) in 2005. It defines 15 political goals concerning IT-security. The state of the document is something like a recommendation or a political road map.

To a growing extent, organised crime and international terrorism are involved in computer related incidents. The Ministry of the Interior identifies denial of service, spyware, eavesdropping, man in the middle attacks, and hacking. Countermeasures are comprised by prevention, reaction, and persistence. Fields of application are the federal government, critical infrastructures, and others as demand arises. According to NPSI, BSI is responsible for the part on the federal government. Co-operation with private industry is necessary, especially in the case of critical infrastructures.

The protection of IT-infrastructures in Germany is not only in the responsibility of specialists, it needs the co-operation of every single citizen. General computer users have to acquire a certain degree of security awareness. The best time to start with may be at school. This concerns especially the proper use of security software and a sense of which URLs to trust and which better not to. In the future,
computer users even may be held liable for any damage their computer may cause to others, especially in case of virus propagation or botnets.

Reliability and trustworthiness of IT products are also important aspects. It means that asserted properties of the system will be maintained over the time span foreseen and under all reasonable conditions of operation. The systems must be safe in the sense that they do no damage to the outer world, neither under normal conditions nor in case of faults.

6.2.2 Bundesnachrichtendienst

The Bundesnachrichtendienst (Federal Intelligence Service, BND) is the foreign intelligence agency of the German government, under the control of the Chancellor's Office. Its headquarters are in Pullach near Munich, and Berlin (planned to be centralised in Berlin by 2011). The BND has 300 locations in Germany and foreign countries. In 2005, the BND employed around 6,050 people, 10% of them Bundeswehr soldiers; those are officially employed by the "Amt für Militärkunde" (Office for Military Sciences), which is just a camouflage name. The annual budget of the BND exceeds 430,000,000 €.

The BND acts as an early warning system to alert the German government to threats to German interests from overseas. It depends heavily on wiretapping and electronic surveillance of international communications. It collects and evaluates information on a variety of areas such as international terrorism, WMD (weapons of mass destruction) proliferation and illegal transfer of technology, organised crime, weapons and drug trafficking, money laundering, illegal migration and information warfare. As Germany’s only overseas intelligence service, the BND gathers both military and civil intelligence.

The domestic secret service counterparts of the BND are the Bundesamt für Verfassungsschutz (Federal Office for the Protection of the Constitution, BfV) and 16 counterparts at the federal state level (Landesämter für Verfassungsschutz or State Offices for the Protection of the Constitution); there is also a separate military intelligence organisation, the Militärischer Abschirmdienst (lit. military screening service, MAD).

The predecessor of the BND is the pre-war German military intelligence agency in the General Staff, led by Wehrmacht General Reinhard Gehlen. In 1946 Gehlen set up an intelligence agency informally known as the Gehlen Org, and recruited many of his former co-workers. On 1 April 1956 the Bundesnachrichtendienst was created from the Gehlen Org, and was transferred to the German government. Reinhard Gehlen remained President of the BND until 1968.

Structure
The Bundesnachrichtendienst is divided into 8 branches, with different operational intelligence tasks:

- Operative Aufklärung / Human Intelligence
- Technische Aufklärung / Signals Intelligence
- Auswertung / Analysis
- Steuerung und zentrale Dienstleistung / Administration
- Organisierte Kriminalität & Internationaler Terrorismus / Organized Crime & International Terrorism
- Technische Unterstützung / Technical Support
- Schule des BND / BND School
- Sicherheit / Security & Defense

The head of the Bundesnachrichtendienst is its President. The President of the BND has two deputies: one Vice-President and - since December 2003 - one Vice-President for military affairs. Prior to that time there was only one Vice-President.

6.2.3 Militärische Abschirmdienst

The Militärische Abschirmdienst (MAD), full name Amt für den Militärischen Abschirmdienst (official English name: "Federal Armed Forces Counterintelligence Office") is the German military intelligence service. It has about 1,300 military and civilian employees. Its headquarters are in the Konrad Adenauer Barracks in Cologne, North Rhine-Westphalia and there are 14 regional offices throughout Germany. In 1995, it had an annual budget of 74 million Euros.

The MAD is part of the Bundeswehr. As a domestic intelligence service, it has similar functions, within the military, as the civilian intelligence services (Verfassungsschutz). The main duties of the MAD are counterintelligence and detection of "anticonstitutional activities" within the Bundeswehr. Other duties include the protection of Bundeswehr properties from sabotage and foreign espionage. Members of the MAD are also involved in planning and construction of buildings with high security requirements. The legal basis for the MAD is the MAD Law of 1990-12-20, as amended by Article 8 of the law of 2005-04-22 Organisation.

In addition to the department of administrative affairs, there are the following specialist departments:

Department I: Central services
Department II: Counter-extremism
Department III: Counterespionage
Department IV: Protection of secrets (personnel and material)
Department V: Technology
The MAD developed out of a liaison office between the Allies and the German government and was founded in its present form in 1956, after the Bundeswehr had been created. Until 1984, it was called "Amt für Sicherheit der Bundeswehr" (ASBw). In September 1984, on the basis of the Höcherl report, the service was restructured and more civilian positions were created. After the former East German army, the National People's Army (NVA) was incorporated into the Bundeswehr in 1990; the MAD had 7 groups and 28 regional offices. This was reduced to 14 offices in 1994 when there was a reduction of armed forces.

6.2.4 The Bundesamt für Verfassungsschutz

The Bundesamt für Verfassungsschutz (BfV, "Federal Office for the Protection of the Constitution") is the Federal Republic of Germany's domestic intelligence agency. Its main function is the surveillance of anti-constitutional activities in Germany. The Bundesamt für Verfassungsschutz with its headquarters at Cologne is a federal institution under the control of the German Ministry of the Interior. 16 independent state based services (Landesämter für Verfassungsschutz, "State Offices for the Protection of the Constitution") exist in addition to this federal office.

Coordination between the different services and the parallelism of the state-based services is an ongoing problem. A merger into a single federal service has been the topic of discussion, but the proposal faces strong political resistance due to the highly regarded principles of federalism.

The main job of the Verfassungsschutz is to observe organizations that are considered a threat to the "free and democratic basic order" (Freiheitlich-demokratische Grundordnung) of the Federal Republic of Germany. While they do use all kinds of surveillance technology and infiltration, most of their information is assembled from publications of the observed organisations. The information is compiled into yearly reports (Verfassungsschutzberichte) which are made available to the public; presumably there are more detailed, non-public reports given to the governments.

The organizations being currently observed by the Verfassungsschutz fall into the following groups:

- Right-wing political extremists (mainly Neo-Nazis, including the NPD and DVU political parties)
- Left-wing political movements, platforms, activists and parties like Attac, Indymedia, the Berlin "Sozialforum" and parts of the left-wing parties Die Linke, PDS or the WASG
- Extremist organisations of foreigners living in Germany (most prominently Islamist terrorists)
- Scientology (considered by the German government an authoritarian, anti-democratic commercial organisation rather than a religion)
Some of the Verfassungsschutz organisations have been given additional jobs by specific laws, such as the protection of government-related classified information, the monitoring of foreign secret services, or the monitoring of organised crime.

6.2.5 Bundeskriminalamt (BKA, Federal Police Office)

The BKA is subordinate to the Federal Ministry of the Interior. Its responsibilities are the coordination of law enforcement in cooperation with criminal investigation bureaux of the individual states of Germany (these state investigation bureaux are known as Landeskriminalamt) and to conduct investigations in serious crimes, especially when other countries are involved. Approximately 5,200 BKA personnel operate nationwide. The BKA’s missions include:

- Coordinating cooperation between the federation and state police forces (especially state criminal investigation authorities) and with foreign investigative authorities.
- Collecting and analyzing criminal intelligence, managing the INPOL database of all important crimes and criminals.
- Investigating cases of terrorism, extremism, espionage, or economic and financial crime.
- Protection of federal witnesses.
- Acting as a clearing house for identifying and cataloging images and information on victims of child sexual exploitation.
- Information Technology.

The BKA only becomes involved in cases when requested by Land authorities or in cases involving two or more Länder. The federal prosecutor can also direct it to investigate cases of special public interest. The BKA also provides assistance to states in forensic matters, research and organized crime investigations. It is Germany’s national central bureau for the European Police Office (Europol), Schengen Information System and the International Criminal Police Organisation (Interpol).

Kriminalistisches Institut (KI)

The “Kriminalistisches Institut” of the BKA is an institution for application oriented research and development in the field of criminology. Among others, support service is provided to police agencies regarding investigations concerning IT technology. A technical service centre is maintained for supporting the fight against computer crime. Police officers are educated in related technologies. General research on the application of IT technology in the police service is also done. Projects are generally done in cooperation with outside research.
establishments. The KI regularly warns the general public about IT related criminal menaces like "phishing" attacks etc.

6.2.6 Civil Security Research

The Federal Ministry of Education and Research (BMBF) has performed an inventory on civil security research whose results have been published in the document "Research for Civil Security, An Inventory: Research Landscape and Contacts" [BMBF RCS].

During the survey on the status of security research in Germany, about 1200 institutions, companies and associations have been contacted and were asked to complete customized questionnaires about activities in the area of civil security research in publicly promoted projects in Germany and on an international level. Survey participants could present their competences, products and projects leading to profiles to get an overview of potential cooperation partners. The analysis of the feedback has shown that most of the industrial companies are not operating exclusively in the security sector, but are developing security solutions on the basis of their core competences, e.g. such as sensor technology, electronics, communication technology or even nano-technology.

Industrial companies are more focusing on the area of security of critical infrastructures, due to its demand for security products. Research institutes and major enterprises have shown a high participation in European R&D projects. As a main requirement, the promotion of the networking of the security research among the contributing fields of innovation and research disciplines and the pooling of the existing competences has been identified.

The BMBF published its new research program ICT 2020 at the CeBIT 2007 fair in Hannover in March 2007. This program was launched in cooperation with the scientific and industrial sector to improve the transformation of research results into products. Within ICT 2020 the Federal Government will fund ICT projects within the next three years with a budget of about one billion €. The program includes support for civil security research for the next four years with a budget of about 123 million € (see link: http://www.foerderinfo.bmbf.de/de/1837.php).

In this context the BMBF is funding projects which protect data communication independent of hardware and operating system, and basic mathematical work for the verification of ICT systems. The BMBF pursues the following main objectives:

- correctness, security and reliability of software systems,
- integration of methods of formal program development (formal specification, transformation and verification, consistent reference model),
- development of verifiable application software components,
• system and software requirement analysis,
• innovative integrated ICT security systems for the secure design, installation, configuration and operation of ICT systems, for personal protection and trustworthiness of systems, and,
• security of new ICT methods and techniques.

6.2.7 IT Security Activities in the Commercial Sector

Some IT Security activities related to the commercial sector such as the TeleTrusT Information Security Professional Certificate (TISP) have already been described in the SIT study for IPA [IPA 07-2].

Initiative “Germany Securely in the Net”

The special initiative "Deutschland sicher im Netz" (Germany Securely in the Net) has been launched in 2005 by 13 industrial partners under the patronage of the Federal Ministry of Economics and Technology (BMWi).

At the IT summit in 2006, the initiative has been established as a registered association. A cooperation agreement has been signed in 2007 between the Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM, Association for Information Technology, Telecommunications and New Media) as the representative of the "Deutschland sicher im Netz e.V." association and the Federal Ministry of the Interior (BMI) that has taken the future patronage. The continuous and effective engagement of the partners and their activities in the area of ICT security are stated in their so-called “Handlungsversprechen” (activity plan) that covers the following topics:

• appeals committee,
• development of secure software,
• general security issues,
• media competencies,
• online application center,
• secure e-commerce,
• security barometer, and,
• security checks.

During the course of the activities of the association, existing security risks will be identified and recommendations and guidelines will be provided to cope with these risks. In this context, the association members HP, SAP and Utimaco will jointly develop a road map, “secure enterprise”.

• Short Road: targeting at enterprises that want to get a fast overview of main topics of IT security, and that try to achieve a first overview of their security status,

• Mean Road: targeting at enterprises that want to increase their security level needed for continuous business operation regarding the availability, confidentiality and integrity of their ICT systems, and,

• Long Road: targeting at enterprises with high innovative products and high protection requirements.

The "Deutschland sicher im Netz e.V." association is a central partner for politics, societal groups and science in the area of ICT security. In this context, the association is also active in the implementation of ICT initiatives of the Federal Government (e.g. National Plan for Information Infrastructure Protection [BMI NPIIP]).

The association provides the following information, tools and services for the implementation of security strategies:

• advisory service by official advisors: see link: https://www.sicher-im-netz.de/default.aspx?sicherheit/ihre/check/berater/default,

• continuous security information service: see link: https://www.sicher-im-netz.de/default.aspx?initiative/informatives/default,


• partner information about participating enterprises, associations and institutions: see link: https://www.sicher-im-netz.de/default.aspx?initiative/partner/default,

• provision of tools to protect PCs,

• security awareness raising measures for controlled and trustful usage of ICT technology,

• security portal: see link: https://www.sicher-im-netz.de/, and the,


The IT security package contains the following set of ICT security measures and information for business managers, IT personal, and employees that complement the deployed security technology:

• check lists,

• damage events,

• emergency rules,

• liability risks,
• practical guidelines and instructions,
• security policies, and the,
• training of specialist dealers and system houses.

The first step of security measures deals with the identification of the IT security status and an overview of potential ICT security risks and the ITCT security policy. For this purpose, the IT security package contains the following tools:

• compact 4x4 check list as a comprehensive IT security evaluation instrument,
• MSAT tool: Microsoft Security Assessment Tool, including detailed questionnaire to identify and remove security risks, and the,
• MSAT user manual.

The second step of security measures focuses on the organization of effective protection including the following activities and support measures:

• guidelines for secure deletion of data,
• production of binding security guidelines for data storage, data archiving, virus protection, and emergency rules,
• provision of an emergency flyer with important information and instructions in the case of emergencies,
• provision of best practices examples for writing security policies,
• provision of documents as input for the writing of security policies and security,
• provision of materials for the sensitization of employees for the effective and secure usage of ICT during daily business operations,
• security measures after IT security violations,
• template for education and training, and sensitization of staff,
• template for the specification of a data security concept,
• template for the specification of a security policy for ICT usage,
• template for the specification of a security policy for Internet usage,
• template for the specification of a security policy for outsourcing,
• template for the specification of a security policy,
• template for the specification of a virus protection concept,
• template for the specification of an archiving concept,
• template for the specification of an emergency concept,
• template for the specification of security guidelines for administrators, and the,
• template for the specification of security guidelines for users.

The third step of security measures focuses on the organization of data protection including the following activities and support measures:

• provision of a praxis-oriented example of a security policy for data protection, and the,
• provision of a security guideline with praxis-oriented information about the organization and implementation of data protection.
The forth step of security measures focuses on the use of ICT including the following activities and support measures:

- advices on the use of the system recovery function under Windows XP,
- basic instructions for viruses and worms protection,
- basic rules for the handling of viruses in mails,
- basic security instructions for firewalls and specific instructions for the operation of Windows firewalls,
- description of new security functions in Windows XP,
- description of Windows XP update possibilities,
- example of a security policy on data protection,
- example of security policy on data privacy,
- information about data protection for ICT staff,
- information about the security of mobile phones,
- instruction for the protection of remote access,
- instruction for the security configuration of Windows XP clients,
- instructions and guidelines on the secure use of e-mails,
- instructions for avoiding unwanted accessibility of services via Internet under Linux,
- instructions for backup and recovery of servers,
- instructions for backup of server networks,
- instructions for ensuring secure passwords within whole organizations,
- instructions for intrusion detection,
- instructions for protection of clients against network attacks,
- instructions for protection of stand-alone Windows XP clients,
- instructions for providing updates with Windows update and automatic updates,
- instructions for securing active directory for administration groups and accounts,
- instructions for securing Internet information services,
- instructions for securing remote clients and portable computers,
- instructions for securing Windows Professional clients in Windows server environments,
- instructions for securing Windows XP Professional clients in Windows server environments,
- instructions for securing WLAN,
- instructions for the actualization of Linux security updates,
- instructions for the avoidance of connections of Windows computers to the Internet,
- instructions for the protection of data by means of hard disks encryption with ESF,
- instructions for the protection of networks by identification of network perimeters,
- instructions for the protection of Windows 2000 Professional in peer-to-peer network environments,
- instructions for the protection of Windows XP in peer-to-peer network environments,
- instructions for the secure use of passwords,
- instructions for the selection of secure passwords,
- instructions for the update of Windows networks,
- instructions for the use of network ports by main Microsoft server products,
- overview of common file types and their vulnerabilities related to viruses and worms,
- overview of potential damages due to insufficient ICT security measures,
- security concept for Windows XP,
- security measures for employees to ensure the implementation of security policies in enterprises, and the,
- software update services.

The initiative also provides a set of approved IT security solutions for different branches and applications, such as:

- example of a security policy on data protection,
- example of a security policy on the use of anti virus products,
- example of a security policy on the use of information and communication with third parties,
- example of a security policy on the use of IT infrastructures and communication components,
- example of a security policy on the use of IT pass words,
- example of a security policy on the use of standards for the operation of IT systems or networks,
- example of a security policy on the use of standards for the use of mobile devices,
- examples of best practices in e-commerce,
- examples of best practices regarding secure handling of data,
- examples of IT security concepts in the electronic sector,
- examples of IT security concepts in the logistics sector,
- examples of IT security concepts in the services sector, and,
- examples of IT security concepts in the trade sector.

Further information about ICT security is provided by the following links:

- BSI as neutral agency responsible for all matters of ICT security: see link: http://www.bsi.de/,
- BSI IT Base Protection Manual: see link: http://www.bsi.de/gshb,
- data protection portal: see link: http://www.datenschutz.de/,
6.3 United Kingdom

6.3.1 MI5

The Security Service, commonly known as MI5 (Military Intelligence, Section 5), is the United Kingdom's counter-intelligence and security agency and is part of the intelligence machinery alongside the Secret Intelligence Service (SIS or MI6), Government Communications Headquarters (GCHQ) and the Defence Intelligence Staff (DIS). All come under the direction of the Joint Intelligence Committee (JIC). The service has a statutory basis in the Security Service Act 1989 and the UK Intelligence Services Act of 1994. Its remit includes the protection of British parliamentary democracy and economic interests, fighting serious crime, militant separatism, terrorism and espionage within the UK. While mainly concerned with internal security, it does have an overseas role in support of the mission. The Security Service comes under the authority of the Home Secretary.

The commitment for the development of secure software is another main topic of the activity plan of the initiative. In this context, Microsoft and SAP have committed to support software developers and students at technical universities by presenting concepts for the development of secure software and procedures to cope with security deficiencies. Both companies have organized joint workshops between the industry and the university sector on secure programming.

Further details about the initiative are provided at the security portal (see link: https://www.sicher-im-netz.de/).
within the Cabinet of the United Kingdom. The service is headed by a Director General of the British Civil Service who is directly supported by an internal security organization, secretariat, legal advisory branch and information services branch. The Deputy DG is responsible for the operational activity of the service, being responsible for four branches: international counter-terrorism, National Security Advice Centre (counter proliferation and counter espionage), Irish and domestic counter-terrorism and technical and surveillance operations. The service is subject to the direction of the Joint Intelligence Committee for intelligence operational priorities and liaises with the SIS, GCHQ, DIS and a number of other bodies within the British government and industrial base. The service is overseen by the Intelligence and Security Committee of Members of Parliament directly appointed by the Prime Minister. Judicial oversight is also vested in the Interception of Communications Commissioner and the Intelligence Services Commissioner. The end of the Cold War resulted in a change in emphasis for the operations of the service, assuming responsibility for the investigation of all Irish republican activity on the mainland and increasing the effort countering other forms of terrorism, particularly in more recent years the more widespread threat of Islamist extremism. In 1996, legislation formalized the extension of the Security Service's statutory remit to include supporting the law enforcement agencies in their work against serious crime. Tasking was reactive, acting at the request of law enforcement bodies. This role has subsequently been passed to the Serious Organized Crime Agency (SOCA).

6.3.2 Secret Intelligence Service

The Secret Intelligence Service (SIS), commonly known as MI6 (Military Intelligence, Section 6) is the United Kingdom's external intelligence agency. Under the direction of the Joint Intelligence Committee (JIC), it works alongside the Security Service (MI5), Government Communications Headquarters (GCHQ) and the Defence Intelligence Staff (DIS). Since 1995, the Secret Intelligence Service has had its headquarters at Vauxhall Cross on the South Bank of the Thames.

The Service is derived from the Secret Service Bureau, which was founded in 1909. It was a joint initiative of the Admiralty and the War Office to control secret intelligence operations in the UK and overseas, particularly concentrating on the activities of the Imperial German government. The Bureau was split into naval and army sections which, over time, specialised in foreign espionage and internal counter-espionage activities respectively. This specialisation was because the Admiralty wanted to know the maritime strength of the Imperial German Navy. This specialisation was formalised before 1914. When World War I started, the two sections underwent administrative changes so that the foreign section became the Directorate of Military Intelligence Section 6 (M16), the name by which it is frequently known in popular culture today. Its first director was Captain Sir George Mansfield Smith-Cumming, who often dropped the "Smith" in routine communication. He typically signed correspondence with his initial "C" in green
ink. This usage evolved as a code name, and has also been used by all subsequent directors of SIS.

Under Director Sinclair, the following sections were created:

- An economic intelligence section, Section VII, to deal with trade, industrial and contraband.

- A clandestine radio communications organisation, Section VIII, to communicate with operatives and agents overseas.

During the Second World War the human intelligence work of the service was amended by the cryptanalytic effort undertaken by the Government Code and Cypher School (GC&CS), the bureau responsible for interception and decryption of foreign communications at Bletchley Park. GC&CS was the source of ULTRA intelligence. ULTRA permitted Allied success in the Battle of the Atlantic.

The end of the Cold War led to a reshuffle of existing priorities. The Soviet Bloc ceased to swallow the lion's share of operational priorities, although the stability and intentions of a weakened but still nuclear-capable Federal Russia constituted a significant concern. Instead, functional rather than geographical intelligence requirements came to the fore such as counter-proliferation (via the agency's Production and Targeting, Counter-Proliferation Section) which had been a sphere of activity since the discovery of Pakistani physics students studying nuclear-weapons related subjects in 1974; counter-terrorism (via two joint sections run in collaboration with the Security Service, one for Irish republicanism and one for international terrorism); counter-narcotics and serious crime (originally set up under the Western Hemisphere Controllerate in 1989); and a 'global issues' section looking at matters such as the environment and other public welfare issues. In the mid-1990s these were consolidated into a new post of Controller, Global and Functional.

6.3.3 CPNI

CPNI (Centre for the Protection of National Infrastructure) is a British national institution affiliated with MI5, the British secret service. The purpose of CPNI is to keep business and the general public informed about threats to the crucial infrastructure. CPNI is formed from the merge of two organisations, namely NISCC (National Infrastructure Security Co-ordination Centre) and NSAC. (The following information has been taken from the CPNI home page http://www.cpni.gov.uk/.)

CPNI advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services (delivered by the communications, emergency services, energy, finance, food, government, health, transport and water sectors) safer. Without these services, the UK could suffer serious consequences, including severe economic damage, grave social
disruption, or even large scale loss of life. CPNI advice is targeted primarily at the critical national infrastructure (CNI) - those key elements of the national infrastructure which are crucial to the continued delivery of essential services to the UK. CPNI is introducing a new mechanism for issuing advisories about computer security incidents. In keeping with CPNI's holistic approach to protective security matters, the new mechanisms will encompass physical and personnel security issues as well.

CPNI advice is targeted primarily at the critical national infrastructure (CNI) - those key elements of the national infrastructure which are crucial to the continued delivery of essential services to the UK. Without these key elements, the essential services could not be delivered and the UK could suffer serious consequences, including severe economic damage, grave social disruption, or even large scale loss of life.

CPNI also has special access to intelligence and information about terrorism and other threats which informs our advice and priorities. CPNI advice is provided to national infrastructure businesses and organisations in a variety of ways, including face-to-face advice through teams of sector based and specialist advisers, training, online information and written advisory products. Our closest relationship is with those organisations which operate the key elements on which essential services depend.

CPNI advice is integrated across the physical, personnel and information security disciplines both in response to user requirements and derived from expert knowledge about how to make the national infrastructure less vulnerable. Many of the counter terrorism measures suggested can also contribute to an effective crime reduction strategy.

The threat from espionage (or spying) against the UK did not end with the collapse of Soviet communism in the early 1990s. Several countries are actively seeking British information and material to advance their own military, technological, political and economic programmes. In the past, espionage activity was typically directed towards obtaining political and military intelligence. This remains the case, but in today's high-tech world, the intelligence requirements of a number of countries also include new communications technologies, IT, genetics, aviation, lasers, optics, electronics and many other fields.

The UK is a high priority espionage target and a number of countries are actively seeking UK information and material to advance their own military, technological, political and economic interests. The threat against UK interests is not confined to the UK itself. A foreign intelligence service operates best in its own country and some may therefore find it easier to target UK interests at home, where they can control the environment and where the UK traveller may let their guard drop.
Terrorism is not just about physical attack. It might take the form of attacks on vital information or communication systems, causing disruption and economic damage. Some attacks are easier to carry out if the terrorist is assisted either directly or indirectly by an 'insider' or by someone with specialist knowledge or access. Terrorism may include threats or hoaxes designed to frighten and intimidate.

There are three strong business reasons why organisations should plan to deter such acts, or at least to minimise their impact. They are:

**Legal obligations**

In the event of an attack, your preparation and contingency plans are likely to come under scrutiny. Although the police and other agencies can offer advice, it is up to the owner or occupier to seek out and act upon that advice. In any subsequent inquiries or court proceedings, you would need to show that you took the relevant legislation into account.

**Business continuity**

Ensure that your business is able to cope with an attack and return to normality as soon as possible. This is particularly important for smaller businesses that may not have the resources to withstand even a few days without trading.

**Loss of reputation**

Your business or organisation will lose its good name if it does not fulfil its legal obligations and/or business continuity plans in the event of a terrorist attack. The resulting loss of reputation may adversely affect your business.

There is limited value in safeguarding your own business premises in isolation. Take into account your neighbours' plans, particularly if you are in a multi-occupancy building. You may also wish to discuss your plans with the emergency services.

Some attacks, whether from criminals, terrorists or competitors seeking a business advantage, may rely upon the co-operation of an insider. This could be an employee or any contract or agency staff (e.g. cleaner, caterer, security guard) who has authorised access to your premises. If an employee, he or she may already be working for you, or may be someone newly joined who has infiltrated your organisation specifically in order to seek information or exploit the access that the job might provide. Almost all physical and electronic attacks can be assisted or conducted by an insider. There are some attacks that can only be committed by insiders, such as the unauthorised release of proprietary information, or the sabotage of assets that only employees can access. In addition, there are some tactics that insiders are likely to use in the course of preparing or conducting their...
attacks; these include manipulation (deliberate attempts to acquire information or access by manipulating staff).

The techniques are often very simple, exploiting basic human tendencies such as the desire to return a favour or to help a colleague in need, but they can be used with damaging effect. Attackers may try to gain information piecemeal over a period of time, asking for small favours or gaining information through seemingly innocent conversation. Determined attackers prepare well, learning about a company's structure and language in advance. They might pretend to be a co-worker, a new employee or a delivery person. They might send emails with attachments containing malicious code or pretend to have lost their computer password.

Methods of defending against this sort of attack include the following:

- provide specific training in detecting manipulative attempts to frontline and customer facing staff.
- warn all staff to be alert to anyone asking for sensitive or restricted information.
- be alert to an unknown enquirer who tries to extract information in a rush, with intimidation, emphasising authority or refusing to give contact details.
- Sabotage is often committed by a former employee seeking revenge on their employer because of a personal grudge caused by a negative work related event such as dismissal. Although it is sometimes planned well in advance, it can also be the result of an opportunistic moment.
- Sabotage does not have to be committed on site, it can be triggered remotely. In most cases, it causes a financial loss to the organisation or damage to its reputation. The following strategies will help to lower the risk of an act of sabotage.
- encourage managers to be alert to individuals who are excessively negative about the organisation or their work.
- establish a formal grievance procedure for staff to vent their feelings.
- set up an easy and confidential system for staff to report any abnormal behaviour from their colleagues.
- back up your information, preferably keeping a secure copy in another location.
- when employment is terminated - for whatever reason - ensure that all access to systems, sites and information is ended.
- ensure you have polices and procedures in place to prevent attack by remote access.
- protecting information is a vital part of every security effort whether that information is held electronically or by other means. Efficient businesses rely on the confidentiality, integrity and availability of their data. Security professionals need to ask.
- can someone read this information?
can they change it? And,
• can they prevent me or my customers from reading it?

CPNI actively promotes information sharing to best address the threat from an electronic attack against information systems. As part of this policy, CPNI issues a variety of documents as a means of improving security awareness and practices. A full listing of these documents can be found in their Products and Services section. The sharing of information about the risks facing networks is self evidently beneficial to both government and industry. If a mechanism can exist through which one company can learn from the experiences, mistakes, and successes of another, without fear of exposing company sensitivities to competitors and the media, then every participant can improve their level of assurance.

This mechanism, called an Information Exchange, is based upon the personal trust of representatives, sharing information in a confidential meeting, run under a version of the 'Chatham House Rule'. Trust is built up slowly; representatives at Information Exchanges are expected to attend all meetings, which are held every two months. Meeting face-to-face, they are building up a trusted, relatively small community with a common interest. Each organisation can put forward a maximum of two representatives, and cannot send substitutes to attend; a stranger turning up at a meeting would inhibit the sharing of sensitive information.

**WARPs**

A WARP (Warning, advice and reporting point) is a community based service for sharing up-to-date advice on information security threats, incidents and solutions. WARPs were developed by CPNI (former NISCC) as part of its Information Sharing Strategy in recognition of the need to provide a cost-effective way to facilitate information security among a diverse range of organisations, many of which form part of the CNI.

A WARP works because its membership is a community, based on geography, technology, business need or another area of common interest. On the ground, this means that a security concern of one member is probably a concern of the other members and their WARP is the most effective way of sharing information between them.

There is a growing trend for electronic devices and systems to be connected through a variety of networks. There are also increasing commercial pressures for disparate company networks to be inter-connected, often using the Internet. These pressures expose both corporate and operational information to increasing threats of electronic attack on systems previously held to be secure.

**SCADA technology**
SCADA is the acronym for Supervisory Control And Data Acquisition. SCADA is any system that performs supervisory control and data acquisition, independent of its size or geographical distribution. SCADA systems are typically used to perform data collection and control at the supervisory level. Some SCADA systems only monitor without doing control, these systems are still referred to as SCADA systems. The process under supervision can be industrial, infrastructure or facility based as described below:

- Industrial processes include: manufacturing/production/power generation/fabrication/refining - continuous, batch, repetitive or discrete.

- Infrastructure processes may be public or private and include: water treatment and distribution, wastewater collection and wastewater treatment, oil & gas pipelines, electrical power transmission and distribution and large communication systems.

- Facility processes in private or public facilities including: buildings, airports, ships or space stations in order to monitor and control: HVAC, access control, energy consumption management.

The SCADA systems for these applications all perform Supervisory Control And Data Acquisition, even though the use of the systems are very different. Recently, the security of SCADA-based systems has come into question as they are increasingly seen as extremely vulnerable to cyberwarfare/cyberterrorism attacks on several fronts. In particular, security researchers are concerned about:

- the lack of concern about security and authentication in the design, deployment and operation of existing SCADA networks,
- the mistaken belief that SCADA systems have the benefit of security by obscurity through the use of specialized protocols and proprietary interfaces,
- the mistaken belief that SCADA networks are secure because they are supposedly physically secured,
- the mistaken belief that SCADA networks are secure because they are supposedly disconnected from the Internet.

The mission critical nature of a large number of SCADA systems, such attacks could, in a worst case scenario, cause massive financial losses through loss of data or actual physical destruction, misuse or theft, even loss of life, either directly or indirectly. Whether such concerns will cause a move away from the use of existing SCADA systems for mission critical applications towards more secure architectures and configurations remains to be seen, given that at least some influential people in corporate and governmental circles believe that the benefits and lower initial costs of SCADA based systems still outweigh potential costs and risks. Recently, multiple security vendors, such as Check Point and Innominate...
have begun to address these risks by developing lines of specialized industrial
firewall and VPN solutions for TCP/IP-based SCADA networks.

Strong links forged with network operators, infrastructure-owners and end users enable CPNI to
deliver authoritative and timely advice. Almost all critical industrial infrastructures
and processes are managed remotely from central control rooms, using
computers and communications networks. The flow of gas and oil through pipes;
the processing and distribution of water; the management of the electricity grid;
the operation of chemical plants; and the signalling network for railways. These all
use various forms of process control or 'supervisory control and data acquisition' -
SCADA technology.

Until recently, the term SCADA was unknown outside its niche area in industry.
Today it is one of the key issues for infrastructure protection.

CPNI is helping the CNI to understand and mitigate electronic attack risks to
SCADA systems and has developed globally-recognised expertise on SCADA
security. The CPNI SCADA program includes:

- CPNI-funded vulnerability and protection research;
- SCSIE, a confidential industry-CPNI forum that meets regularly to exchange
  information on SCADA threats, incidents and mitigation;
- a close working relationship to the SCADA programs being developed in USA,
  Canada, Australia, New Zealand and Europe.

An operating system is a software interface between the hardware and the user.
There are three characteristics of good system security: identity and
authentication; access control; and audit and accountability. This security can be
applied in two stages; during design of the system and by configuring the system
(a process also known as hardening). Securing any system is an ongoing
commitment and should form part of routine maintenance. The following
documents have been issued to assist in securing systems. Applications are pieces
of software performing specific tasks. It is essential to understand that they do not
exist in a vacuum and their security must be considered in the environment they
inhabit. There are two considerations of application security: internal security, if the
application fails, does it do so in a safe manner; and the relationship with the
computer it operates on, does it require excessive privileges? CPNI works on many
levels to protect the nation's national infrastructure (NI) from attack. Its experts
produce a range of up-to-date publications designed to mitigate the risks faced by
the operators of the NI.

Research and Development (R&D) Programme

CPNI conducts a Research and Development (R&D) Programme to provide the
technical knowledge to underpin the timely delivery of authoritative electronic
security advice to protect the UK's critical national infrastructure against national
security threats. CPNI works with partners to enhance future capability.
The UK critical infrastructure relies upon a huge range and complex mix of different technologies and cultural factors. CPNI needs access to expertise in all these areas to understand their vulnerabilities, dependencies and how to use the technology securely in context.

The research and development programme has four strands:

- internal expertise
- technology watch and dissemination
- outreach and cooperation
- academic research

The security implications of living in an electronically integrated world raise inter-dependency issues related to SCADA and Process Control systems, and Next Generation Networks. Such technologies require security research in the areas of:

- system security engineering
- vulnerability discovery and remediation
- real-time malicious code identification
- network forensics
- inter-dependency modelling
- trust in networking communities

The Physical & Personnel Research programme is funded and managed by CPNI and operates through a range of research and development suppliers. The programme does not tend to issue open calls for tenders, but if you are a research and development organisation operating in our area of interest they, would be happy to talk to you.

The Physical & Personnel Research and development programme operates by:

- commissioning basic research to develop technical knowledge, tools, techniques, standards and equipment to address national security threats in key priority areas,
- development of security standards for physical security equipment and installation,
- practical evaluation of commercially available off-the-shelf equipment,
- horizon-scanning to identify emerging technologies for security applications,
- building partnerships to leverage funding and burden share with others,
- The programme covers the following areas,
- human factors - for example, biometrics, human behaviour, design of systems,
- electronics and control systems - for example, detection and vision systems, access control, multi-sensor networks, in-vehicle systems, SCADA, and so on,
- structural - for example, ballistics and blast, physical barriers, containers and doors, design, air flow,
screening and detection - for example, explosives, weapons, chemical, biological and radiological materials.

Protecting an organisation's information is the responsibility of all staff, and to be fully effective, it requires regular security training to help staff guard against attacks on information. Sometimes deliberate attempts are made to acquire information or access by manipulating staff by using a range of influencing techniques. This is sometimes described as 'social engineering', creating situations in which someone will willingly provide access to information, sites or systems to someone unauthorised to receive it. Customer facing personnel who have been trained to be helpful and informative can be particularly vulnerable to such attacks (for example receptionists, IT helpdesk staff).

6.3.4 Dstl - Defence Science and Technology Laboratory

Established: July 2, 2001
Acting Chief Executive: Frances Saunders
Turnover: £353.3 million (2004/5)
Operating Profit: £18.5 million (2004/5)
Employees: 3,328 employees (March 2005)

The Defence Science and Technology Laboratory (Dstl) is an Executive Agency of the UK Ministry of Defence (MOD). It operates as a Trading Fund, owned by the Secretary of State for Defence.

Its stated mission is "to create the winning edge for UK forces and government through the best use of science and technology". Its stated vision is "to be the indispensable source of science and technology at the heart of defence".

Dstl carries out a broad range of work from high-level analysis in support of policy and procurement decisions, to research in areas such as biomedical science and electronics, alongside operational work such as forensic analysis of explosives.

In July 2001, the Defence Evaluation and Research Agency (DERA) was split into two parts. Dstl was established to carry out science and technology work that is best done within government, while the majority was transferred to the part-privatised QinetiQ.

Organisation

Dstl is a Trading Fund within the Ministry of Defence —it is responsible for managing its own budget, funded by contracts for specific work. Most funding comes from the Ministry of Defence, although a small portion comes from other government departments and commercial sources. According to 2004/5 figures, around 88% of Dstl's income comes from MOD. The remaining 12% of income
comes from other government departments (45%) and non-exchequer sources, including QinetiQ and foreign governments (55%).

Dstl consists of the following departments:

- Environmental Sciences
- Detection
- Physical Sciences
- Biomedical Sciences
- Sensors and countermeasures
- Energetics
- Electronics
- Policy and Capability Studies
- Naval Systems
- Land Battlespace Systems
- Air and Weapons Systems
- Joint Systems
- Information Management
- Knowledge Services

Locations

Dstl currently has a number of establishments at sites including:

- Alverstoke, Hampshire
- Bedford, Bedfordshire
- Farnborough, Hampshire
- Fort Halstead, Kent
- Malvern, Worcestershire
- Pershore, Worcestershire
- Porton Down, Wiltshire
- Portsdown West, Hampshire
- Winfrith, Dorset

It is currently consolidating to three core sites: Fort Halstead, Porton Down, and Portsdown West, under a project known as "INSPIRE", due to complete in 2009.

The Chief Executive from 2001 to 2006 was Martin J Earwicker. The position is presently vacant (May 2007), with Frances Saunders currently acting as Chief Executive.

Ploughshare Innovations
In April 2005, the technology transfer company Ploughshare Innovations Ltd. was formed. This company has the mission statement "To actively pursue the commercial exploitation of publicly funded research for the benefit of all". The purpose of Ploughshare Innovations Ltd. is to commercialise on the intellectual property developed within Dstl (predominantly from MOD funded defence science research), using a similar business model to the commercial activities of QinetiQ.

6.3.5 CESG

CESG is the Information Assurance (IA) arm of GCHQ and is based in Cheltenham, Gloucestershire, UK. It is the UK Government’s National Technical Authority for IA, responsible for enabling secure and trusted knowledge sharing to help their customers achieve their business aims. (The following information has been taken from the CESG home page http://www.cesg.gov.uk/.)

CESG has existed in one form or another for the past 80 years. Its origins grew out of the dangers inherent in poor radio communications security that became apparent during World War I. As a result of severe security compromises that were experienced by British forces during that war, the British government decided to set up a special organisation both to study the methods of cipher communications of foreign powers and to advise on the security of British codes and ciphers.

In 1919, following a Cabinet decision, the Government Code and Cipher School (GC&CS) was established (which was later to become the Government Communications Headquarters (GCHQ)). The GC&CS was originally set up under the civil administration of the Admiralty, but with the decline in military signal traffic after the end of World War I, it was then placed under the administrative responsibility of the Foreign Office in 1922.

The communications security part of the GC&CS could only advise on the use of the various cipher systems, but had no authority to mandate government departments or the services to use those ciphers and procedures which were really secure. This weakness was recognised during World War II, and in 1944 clearer lines of authority were established, with the communications security section of the GC&CS becoming responsible to a Cipher Policy Board.

In the early 1950s, a review of the Cipher Policy Board's organisation and terms of reference led to the creation of a new agency, the London Communications Security Agency (LCSA). The LCSA now had its own Director but still remained administratively under what was by then GCHQ.

In 1965, the LCSA became the Communications-Electronics Security Department (CESD), still based primarily in London, although parts were now co-located with
GCHQ in Cheltenham, Gloucestershire. In 1969, CESD formally merged organisationally with GCHQ and was renamed the Communications-Electronics Security Group (CESG). In 1978, the last London elements of CESG moved to Cheltenham, Gloucestershire, where it has remained to the present.

One of the more significant changes to CESG since the late 70's has been the move to operating on a cost-recovery basis, rather than being funded directly by central government. Since 1997, CESG now charges for most of the information security/information assurance services it offers.

Today, Government turns to CESG as its National Technical Authority for advice and services to protect its voice and data networks. In this network enabled environment, Communications-Electronics Security no longer adequately describes the full extent of the organisations work, so in 2002 it was decided to drop the expanded name. The title CESG was retained as it has an excellent reputation as an independent technical organisation with a critical role in keeping the Government’s IT systems safe.

In October 2003, CESG moved into the new GCHQ/CESG accommodation, which co-locates both under one roof for the first time in the history of both organisations.

What is Information Assurance?

There is little information that exists that will not at one time or another be stored or transmitted electronically. Information on paper as soon as it is faxed or input into a computer, enters the electronic world. From here the information can be changed, deleted or broadcast to the world.

Electronic information must be readily available when needed and trusted to be accurate. Sometimes there are confidentiality concerns. Ensuring the confidentiality, availability and integrity of all electronically held information is the goal. "Information Assurance" is the term we use to describe this goal.

Through the use of appropriate security products and procedures, it is hoped to achieve reasonable assurance that electronic information is adequately protected from unauthorised change or dissemination and ensure the information is always available.

Helping the owners of electronic information to determine the products and procedures to achieve Information Assurance is what CESG is here for. CESG aims to protect and promote the vital interests of the UK by providing advice and assistance on the security of communications and electronic data. They deliver information assurance policy, services, and advice that government and other customers need to protect vital information services. They work on a cost recovery...
basis for all customer-specific solutions and services, though IA Policy and Guidance documentation is usually free of charge to the UK official community. With experience acquired over decades of working with customers on projects and problems, CESG is well qualified to give you authoritative advice on assessing current and foreseeable risks. Specific services include:

Technical Advice
- Initial technical advice on design options for secure IT architectures
- In-depth technical consultancy on specific Information Assurance (IA) issues
- Help with interpreting national security standards such as BS7799
- Guidance on the use and deployment of cryptographic and other certified IA products
- Advice on algorithm use and suitability

Documentation
- Production of system security documentation (SSP, SyOPs etc)
- Advice on sources and status of technical documentation
- Verbal and written feedback on technical documentation

Other Services
- Assignment of an adviser to attend meetings and provide continuity of advice throughout a project's life
- Information on suppliers of approved / certified products
- Help-desk style telephone advice
- Access to alternative sources of technical advice
- Training on specific Information Assurance issues

Their core clientele are HMG's many central government departments and agencies and the Armed Forces. However, they also provide services to bodies in the wider public sector and to various private sector companies. These include local government, the health sector, law enforcement. They work closely with the Security Service by providing technical IA expertise as they support the essential services forming the Critical National Infrastructure, such as power and water, without which the country would stop working.
7 Appendix

7.1 Evaluation of EU-projects NESSIE and eSTREAM

The five already publicly known, but not formally submitted to the project, are marked with a "*". Most may be used by anyone for any purpose without needing to seek a patent license from anyone; a license agreement is needed for those marked with "#", but the licensors of those have committed to "reasonable non-discriminatory license terms for all interested", according to a NESSIE project press release. In a first phase, an open call for the submission of cryptographic primitives as well as for evaluation methodologies for these primitives is published. This call includes a request for the submission of block ciphers (as for the AES call), but also of other cryptographic primitives including hash functions, additive stream ciphers, and digital signature algorithms. In addition, it asks for evaluation methodologies for these primitives. The scope of the call is defined together with the project industry board. This call has been published in March 2000. In parallel, a software toolbox will be developed for generic and, later on, specific evaluations of primitives, taking into account the submitted testing methodologies. A first part of the security evaluation will consist of an analysis of the AES finalists, resulting in joint comments towards NIST (US). Next, the evaluation of submitted primitives will start off with a fast screening of the submissions followed by a first evaluation. In parallel, a first performance evaluation will be executed, only implementing critical parts of the algorithms. Based on this evaluation, a set of submissions will be shortlisted (finalists). The second phase of the project will consist of a thorough security evaluation of the finalists, combined with a performance evaluation that will produce realistic performance estimates of optimised implementations (including software, hardware, and smart card). This will allow for comparing the speed of the primitives on a fair and equal basis. The final results (a recommended portfolio of cryptographic primitives) will be widely disseminated and entered into the relevant standardisation bodies.

The NESSIE evaluation process is an open process. Thus as part of the evaluation process, the NESSIE project welcomes comments about both submitted primitives and the evaluation process. To facilitate this process, four NESSIE workshops will be organised. The first took place on 13-14 November 2000, shortly after the deadline for submission of primitives. The second workshop took place on 12-13 September 2001, shortly after the end of the first phase of the project, the third workshop took place on 6-7 November 2002, and the fourth workshop takes place on 26-27 February 2003 (jointly with the STORK project). A timetable for the NESSIE project is given below.
The project may recommend a different block cipher than AES (if technical reasons support this), and will recommend primitives that can be used for challenging environments such as Gigabit networking, wireless communications, PDAs, and smart cards. The recommended primitives for digital signatures can support the European Electronic Signature Standardisation Initiative. By-products of the process will be an evaluation methodology and the improvement of the state-of-the-art in the area. The project will build consensus within the European security industry and gather support for the standardisation effort through a project industry board and through the 5th Framework programme. Members of the project industry board are: Algorithmic Research (Israel), Amtec SpA (I), Baltimore Technologies (IRL), Cryptomathic (DK), Deutsche Telekom AG (D), Entrust Technologies (CH), Ericsson Radio Systems AB (SE), Europay International (B), Gemplus (F), Hewlett-Packard Laboratories (UK), Isabel (B), KPN Research (NL), NDS (Israel), Nokia (Finland), Oberthur Card Systems (F), RSA Laboratories Europe (SE), Security Design International (UK), STMicroelectronics (F), S.W.I.F.T. (B), Telenor Research (N), Telsy Elettronica SpA (I), Thomson-CSF (F), Thomson Multimedia (F), Utimaco (D), Vodafone (UK), Zaxus (UK).

Expected achievements and impact:

- to publish an open call for cryptographic primitives and testing methodologies, and to solicit submissions;
- to provide joint comments on the AES finalists;
- to select from the submitted primitives a recommended subset; the main criterion for the selection process will be based on security and requirements of applications; other criteria will include performance, and flexibility. It will consist of two phases: preliminary screening and first evaluation and secondly thorough evaluation;
- to develop a methodology for security and performance evaluation of primitives;
- to disseminate results through four open workshops (one near the end of the first year, one half-way the project, one at the end of year 3, and one at the end of the project) and scientific publications;
- to build consensus within a project industry board, that will be consulted on a regular basis;
- to input results to standardisation bodies;
- to meet emerging generic security requirements of global networks and ubiquitous embedded systems, taking into account scalability requirements.

None of the six stream ciphers submitted to NESSIE were selected since every one fell to cryptanalysis. This surprising result led to the eSTREAM project.

Block ciphers

- MISTY1: Mitsubishi Electric
- Camellia: Nippon Telegraph and Telephone and Mitsubishi Electric
- SHACAL-2: Gemplus
- AES*: (Advanced Encryption Standard) (NIST, FIPS Pub 197) (aka Rijndael)

Public-key encryption

- ACE Encrypt#: IBM Zurich Research Laboratory
- PSEC-KEM: Nippon Telegraph and Telephone Corp
- RSA-KEM*: (draft of ISO/IEC 18033-2)

MAC algorithms and cryptographic hash functions

- Two-Track-MAC: Katholieke Universiteit Leuven and debis AG
- UMAC: Intel Corp, Univ. of Nevada at Reno, IBM Research Laboratory, Technion Institute, and Univ. of California at Davis
- CBC-MAC*: (ISO/IEC 9797-1)
- HMAC*: (ISO/IEC 9797-1)
- WHIRLPOOL: Scopus Tecnologia S.A. and K.U.Leuven
- SHA-256*, SHA-384* and SHA-512*: NSA, (US FIPS 180-2)

Digital signature algorithms

- ECDSA #: Certicom Corp
- RSA-PSS: RSA Laboratories
- SFLASH: Schlumberger Corp

Identification schemes

- GPS-auth: Ecole Normale Supérieure, France Télécom, and La Poste

eSTREAM

eSTREAM is a project to identify "new stream ciphers that might become suitable for widespread adoption", organised by the EU ECRYPT network. It was set up as a result of the failure of all six stream ciphers submitted to the NESSIE project. The call for primitives was first issued in November 2004. The project is due to complete in May 2008. The project is divided into separate phases and the project goal is to find algorithms suitable for different application profiles.

Profiles

The submissions to eSTREAM fall into either or both of two profiles:

- Profile 1: "Stream ciphers for software applications with high throughput requirements"
Profile 2: "Stream ciphers for hardware applications with restricted resources such as limited storage, gate count, or power consumption."

Both profiles contain an "A" subcategory (1A and 2A) with ciphers that also provide authentication in addition to encryption. The evaluation is given in what follows.

Phases

Phase 1

Phase 1 included a general analysis of all submissions with the purpose of selecting a subset of the submitted designs for further scrutiny. The designs were scrutinized based on criteria of security, performance (with respect to the block cipher standard AES, as well as the other candidates), simplicity and flexibility, justification and supporting analysis, and clarity and completeness of the documentation. Submissions in Profile 1 were only accepted if they demonstrated software performance superior to AES-128 in counter mode.

The Phase 1 activities included a large amount of analysis and presentations of analysis results as well as discussion. Also the project developed a framework for testing the performance of the candidates. The framework was then used to benchmark the candidates on a wide variety of systems.

Phase 2

On 27 March 2006 the eSTREAM project officially announced the end of Phase 1. On 1 August 2006 Phase 2 was officially started. For each of the profiles a number of algorithms have been selected to be Focus Phase 2 algorithms. These are designs that eSTREAM finds of particular interest and encourages more cryptanalysis and performance evaluation on these algorithms. Additionally a number of algorithms for each profile are accepted as Phase 2 algorithms, meaning that they are still valid as eSTREAM candidates. The Focus 2 candidates will be re-classified every six months.

Phase 3

Phase 3 started in April 2007. Candidates for Profile 1 (Software) are CryptMT (Version 3), Dragon, HC (HC-128 and HC-256), LEX (LEX-128, LEX-192 and LEX-256), NLS (NLSv2, encryption only not authentication), Rabbit, Salsa20 and SOSEMANUK. Candidates for Profile 2 (Hardware) are DECIM (DECIM v2 and DECIM-128), Edon80, F-FCSR (F-FCSR-H v2 and F-FCSR-16), Grain (Grain v1 and Grain-128), MICKEY (MICKEY 2.0 and MICKEY-128 2.0), Moustique, Pomaranch (Version 3) and Trivium.

Submissions
<table>
<thead>
<tr>
<th>Key</th>
<th>Cipher Description</th>
<th>Phase</th>
<th>Authors/Inventors</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>a &quot;Focus Phase 2&quot; cipher</td>
<td>3</td>
<td>Makoto Matsumoto, Hagita Mariko, Takuji Nishimura and Matsuo Saito</td>
</tr>
<tr>
<td>2</td>
<td>A &quot;Phase 2&quot; cipher</td>
<td>3</td>
<td>Come Berbain, Olivier Billet, Anne Canteaut, e.a.</td>
</tr>
<tr>
<td>3</td>
<td>A &quot;Phase 3&quot; cipher</td>
<td>3</td>
<td>Ed Dawson, Kevin Chen, Matt Henricksen, e.a.</td>
</tr>
<tr>
<td>A</td>
<td>An &quot;archived&quot; cipher</td>
<td>3</td>
<td>Danilo Gligoroski, Smile Markovski, Ljupco Kocarev e.a.</td>
</tr>
<tr>
<td>M</td>
<td>Includes a MAC</td>
<td>3</td>
<td>Thierry Berger, François Arnault e.a.</td>
</tr>
<tr>
<td>P</td>
<td>Patented</td>
<td>3</td>
<td>Martin Hell, Thomas Johansson and Willi Meier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Alex Biryukov</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Steve Babbage and</td>
</tr>
</tbody>
</table>

Selected as Phase 3 candidates:
<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Analysis Function in the EU Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>MICKEY-128 2.0)</td>
<td>Matthew Dodd</td>
</tr>
<tr>
<td>MOSQUITO (aka Moustique)</td>
<td>Joan Daemen and Paris Kitsos</td>
</tr>
<tr>
<td>NLS (NLSv2, encryption-only)</td>
<td>Gregory Rose, Philip Hawkes, Michael Paddon e.a.</td>
</tr>
<tr>
<td>Pomaranch (Version 3)</td>
<td>Cees Jansen and Alexander Kolosha</td>
</tr>
<tr>
<td>Rabbit</td>
<td>P Martin Boesgaard, Mette Vesterager, Thomas Christensen</td>
</tr>
<tr>
<td>Salsa20</td>
<td>Daniel Bernstein</td>
</tr>
<tr>
<td>SOSEMANUK</td>
<td>Come Berbain, Olivier Billet, Anne Canteaut, e.a.</td>
</tr>
<tr>
<td>Trivium</td>
<td>Christophe De Cannière and Bart Preneel</td>
</tr>
</tbody>
</table>
8 References


[EUP DR] Draft report of the EU parliament on “Time to move up a gear - Creating a Europe of entrepreneurship and growth”, August 2006


[IPA 07-1] SIT Fraunhofer Study for IPA on “Current Status of Software Vulnerability Handling Scheme in the EU Region”, February 2007


9 Contact Information and Links

This chapter contains a set of pairs of tables with each pair for a specific country or supra-national organization that provides links for distinct objectives and organizations, and contact information respectively.

Table 5: International Links

<table>
<thead>
<tr>
<th>ORGANIZATION OR TOPIC</th>
<th>ACRONYM OR LOGO</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIRST Forum of Incident Response and Security Teams</td>
<td>first</td>
<td><a href="http://www.first.org/">http://www.first.org/</a></td>
</tr>
<tr>
<td>ISO International Standardization Organization</td>
<td>ISO</td>
<td><a href="http://www.iso.org">http://www.iso.org</a></td>
</tr>
<tr>
<td>ITU International Telecommunication Union</td>
<td>ITU</td>
<td><a href="http://www.itu.int/home">http://www.itu.int/home</a></td>
</tr>
<tr>
<td>OECD, Organisation for Economic Co-operation and Development</td>
<td>OECD</td>
<td><a href="http://www.oecd.org/">http://www.oecd.org/</a></td>
</tr>
</tbody>
</table>

Table 6: European Links

<table>
<thead>
<tr>
<th>ORGANIZATION OR TOPIC</th>
<th>ACRONYM OR LOGO</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORGANIZATION OR TOPIC</td>
<td>ACRONYM OR LOGO</td>
<td>LINK</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>----------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Business Incubators</td>
<td></td>
<td><a href="http://cordis.europa.eu/incubators/">http://cordis.europa.eu/incubators/</a></td>
</tr>
<tr>
<td>Collective Research network</td>
<td></td>
<td><a href="http://www.cornet-era.net/">http://www.cornet-era.net/</a></td>
</tr>
<tr>
<td>European Law</td>
<td></td>
<td><a href="http://europa.eu.int/eur-lex/en/oj">http://europa.eu.int/eur-lex/en/oj</a></td>
</tr>
<tr>
<td>ECSIRT European CSIRT Network</td>
<td></td>
<td><a href="http://www.ecsirt.net/">http://www.ecsirt.net/</a></td>
</tr>
<tr>
<td>EISPP European Information Security Promotion Program</td>
<td></td>
<td><a href="http://www.eispp.org">http://www.eispp.org</a></td>
</tr>
<tr>
<td>Enhanced Competitiveness and Co-operation through</td>
<td></td>
<td><a href="http://www.gcom.ie/ecitt/projdesc.htm">http://www.gcom.ie/ecitt/projdesc.htm</a></td>
</tr>
<tr>
<td>Information Technology and Telecommunications (ECITT)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ENISA European Network and Information Security Agency</td>
<td></td>
<td><a href="http://www.enisa.eu.int/">http://www.enisa.eu.int/</a></td>
</tr>
<tr>
<td>EU Gateway to Japan</td>
<td></td>
<td><a href="http://www.gatewaytojapan.org">http://www.gatewaytojapan.org</a></td>
</tr>
<tr>
<td>EUREKA</td>
<td></td>
<td><a href="http://www.eureka.be">www.eureka.be</a></td>
</tr>
<tr>
<td>EuroISPA European Internet Services Providers Association</td>
<td></td>
<td><a href="http://www.euroispa.org/">http://www.euroispa.org/</a></td>
</tr>
<tr>
<td>Europe direct</td>
<td></td>
<td><a href="http://europa.eu.int/europedirect/index_en.htm">http://europa.eu.int/europedirect/index_en.htm</a></td>
</tr>
<tr>
<td>Organization or Topic</td>
<td>Acronym or Logo</td>
<td>Link</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------</td>
<td>------</td>
</tr>
<tr>
<td>Europe direct information about the EU</td>
<td><img src="http://ec.europa.eu/europedirect/" alt="Europe Direct Logo" /></td>
<td><a href="http://ec.europa.eu/europedirect/">http://ec.europa.eu/europedirect/</a></td>
</tr>
<tr>
<td>Joint Research Centre</td>
<td><img src="http://www.jrc.cec.eu.int/" alt="Joint Research Centre Logo" /></td>
<td><a href="http://www.jrc.cec.eu.int/">http://www.jrc.cec.eu.int/</a></td>
</tr>
<tr>
<td>Public Procurement</td>
<td><img src="http://simap.eu.int/" alt="SIMAP Logo" /></td>
<td><a href="http://simap.eu.int/">http://simap.eu.int/</a></td>
</tr>
<tr>
<td>SOLVIT network</td>
<td><img src="http://europa.eu.int/solvit/site/info/index_en.htm" alt="SOLVIT Logo" /></td>
<td><a href="http://europa.eu.int/solvit/site/info/index_en.htm">http://europa.eu.int/solvit/site/info/index_en.htm</a></td>
</tr>
<tr>
<td>Your Europe legal rights as an EU citizen or family member and as a business</td>
<td><img src="http://ec.europa.eu/youreurope/" alt="Your Europe Logo" /></td>
<td><a href="http://ec.europa.eu/youreurope/">http://ec.europa.eu/youreurope/</a></td>
</tr>
</tbody>
</table>
Table 7: Contact Information about European Organizations

<table>
<thead>
<tr>
<th>ORGANIZATION</th>
<th>PHONE</th>
<th>FAX</th>
<th>ADDRESS / E-MAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENISA European Network Information Security Agency</td>
<td>+30 28 1039 1280</td>
<td>+30 28 1039 1410</td>
<td>ENISA - European Network and Information Security Agency, PO Box 1309, 710 01, Heraklion, Greece, <a href="mailto:info@enisa.eu.int">info@enisa.eu.int</a></td>
</tr>
<tr>
<td>EU Gateway to Japan</td>
<td>+32 2 282 08 70</td>
<td>+32 2 230 00 38</td>
<td><a href="mailto:gatewaytojapan@eurochambres.eu">gatewaytojapan@eurochambres.eu</a></td>
</tr>
<tr>
<td>EUREKA</td>
<td>+32 2 777 09 63</td>
<td></td>
<td>EU REKA Secretariat, Brussels, <a href="mailto:sally.horspool@es.eureka.be">sally.horspool@es.eureka.be</a></td>
</tr>
<tr>
<td>European Commission Internal Market Directorate General SOLVIT</td>
<td></td>
<td></td>
<td>B, 1049 Bruxelles, Belgium, <a href="mailto:solvit@ec.europa.eu">solvit@ec.europa.eu</a></td>
</tr>
<tr>
<td>OSHA European Agency for Safety and Health at Work</td>
<td>+34 944 794 36</td>
<td>+34 944 794 383</td>
<td>The European Agency for Safety and Health at Work, Gran Via 33 E-48009 Bilbao, Spain <a href="mailto:information@osha.europa.eu">information@osha.europa.eu</a></td>
</tr>
</tbody>
</table>

Table 8: Japanese Links

<table>
<thead>
<tr>
<th>ORGANIZATION OR TOPIC</th>
<th>ACRONYM OR LOGO</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPA Information-technology Promotion Agency</td>
<td>IPA</td>
<td><a href="http://www.ipa.go.jp/security/index-e.html">http://www.ipa.go.jp/security/index-e.html</a></td>
</tr>
<tr>
<td>JPCERT/CC Japan Computer Emergency Response Team Coordination Center</td>
<td>JPCERT/CC</td>
<td><a href="http://www.jpcert.or.jp/english/">http://www.jpcert.or.jp/english/</a></td>
</tr>
</tbody>
</table>
### French Links

<table>
<thead>
<tr>
<th>Organization or Topic</th>
<th>Acronym or Logo</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFNOR Standardization Body</td>
<td><img src="http://www.afnor.fr/portail.asp" alt="AFNOR Logo" /></td>
<td><a href="http://www.afnor.fr/portail.asp">http://www.afnor.fr/portail.asp</a></td>
</tr>
<tr>
<td>Industrial relationships Regulation</td>
<td><img src="http://www.industrie.gouv.fr" alt="Industrial Relations Logo" /></td>
<td><a href="http://www.industrie.gouv.fr">http://www.industrie.gouv.fr</a></td>
</tr>
<tr>
<td>CertIST CERT Organization</td>
<td><img src="http://www.certist.com" alt="CertIST Logo" /></td>
<td><a href="http://www.certist.com">http://www.certist.com</a></td>
</tr>
<tr>
<td>CERT-LEXSI CERT Organization</td>
<td><img src="http://www.lexsi.com" alt="CERT-LEXSI Logo" /></td>
<td><a href="http://www.lexsi.com">http://www.lexsi.com</a></td>
</tr>
</tbody>
</table>
Table 10: Contact Information about French Organizations

<table>
<thead>
<tr>
<th>ORGANIZATION</th>
<th>PHONE</th>
<th>FAX</th>
<th>ADDRESS / E-MAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFNOR Association Française de Normalisation</td>
<td>+33 1 42 91 5555</td>
<td>+33 1 42 91 5656</td>
<td>Tour Europe, 92049 Paris La Défense Cedex 7</td>
</tr>
<tr>
<td>CERTA Computer Emergency Response Team</td>
<td>+33 1 71 7584 50</td>
<td>+33 1 71 7584 70</td>
<td>SGDN/DCSSI/CERTA 51, boulevard de La Tour-Maubourg, 75700 Paris, France</td>
</tr>
<tr>
<td>Cert:IST CERT Industries, Services &amp; Tertiary</td>
<td>+33 5 3435 3388</td>
<td>+33 5 3435 3389</td>
<td>Cert:IST, C/O Alcatel CIT26 avenue JF Champollion, BP 63576, F-31035 Toulouse Cedex 1 France</td>
</tr>
<tr>
<td>CERT-LEXSI</td>
<td>+33 1 5586 8214</td>
<td>+33 1 5586 8889</td>
<td>CERT-LEXSI, 12, 16 rue de Vincennes, 93100 MONTREUIL, France</td>
</tr>
<tr>
<td>DCSSI Central Directorate for Information System Security</td>
<td>+33 1 41 463720</td>
<td>+33 1 41 463701</td>
<td>18, rue du Docteur Zamenhof 92 131 Issy-Les-Moulineaux, France</td>
</tr>
<tr>
<td>Fonds de développement des PMI FDPMI</td>
<td>+ 33 1 43 19 36 36</td>
<td></td>
<td>Secrétariat d'état à l'Industrie DAR-PMI, 20 avenue de Ségur, 75353 Paris SP 07,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>France</td>
</tr>
<tr>
<td>Ministry of Economics, Finance and Industry</td>
<td>+33 1 44 87 12 23</td>
<td>+33 1 44 87 12 96</td>
<td>Ministère de l'économie et des Finances Secrétariat Général du Comité Interministériel, 2 Boulevard Diderot 75572 Cedex 12 Paris, France, <a href="mailto:solvit@sgae.gouv.fr">solvit@sgae.gouv.fr</a></td>
</tr>
<tr>
<td>Renater CERT</td>
<td>+33 1 5394 2044</td>
<td>+33 1 5394 2031</td>
<td>c/o ENSAM 151 boulevard de l'Hôpital, 75013 Paris, France</td>
</tr>
</tbody>
</table>

Table 11: German Links

<table>
<thead>
<tr>
<th>ORGANIZATION OR TOPIC</th>
<th>ACRONYM OR LOGO</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>BITKOM IT Industry Organization</td>
<td><img src="http://www.bitkom.org/" alt="BITKOM" /></td>
<td><a href="http://www.bitkom.org/">http://www.bitkom.org/</a></td>
</tr>
<tr>
<td>ORGANIZATION OR TOPIC</td>
<td>ACRONYM OR LOGO</td>
<td>LINK</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------</td>
<td>------</td>
</tr>
<tr>
<td>BMI</td>
<td>Federal Ministry of the Interior</td>
<td><a href="http://www.bmi.bund.de">http://www.bmi.bund.de</a></td>
</tr>
<tr>
<td>BSI</td>
<td>Federal Office for Information Security, GER</td>
<td><a href="http://www.bsi.bund.de/">http://www.bsi.bund.de/</a></td>
</tr>
<tr>
<td>Bürger-CERT</td>
<td>CERT Organization</td>
<td><a href="http://www.buerger-cert.de/">http://www.buerger-cert.de/</a></td>
</tr>
<tr>
<td>CERT-Bund</td>
<td>CERT Organization</td>
<td><a href="http://www.bsi.bund.de/certbund/">http://www.bsi.bund.de/certbund/</a></td>
</tr>
<tr>
<td>CERT-Verbund</td>
<td>CERT Organization</td>
<td><a href="http://www.cert-verbund.de/">http://www.cert-verbund.de/</a></td>
</tr>
<tr>
<td>Initiative “Germany Securely in the Net”</td>
<td></td>
<td><a href="https://www.sicher-im-netz.de/">https://www.sicher-im-netz.de/</a></td>
</tr>
<tr>
<td>NRW Secure IT Initiative</td>
<td></td>
<td><a href="http://www.secure-it.nrw.de/">http://www.secure-it.nrw.de/</a></td>
</tr>
<tr>
<td>SymantecStore</td>
<td></td>
<td><a href="http://security.symantec.com/">http://security.symantec.com/</a></td>
</tr>
<tr>
<td>TechConsult</td>
<td></td>
<td><a href="http://www.techconsult.de/">http://www.techconsult.de/</a></td>
</tr>
</tbody>
</table>
### Table 12: Contact Information about German Organizations

<table>
<thead>
<tr>
<th>Organization</th>
<th>Phone 1</th>
<th>Phone 2</th>
<th>Fax 1</th>
<th>Fax 2</th>
<th>Address / E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMI Federal Ministry of the Interior</td>
<td>+49 1888 681 0</td>
<td>+49 1888 681</td>
<td>+49 1888 681</td>
<td>+49 1888 681</td>
<td>BMI Telekom 101 D, 10559 Berlin, Germany / <a href="mailto:poststelle@bmi.bund.de">poststelle@bmi.bund.de</a></td>
</tr>
<tr>
<td>BSI Federal Office for Information Security</td>
<td>+49 228 9582 141</td>
<td>+49 228 9582 141</td>
<td>+49 228 9582 141</td>
<td>+49 228 9582 141</td>
<td>Bundesamt für Sicherheit in der Informationstechnik, Referat I 2.1 / CERT-Bund Postfach 200363, D-53133 Bonn, Germany, E-Mail: <a href="mailto:certbund@bsi.bund.de">certbund@bsi.bund.de</a></td>
</tr>
<tr>
<td>CERT-Bund</td>
<td>+49 1888 9582 222</td>
<td>+49 1888 9582 222</td>
<td>+49 1888 9582 222</td>
<td>+49 1888 9582 222</td>
<td>Bundesamt für Wirtschaft und Ausfuhrkontrolle, Frankfurter Straße 29-31, D-65760 Eschborn, Germany</td>
</tr>
<tr>
<td>Federal Ministry of Economics and Technology</td>
<td>+49 3018 615 6444</td>
<td>+49 3018 615</td>
<td>+49 3018 615</td>
<td>+49 3018 615</td>
<td>Bundesamt für Wirtschaft und Ausfuhrkontrolle, Frankfurter Straße 29-31, D-65760 Eschborn, Germany</td>
</tr>
<tr>
<td>Federal Office of Economics and Export Control</td>
<td>+49 6196 404 0</td>
<td>+49 6196 404</td>
<td>+49 6196 404</td>
<td>+49 6196 404</td>
<td>Bundesamt für Wirtschaft und Ausfuhrkontrolle, Frankfurter Straße 29-31, D-65760 Eschborn, Germany</td>
</tr>
<tr>
<td>German Federation of Industrial Research Associations AiF</td>
<td>+49 30 48163 451</td>
<td>+49 30 48163 451</td>
<td>+49 30 48163 451</td>
<td>+49 30 48163 451</td>
<td>Arbeitsgemeinschaft industrieller Forschungsvereinigungen &quot;Otto von Guericke&quot; e.V. (AiF), Tschakowski Str. 45-49, D-13156 Berlin, Germany</td>
</tr>
<tr>
<td>International Technology Cooperation Network</td>
<td>+49 30 48163 470</td>
<td>+49 30 48163 470</td>
<td>+49 30 48163 470</td>
<td>+49 30 48163 470</td>
<td>International Technology Cooperation Network, Tschakowskistra. 49, D-13156 Berlin, Germany</td>
</tr>
<tr>
<td>secure-it.nrw</td>
<td>+49 228 22 84 184</td>
<td>+49 228 22 84 184</td>
<td>+49 228 22 84 184</td>
<td>+49 228 22 84 184</td>
<td>Agentur »secure-it.nrw«, bei der IHK Bonn/Rhein-Sieg, Bonner Talweg 17, D-53113 Bonn, Germany / <a href="mailto:info@secure-it.nrw.de">info@secure-it.nrw.de</a></td>
</tr>
<tr>
<td>TeleTrusT Deutschland e.V.</td>
<td>+49 361 3460 531</td>
<td>+49 361 3460 531</td>
<td>+49 361 3460 531</td>
<td>+49 361 3460 531</td>
<td>Zenit GmbH, Zentrum für Innovation und Technik in NRW, Bismarckstr. 28, 45470 Mülheim an der Ruhr, Germany / <a href="mailto:info@zenit.de">info@zenit.de</a></td>
</tr>
<tr>
<td>ZENIT GmbH</td>
<td>+49 208 30004 0</td>
<td>+49 208 30004 0</td>
<td>+49 208 30004 0</td>
<td>+49 208 30004 0</td>
<td>ZENIT GmbH, Zentrum für Innovation und Technik in NRW, Bismarckstr. 28, 45470 Mülheim an der Ruhr, Germany / <a href="mailto:info@zenit.de">info@zenit.de</a></td>
</tr>
<tr>
<td>Euro Info Center</td>
<td>+49 208 30004 21</td>
<td>+49 208 30004 21</td>
<td>+49 208 30004 21</td>
<td>+49 208 30004 21</td>
<td>ZENIT GmbH, Zentrum für Innovation und Technik in NRW, Bismarckstr. 28, 45470 Mülheim an der Ruhr, Germany / <a href="mailto:info@zenit.de">info@zenit.de</a></td>
</tr>
</tbody>
</table>
Table 13: United Kingdom Links

<table>
<thead>
<tr>
<th>ORGANIZATION OR TOPIC</th>
<th>ACRONYM OR LOGO</th>
<th>LINK</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSI British Standards Institute</td>
<td><img src="image" alt="BSI Logo" /></td>
<td><a href="http://www.bsi-global.com/News/Information/British+Standards.xalter">http://www.bsi-global.com/News/Information/British+Standards.xalter</a></td>
</tr>
<tr>
<td>BTCERTCC CERT Organization</td>
<td><img src="image" alt="BTCERTCC Logo" /></td>
<td><a href="http://www.btcert.bt.com">http://www.btcert.bt.com</a></td>
</tr>
<tr>
<td>CPNI Centre for the Protection of National Infrastructure</td>
<td><img src="image" alt="CPNI Logo" /></td>
<td><a href="http://www.cpni.gov.uk">http://www.cpni.gov.uk</a></td>
</tr>
<tr>
<td>DTI Department of Trade and Industry Government Initiatives</td>
<td><img src="image" alt="dti Logo" /></td>
<td><a href="http://www.dti.gov.uk">http://www.dti.gov.uk</a> <a href="http://www.dti.gov.uk/innovation-group/pressrel-271102.htm">http://www.dti.gov.uk/innovation-group/pressrel-271102.htm</a></td>
</tr>
<tr>
<td>IOSH Institution of Occupational Safety and Health</td>
<td><img src="image" alt="IOSH Logo" /></td>
<td><a href="http://www.iosh.co.uk/">http://www.iosh.co.uk/</a></td>
</tr>
<tr>
<td>ITSafe Government Service</td>
<td><img src="image" alt="ITsafe Logo" /></td>
<td><a href="http://www.itsafe.gov.uk/">http://www.itsafe.gov.uk/</a></td>
</tr>
<tr>
<td>IWAR Warfare Security Awareness</td>
<td><img src="image" alt="IWAR Logo" /></td>
<td><a href="http://www.iwar.org.uk/comsec/resources/sa-tools/">http://www.iwar.org.uk/comsec/resources/sa-tools/</a></td>
</tr>
<tr>
<td>JANET-CERT of UKERNA CERT Organization</td>
<td><img src="image" alt="JANET-UKERNA Logo" /></td>
<td><a href="http://www.ja.net/cert/">http://www.ja.net/cert/</a></td>
</tr>
<tr>
<td>MLCIRT CERT Organization</td>
<td><img src="image" alt="MLCIRT Logo" /></td>
<td><a href="http://www.first.org/members/teams/mlcirt/">http://www.first.org/members/teams/mlcirt/</a></td>
</tr>
<tr>
<td>NSSF National Standardization Strategic Framework</td>
<td><img src="image" alt="NSSF Logo" /></td>
<td><a href="http://www.nssf.info">http://www.nssf.info</a> <a href="http://www.nssf.info/index.xalter">http://www.nssf.info/index.xalter</a></td>
</tr>
</tbody>
</table>
Table 14: Contact Information about Organizations in the United Kingdom

<table>
<thead>
<tr>
<th>Organization</th>
<th>Phone</th>
<th>Fax</th>
<th>Address / E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>BT SBS</td>
<td>+44 1255 220719</td>
<td>+44 113 244 5657</td>
<td>Bt Secure Business Services PP 1.14 Sevenoaks, Workstyle Building, 160 London Road, Sevenoaks, TN13 1BT, United Kingdom <a href="mailto:secure.business@bt.com">secure.business@bt.com</a></td>
</tr>
<tr>
<td>BTCERTCC</td>
<td>+44 1908 641100</td>
<td>+44 1908 230343</td>
<td>Bt CERTCC PP LF16 Libra House, Sunrise Parkway, Linford Wood, Milton Keynes, Bucks MK14 6PH, United Kingdom <a href="mailto:bctertcc@bt.com">bctertcc@bt.com</a></td>
</tr>
<tr>
<td>Centre for the Protection of National Infrastructure CPNI</td>
<td>+44 20 7233 8182</td>
<td></td>
<td>Central Support, PO Box 60628, SW1 9HA</td>
</tr>
<tr>
<td>CESG Communications Electronics Security Group</td>
<td>+44 1242 221491 ext 39365</td>
<td>+44 1242 221491 ext 39365</td>
<td><a href="mailto:iacs@cesg.gsi.gov.uk">iacs@cesg.gsi.gov.uk</a> <a href="mailto:CESGweb@cesg.gsi.gov.uk">CESGweb@cesg.gsi.gov.uk</a> <a href="mailto:caps@cesg.gsi.gov.uk">caps@cesg.gsi.gov.uk</a> <a href="mailto:policy@cesg.gsi.gov.uk">policy@cesg.gsi.gov.uk</a></td>
</tr>
<tr>
<td>CAPS Fast Track Assessment Portal CAPS Policy</td>
<td>+44 113 207 6002 6027</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CITIGROUP</td>
<td>+44 20 7500 4215</td>
<td>+44 20 7500 4610</td>
<td><a href="mailto:first-team@citicorp.com">first-team@citicorp.com</a></td>
</tr>
<tr>
<td>Department of Trade and Industry DTI</td>
<td>+44 171 215 1962</td>
<td>+44 171 931 7194</td>
<td>Response Centre 1 Victoria Street, London SW1H 0ET, UK / <a href="mailto:dti.enquiries@dti.gsi.gov.uk">dti.enquiries@dti.gsi.gov.uk</a></td>
</tr>
<tr>
<td>E-CERT</td>
<td>+44 131 507 750</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EUCS-IRT</td>
<td>+44 1280 996 7370</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSSF</td>
<td>+44 116 257 3100</td>
<td>+44 116 257 3101</td>
<td>Institution of Occupational Safety and Health The Grange, Highfield Drive, Wigston, Leicestershire, LE18 1NN, UK <a href="mailto:techinfo@iosh.co.uk">techinfo@iosh.co.uk</a></td>
</tr>
<tr>
<td>UNIRAS</td>
<td>+44 20 7215 2833</td>
<td>+44 20 7215 2234</td>
<td>Europe and World Trade Directorate, 1 Victoria Street, UK, London SW1H 0ET, <a href="mailto:asm@dti.gsi.gov.uk">asm@dti.gsi.gov.uk</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization</th>
<th>Phone</th>
<th>Fax</th>
<th>Address / E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOSH</td>
<td>+44 870 487 0748</td>
<td>+44 870 487 0749</td>
<td>UNIRAS, PO Box 832, London SW1P 1BG, United Kingdom, <a href="mailto:uniras@nisc.gov.uk">uniras@nisc.gov.uk</a></td>
</tr>
<tr>
<td>SOLVIT Center</td>
<td>+44 116 257 3100</td>
<td>+44 116 257 3101</td>
<td>Institution of Occupational Safety and Health The Grange, Highfield Drive, Wigston, Leicestershire, LE18 1NN, UK, <a href="mailto:techinfo@iosh.co.uk">techinfo@iosh.co.uk</a></td>
</tr>
<tr>
<td></td>
<td>+44 20 7215 2833</td>
<td>+44 20 7215 2234</td>
<td>Europe and World Trade Directorate, 1 Victoria Street, UK, London SW1H 0ET, <a href="mailto:asm@dti.gsi.gov.uk">asm@dti.gsi.gov.uk</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization</th>
<th>Phone</th>
<th>Fax</th>
<th>Address / E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>+44 1255 220719</td>
<td>+44 113 244 5657</td>
<td>Bt Secure Business Services PP 1.14 Sevenoaks, Workstyle Building, 160 London Road, Sevenoaks, TN13 1BT, United Kingdom <a href="mailto:secure.business@bt.com">secure.business@bt.com</a></td>
</tr>
<tr>
<td>BTCERTCC</td>
<td>+44 1908 641100</td>
<td>+44 1908 230343</td>
<td>Bt CERTCC PP LF16 Libra House, Sunrise Parkway, Linford Wood, Milton Keynes, Bucks MK14 6PH, United Kingdom <a href="mailto:bctertcc@bt.com">bctertcc@bt.com</a></td>
</tr>
<tr>
<td>Centre for the Protection of National Infrastructure CPNI</td>
<td>+44 20 7233 8182</td>
<td></td>
<td>Central Support, PO Box 60628, SW1 9HA</td>
</tr>
<tr>
<td>CESG Communications Electronics Security Group</td>
<td>+44 1242 221491 ext 39365</td>
<td>+44 1242 221491 ext 39365</td>
<td><a href="mailto:iacs@cesg.gsi.gov.uk">iacs@cesg.gsi.gov.uk</a> <a href="mailto:CESGweb@cesg.gsi.gov.uk">CESGweb@cesg.gsi.gov.uk</a> <a href="mailto:caps@cesg.gsi.gov.uk">caps@cesg.gsi.gov.uk</a> <a href="mailto:policy@cesg.gsi.gov.uk">policy@cesg.gsi.gov.uk</a></td>
</tr>
<tr>
<td>CAPS Fast Track Assessment Portal CAPS Policy</td>
<td>+44 113 207 6002 6027</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CITIGROUP</td>
<td>+44 20 7500 4215</td>
<td>+44 20 7500 4610</td>
<td><a href="mailto:first-team@citicorp.com">first-team@citicorp.com</a></td>
</tr>
<tr>
<td>Department of Trade and Industry DTI</td>
<td>+44 171 215 1962</td>
<td>+44 171 931 7194</td>
<td>Response Centre 1 Victoria Street, London SW1H 0ET, UK / <a href="mailto:dti.enquiries@dti.gsi.gov.uk">dti.enquiries@dti.gsi.gov.uk</a></td>
</tr>
<tr>
<td>E-CERT</td>
<td>+44 131 507 750</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EUCS-IRT</td>
<td>+44 1280 996 7370</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NSSF</td>
<td>+44 116 257 3100</td>
<td>+44 116 257 3101</td>
<td>Institution of Occupational Safety and Health The Grange, Highfield Drive, Wigston, Leicestershire, LE18 1NN, UK, <a href="mailto:techinfo@iosh.co.uk">techinfo@iosh.co.uk</a></td>
</tr>
<tr>
<td>UNIRAS</td>
<td>+44 20 7215 2833</td>
<td>+44 20 7215 2234</td>
<td>Europe and World Trade Directorate, 1 Victoria Street, UK, London SW1H 0ET, <a href="mailto:asm@dti.gsi.gov.uk">asm@dti.gsi.gov.uk</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization</th>
<th>Phone</th>
<th>Fax</th>
<th>Address / E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOSH</td>
<td>+44 870 487 0748</td>
<td>+44 870 487 0749</td>
<td>UNIRAS, PO Box 832, London SW1P 1BG, United Kingdom, <a href="mailto:uniras@nisc.gov.uk">uniras@nisc.gov.uk</a></td>
</tr>
<tr>
<td>SOLVIT Center</td>
<td>+44 116 257 3100</td>
<td>+44 116 257 3101</td>
<td>Institution of Occupational Safety and Health The Grange, Highfield Drive, Wigston, Leicestershire, LE18 1NN, UK, <a href="mailto:techinfo@iosh.co.uk">techinfo@iosh.co.uk</a></td>
</tr>
<tr>
<td></td>
<td>+44 20 7215 2833</td>
<td>+44 20 7215 2234</td>
<td>Europe and World Trade Directorate, 1 Victoria Street, UK, London SW1H 0ET, <a href="mailto:asm@dti.gsi.gov.uk">asm@dti.gsi.gov.uk</a></td>
</tr>
</tbody>
</table>