Isabelle Abele-Wigert and Myriam Dunn

INTERNATIONAL **CIIP HANDBOOK** 2006

VOL. I

AN INVENTORY OF 20 NATIONAL AND 6 INTERNATIONAL
CRITICAL INFORMATION INFRASTRUCTURE PROTECTION POLICIES

Series Editors
Andreas Wenger and Victor Mauer

Center for Security Studies, ETH Zurich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

CSS
An ETH Center

Isabelle Abele-Wigert and Myriam Dunn

INTERNATIONAL **CIIP HANDBOOK** 2006

VOL. I

AN INVENTORY OF 20 NATIONAL AND 6 INTERNATIONAL
CRITICAL INFORMATION INFRASTRUCTURE PROTECTION POLICIES

Series Editors
Andreas Wenger and Victor Mauer

Center for Security Studies, ETH Zurich

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Contents

Preface

The nature of risks and vulnerabilities in modern societies is becoming more and more transnational today. An open, non-hierarchical dialog on newly recognized vulnerabilities at the physical, virtual, and psychological levels is needed to create new knowledge and a better understanding of new risks and of their causes, interactions, probabilities, and costs.

It was on the basis of these premises that the "Comprehensive Risk Analysis and Management Network" (CRN, www.crn.ethz.ch) was launched in the year 2000 as a joint Swiss-Swedish initiative. The CRN is an internet and workshop initiative for international dialog on national-level security risks and vulnerabilities. As a complementary service to the International Relations and Security Network (ISN, www.isn.ethz.ch), the CRN is coordinated and developed by the Center for Security Studies at the Swiss Federal Institute of Technology (ETH Zurich), Switzerland in cooperation with the current CRN partner institutions:

- The Swedish Emergency Management Agency (SEMA), Sweden,
- The Directorate for Civil Protection and Emergency Planning (DSB), Norway,
- The Swiss Federal Department of Defense, Civil Protection, and Sports (DDPS), Switzerland,
- The Federal Office for National Economic Supply (NES), Federal Department of Economic Affairs, Switzerland.

The International Critical Information Infrastructure Protection (CIIP) Handbook is the product of a joint effort within the CRN partner network. The first edition of the CIIP Handbook, published in 2002, provided an inventory of national protection policies in eight countries: Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States. The 2002 Handbook proved to be such a success that it had to be reprinted soon after first publication. The 2004 edition offered updates on the existing country surveys, six new country studies (Austria, Finland, France, United Kingdom, Italy, and New Zealand), overview chapters on international protection efforts, legal issues, and current trends in research and development, as well as a more profound methodological section and more in-depth analysis in

general. The expert base and the number of staff working on the Handbook were both expanded.

The 2006 edition on hand continues the tradition of the past two editions and goes beyond it at the same time: it not only further expands the country survey section by including India, Japan, the Republic of Korea, Malaysia, Singapore, and Russia, but it is also accompanied by a second volume with in-depth analysis of key issues related to CIIP.

The editors would like to thank Isabelle Abele-Wigert researcher at the Center for Security Studies (CSS) at ETH Zurich (Swiss Federal Institute of Technology) and Myriam Dunn, Senior Research Fellow and CRN coordinator at CSS, for their efforts and their high-quality contribution to this important topic. Additionally, the editors would like to thank all the partners involved, in particular the national experts who generously shared their experience and knowledge with us. We also thank the following for their help in the completion of this project: Stefano Bruno, Christiane Callsen, Christopher Findlay, Fabian Furter, Myriam Käser, and Leo Niedermann. We look forward to continuing the development of and ever closer cooperation within the CRN network.

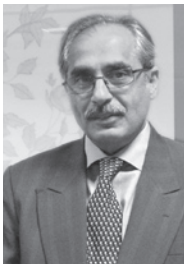
Zurich, February 2006

Prof. Dr. Andreas Wenger
Director,
Center for Security Studies,
ETH Zurich

Dr. Victor Mauer
Deputy Director, Head of Research,
Center for Security Studies,
ETH Zurich

Foreword

Dear Reader,



The Sanskrit saying "Vasudhaiva Kutumbakam" ("the whole world is one family") stresses the mutual connectedness and dependence of all humankind. Whether we compete or collaborate with others, connectedness between people around the world is a fact of life today. Cyberspace has contributed to this reality through the internet and telecom revolutions. The critical sectors of modern society namely energy (power, oil and natural gas, and nuclear energy) transportation (airways, railways, roads, shipping, and space), law enforcement (defense, police intelligence, and the judiciary), ICT (networks and telecom), the financial sector (banking, trade and commerce, financial instruments, and insurance) and public health (medical care, water, and sanitation) are becoming increasingly dependent on ICT structures for enhancing their efficiency and effectiveness. There are important downsides to this phenomenon in that criminals have found new targets to shake the foundation of our communities.

Each nation state is now diverting energies to secure its critical information infrastructure. There is much to learn from each other's experience. I therefore fully support the effort of the Center for Security Studies at the Swiss Federal Institute of Technology (ETH Zurich) to bring together the experiences of various countries in their third edition of the International CIIP Handbook. I strongly feel that this should be a reference book not only for governments, but also for academia and industry.

Let us all join hands across the globe to secure the emerging cyberspace that we benefit so much from.

V.K. Nambiar, Deputy National Security Advisor, New Delhi

Abbreviations

ACIS:	Advisory Committee for Information Security (Finland)
ACMA:	Australian Communications and Media Authority (Australia)
ACSI 33:	Australian Communications-Electronic Security Instruction 33 (Australia)
AFP:	Australian Federal Police (Australia)
AG KRITIS:	Interministerielle Arbeitsgruppe Kritische Infrastrukturen (Germany)
AGD:	Attorney General's Department (Australia)
AGIMO:	Australian Government Information Management Office (Australia)
AgIO:	Cabinet Office Workgroup on Information Operations (Sweden)
AHG:	Ad Hoc Group (NATO)
AHTCC:	Australian High Tech Crime Centre (Australia)
AIPA:	Authority for IT in the Public Administration (Italy)
AIVD:	Algemene Inlichtingen- en Veiligheidsdienst/General Intelligence and Security Service (The Netherlands)
AKSIS:	Arbeitskreis Schutz Kritischer Infrastrukturen/Working Group on Infrastructure Protection (Germany)
AMSD:	Accompanying Measure System Dependability (EU)
APCERT:	Asia Pacific Computer Emergency Response Team
AP-CIRT:	Asia Pacific Security Incident Response Coordination
APEC:	Asia-Pacific Economic Cooperation
AS/NZS:	Australian and New Zealand Standard for Risk Management (Australia/New Zealand)
ASIO:	Australian Security Intelligence Organisation (Australia)
A-SIT:	Center for Secure Information Technology Austria (Austria)
AusCERT:	Australian Computer Emergency Response Team (Australia/New Zealand)
BAKOM:	Bundesamt für Kommunikation/Federal Office for Communication (Switzerland)
BAS:	Protection of Society (Norway)
BBK:	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe/Federal Office for Civil Protection and Disaster Response (Germany)
BCS:	British Computer Society (United Kingdom)
BfV:	Bundesamt für Verfassungsschutz/Federal Office for the Protection of the Constitution (Germany)
BIS:	Bureau of Indian Standards (India)
BIT:	Bundesamt für Informatik und Telekommunikation/Federal Office of Information Technology, Systems, and Telecommunication (Switzerland)
BITKOM:	Bundesverband für Informationswirtschaft, Telekommunikation und Neue Medien (Germany)
BITS:	Banking Industry Technology Secretariat (Korea)
BKA:	Bundeskriminalamt/Federal Office of Criminal Investigation (Germany)
BMBF:	Bundesministerium für Bildung und Forschung/Federal Ministry for Education and Research (Germany)
BMI:	Bundesministerium des Inneren/Federal Ministry of the Interior (Austria; Germany)

BMJ:	Bundesministerium der Justiz/Federal Ministry of Justice (Germany)
BMVg:	Bundesministerium der Verteidigung/Federal Ministry of Defense (Germany)
BMVIT:	Ministry for Traffic, Infrastructure and Technology (Austria)
BMWA:	Bundesministerium für Wirtschaft und Arbeit/Federal Ministry of Economics and Labour (Germany)
BMWi:	Bundesministerium für Wirtschaft and Technologie/Federal Ministry of Economics and Technology (Germany)
BND:	Bundesnachrichtendienst/Federal Intelligence Service (Germany)
BPOL:	Federal Police (Germany)
BSI:	Bundesamt für Sicherheit in der Informationstechnik/ Federal Office for Information Security (Germany)
BVA:	Bundesverwaltungsamt/Federal Office of Administration (Germany)
BVT:	Federal Agency for State Protection and Counter-Terrorism (Austria)
BZK:	Ministry of the Interior and Kingdom Relations (The Netherlands)
CanCERT:	Canadian Computer Emergency Response Team (Canada)
CAPC:	Civil Aviation Planning Committee (NATO)
CART:	Computer Analysis and Response Team (United States)
CAS:	Complex Adaptive Systems
CATS:	Center for Asymmetric Threat Studies (Sweden)
CBA:	Canadian Bankers Association (Canada)
CCIP:	Centre for Critical Infrastructure Protection (New Zealand)
CCIPS:	Computer Crime and Intellectual Property Section (United States)
CCIRC:	Canadian Cyber Incident Response Centre (Canada)
CCPC:	Civil Communication Planning Committee (NATO)
CCS:	Civil Contingencies Secretariat (United Kingdom)
CEA:	Canadian Electricity Association (Canada)
CEN:	European Committee for Standardization
CEP:	Civil Emergency Planning (NATO)
CERT/CC:	Computer Emergency Response Team Coordination Center
CERT:	Computer Emergency Response Team
CERTA:	Computer Emergency Response Team (France)
CERT-Bund:	German Computer Emergency Response Team for Federal Authorities (Germany)
CERT-FI:	Computer Emergency Response Team Finland (Finland)
CERT-In:	Computer Emergency Response Team India (India)
CERT-IST:	Computer Emergency Response Team Industry, Services, and Trade (France)
CERT-IT:	Italian Computer Emergency Response Team (Italy)
CERT-NL:	Computer Emergency Response Team of the Netherlands (The Netherlands)
CERT-PA:	Computer Emergency Response Team for the Public Central Administration (Italy)
CERT-RENATER:	Computer Emergency Response Team (France)
CESG:	Communications-Electronics Security Group (United Kingdom)

CESSSI:	Centre for Training and Advanced Studies on Information Systems Security (France)
CESTI:	Information Technology Security Evaluation Center
CFAA:	Computer Fraud and Abuse Act (United States)
CFSSI:	Information Systems Security Training Center (France)
CHO:	Chief Headquarter of Defense (Norway)
CI:	Critical Infrastructure
CI2RCO:	Critical Information Infrastructure Research Coordination (EU)
CIAC:	Critical Infrastructure Advisory Council (Australia)
CIAO:	Critical Infrastructure Assurance Office (United States)
CIDDAC:	Cyber Incident Detection Analysis Centre (United States)
CIF:	Consultative Industry Forum (Australia)
CII:	Confederation of Indian Industry (India)
CII:	Critical Information Infrastructure
CIIP:	Critical Information Infrastructure Protection
CIO:	Chief Information Officer
CIOS:	National Centre for IO/CIP Studies (Sweden)
CIP:	Critical Infrastructure Protection
CIPG:	Critical Infrastructure Protection Group (Australia)
CIPTF:	Critical Infrastructure Protection Task Force (Canada)
CIRCA:	Computer Incident Response Coordination Austria (Austria)
CIRT:	Computer Incident Response Team
CIS:	Center for International Studies (Switzerland)
CISSI:	Inter-Ministerial Committee for Information Society (France)
CISU:	Critical Infrastructure Studies Unit (Sweden)
CIWG:	Critical Infrastructure Working Group (United States)
CLUSIF:	Club de la Sécurité des Systèmes d'Information Français (France)
CMA:	Communications and Multimedia Act (Malaysia)
CNES:	French Space Agency (France)
CNI:	Critical National Infrastructure
CNIPA:	National Center for Informatics in the Public Administration (Italy)
COBIT:	Control Objectives for Information Technology (United States)
COMSEC:	Communications Security (Finland)
CPC:	Civil Protection Committee (NATO)
CRC:	Communications Research Centre (Canada)
CRIEPI:	Central Research Institute of the Electric Power Industry (Japan)
CRN:	Comprehensive Risk Analysis and Management Network (Switzerland)
CRS:	Congressional Research Service (United States)
CSCs:	Common Services Centres (India)
CSD:	Computer Security Division at NIST (United States)
CSE:	Communications Security Establishment (Canada)
CSEC:	Swedish Certification Body for IT Security (Sweden)
CSIA:	Central Sponsor for Information Assurance (United Kingdom)
CSIAAG:	Communications Sector Infrastructure Assurance Advisory Group (Australia)

CSIRT:	Computer Security Incident Response Team
CSIS:	Canadian Security Intelligence Service (Canada)
CSS:	Center for Security Studies, ETH Zurich (Switzerland)
CSTARC:	Cyber Security Tracking, Analysis and Response Center (United States)
CSTI:	Strategic Advisory Board on Information Technologies (France)
CT:	Counter-terrorism
CTEPA:	Canadian Telecommunications Emergency Preparedness Association (Canada)
CTI:	Commission for Technology and Innovation (Switzerland)
CTOSE:	Cyber Tools On-Line Search for Evidence (EU)
CYCO:	Swiss Coordination Unit for Cybercrime Control (Switzerland)
CYTEX:	Cyber Terror Exercise (Germany)
DCITA:	Department of Communications, Information Technology & the Arts (Australia)
DCSSI:	Directorate for Security of Information Systems (France)
DdoS:	Distributed Denial of Service
DDPS:	Swiss Federal Department of Defense, Civil Protection, and Sports (Switzerland)
DDSI:	Dependability Development Support Initiative (EU)
deNIS:	German Emergency Preparedness Information System (Germany)
DESS:	Domestic and External Security Secretariat (New Zealand)
DFS:	Swedish Information Processing Society (Sweden)
DGTP:	Telecom and Post Directorate (The Netherlands)
DHS:	Department of Homeland Security (United States)
DIA:	Defense Intelligence Agency (United States)
DICO:	Dipartimento di Informatica e Comunicazione/Department of Informatics and Communications (Italy)
DIT:	Department for Innovation and Technologies (Italy)
DIT:	Department of Information Technologies (India)
DoD:	Department of Defense (United States)
DoE:	Department of Energy (United States)
DSB:	Directorate for Civil Protection and Emergency Planning (Norway)
DSD:	Defence Signals Directorate (Australia)
DSG:	Datenschutzgesetz/Data Protection Law (Austria)
DSK:	Datenschutzkommission/Commission on Data Protection (Austria)
DSO:	Departmental Security Officer (New Zealand)
DSTL:	Defence Research Centre (United Kingdom)
DSTO:	Defence Science and Technology Organisation (Australia)
DTI:	Department of Trade and Industry (United Kingdom)
EBIOS:	Expression of the Needs and Identification of Security Objects (France)
ECI:	EU Critical Infrastructures (EU)
ECP.NL:	Electronic Commerce Platform in the Netherlands (The Netherlands)
EDS:	Electronic Digital Signature (Russia)
EFD:	Eidgenössisches Finanzdepartement/Swiss Federal Department of Finance (Switzerland)

EIA:	Electronic Industries Alliance (United States)
EJPD:	Eidgenössisches Justiz- und Polizeidepartement/Federal Department of Justice and Police (Switzerland)
ELAK:	Electronical File (Austria)
EMA:	Emergency Management Act (Canada)
EMP:	Electromagnetic Pulse
ENFSI:	European Network of Forensic Science Institute on Computer Crime (Austria)
ENISA:	European Network and Information Security Agency (EU)
EO:	Executive Order (United States)
EPCIP:	European Program for the Protection of Critical Infrastructure (EU)
ERA:	European Research Area (EU)
ESCG:	E-Security Coordination Group (Australia)
ESRP:	European Security Research Programme (EU)
ETH:	Eidgenössische Technische Hochschule/Swiss Federal Institute of Technology, ETH Zurich (Switzerland)
ETRI:	Electronics & Telecommunications Research Institute (Korea)
ETSI:	European Telecommunications Standards Institute (EU)
EU:	European Union
EUCIWIN:	Critical Infrastructure Warning and Information Network (EU)
EVD:	Eidgenössisches Volkswirtschaftsdepartement/Federal Department of Economic Affairs (Switzerland)
EXYSTENCE:	Complex Systems Network of Excellence (EU)
EZB:	Einsatzzentrale Basisraum (Austria)
FACA:	Federal Advisory Committee Act (United States)
FAPC:	Food and Agriculture Planning Committee (NATO)
FAPSI:	Federal Agency for Government Communications and Information (Russia)
FBI:	Federal Bureau of Investigation (United States)
FDCA:	Finnish Data Communication Association (Finland)
FedCIRC:	Federal Computer Incident Response Center (United States)
Fedpol:	Federal Office of Police (Switzerland)
FEPC:	Federation of Electric Power Companies (Japan)
FERC:	Federal Energy Regulatory Commission (United States)
FFI:	Norwegian Defense Research Establishment (Norway)
FICORA:	Finnish Communications Regulatory Authority (Finland)
FIRST:	Forum of Incident and Security Response Team (Canada)
FMV:	Swedish Defense Material Administration (Sweden)
FOI:	Swedish Defense Research Agency (Sweden)
FOIA:	Freedom of Information Act (United States)
FOITT:	Federal Office of IT, Sytems and Telecommunication (Switzerland)
FP6:	Sixth Framework Program (EU)
FRA:	Swedish National Defense Radio Establishment (Sweden)
FS/ISAC:	Financial Services Information Sharing and Analysis Center (United States)

FSB:	Federal Security Service of the Russian Federation (Russia)
G8:	Group of Eight
GAO:	General Accounting Office (United States)
GCERT:	Government Computer Emergency Response Team (Malaysia)
GCSB:	Communications Security Bureau (New Zealand)
GCSG:	Communications-Electronics Security Group (United Kingdom)
GdIN:	Gruppo di Interesse Nazionale (Italy)
GEA:	Swedish Alliance for Electronic Commerce (Sweden)
GICT:	Global Information and Communication Technologies Department (World Bank Group)
GIP RENATER:	National Network of Telecommunications for Technology, Education, and Research (France)
GOC:	Government Operations Centre (Canada)
GoL:	Government-on-Line (Canada)
GOVCERT.NL:	Government-wide Computer Emergency Response Team (The Netherlands)
HERT:	Hacking Emergency Response Team (The Netherlands)
HSPD:	Homeland Security Presidential Directive (United States)
HTCTD:	High-Tech Crime Technology Division (Japan)
I3P:	Institute for Information Infrastructure Protection (United States)
IA:	Information Assurance
IAAC:	The Information Assurance Advisory Council (United Kingdom)
IAAGs:	Infrastructure Assurance Advisory Groups (Australia)
IABG:	Industrieanlagen-Betriebsgesellschaft (Germany)
IAG:	Infrastructure Analysis Group
IAIP:	Directorate for Information Analysis and Infrastructure Protection (United States)
ICCP:	Committee for Information, Computer, and Communications Policy (OECD)
ICD:	Infrastructure Coordination Division (United States)
ICIC:	Internet Crime Investigation Center (Korea)
ICS:	Secretary of the Interdepartmental Committee on Security (New Zealand)
ICT:	Information and Communication Technologies
ICT-I:	ICT Infrastructure Unit (Switzerland)
IDC:	Interdepartmental Committee on the Protection of the National Information Infrastructure (Australia)
IDS:	Intrusion Detection System
IIPC:	Information Infrastructure Protection Centre (India)
IIPC:	Information Infrastructure Protection Group (Australia)
INFOSEC:	Information Systems Security (Australia, New Zealand)
IO:	Information Operations
IOWG:	Information Operations Working Group
IPA:	Information Technology Promotion Agency (Japan)
IPC:	Industrial Planning Committee (NATO)
IPs:	Infrastructure Profiles

IPSC:	Institute for the Protection and Security of Citizen
IRItaly:	Incident Response Italy (Italy)
ISACs:	Information Sharing and Analysis Centers
ISB:	Informatikstrategieorgan Bund/Federal Strategy Unit for Information Technology (Switzerland)
ISCG:	Information Society Coordination Group (Switzerland)
ISCOM:	Institute for Information and Communication Technologies/Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (Italy)
ISDF:	French Dependability Institute (France)
ISF:	Information Sharing Forum (Malaysia)
ISIDRAS:	Information Security Incident Detection Reporting and Analysis (Australia)
ISIT:	Inter-Ministerial Board for Security (Germany)
ISN:	International Relations and Security Network (Switzerland)
ISP:	Internet Service Provider
ISPA:	Federation of the Austrian Internet Service Providers (Austria)
ISPC:	Information Security Policy Council (Japan)
IST:	Institute for Signal Intelligence and Technical Information (Sweden)
IST:	Information Society Technologies (EU)
ISTDC:	Information Security Technology Development Council (India)
IT:	Information Technology
ITAA:	Information Technology Association of America (United States)
ITAC:	Integrated Threat Assessment Centre (Canada)
ITSEAG:	IT Security Expert Advisory Group (Australia)
ITSEC:	Information Technology Security Evaluation Criteria (France)
ITSEC:	IT Security (Norway)
JIIRP:	Joint Infrastructures Interdependencies Research Program (Canada)
JPCERT/CC:	Japan Computer Emergency Response Coordination Center (Japan)
KIG:	Coordination Group for Information Society (Switzerland)
KIS:	National Information Security Co-ordination Council (Norway)
KISA:	Korean Information Security Agency (Korea)
KISC:	Korea Internet Security Center (Korea)
KISEC:	Korea IT Security Evaluation Center (Korea)
KISIA:	Korea Information Security Industry Association (Korea)
KLPD:	Korps Landelijke Politiediensten (Cyber Crime Unit of the Dutch Police) (The Netherlands)
KrCERT/CC:	Korea Computer Emergency Response Team Coordination Center (Korea)
KSRC:	Korea Spam Response Center (Korea)
KWINT:	Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid (The Netherlands)
MAMPU:	Malaysian Administrative Modernization and Management Planning Unit (Malaysia)
MBG:	Militärbefugnisgesetz (Austria)
MCDA:	Multi-Criteria Decision Approach

MCMC:	Malaysian Communications and Multimedia Commission (Malaysia)
MELANI:	Reporting and Analysis Center for Information Assurance (Switzerland)
METI:	Ministry of Economy, Trade and Industry (Japan)
MEWC:	Ministry of Energy, Water and Communications (Malaysia)
MHA:	Ministry of Home Affairs
MIC:	Ministry of Information and Communication (Korea)
MIT:	Minister for Innovation and Technologies (Italy)
MMS:	Multimedia Messaging Service
MOC:	Ministry of Communications and Information Technology (India)
MoD:	Ministry of Defense
MOSTI:	Ministry of Science, Technology and Innovation (Malaysia)
MyCERT:	Malaysian Computer Emergency Response Team (Malaysia)
MyMIS:	Malaysian Public Sector Management of Information and Communications Technology Security Handbook (Malaysia)
NACOTEL:	National Telecommunications Contingency Plan (The Netherlands)
NASSCOM:	National Association of Software and Service Companies (India)
NATO:	North Atlantic Treaty Organisation
NAZ:	Nationale Alarm Zentrale/National Emergency Operations Center Agency (Switzerland)
NBED:	National Board of Economic Defense (Finland)
NCC:	National Coordinating Center (The Netherlands)
NCI:	National Critical Infrastructures
NCIAP:	National Critical Infrastructure Assurance Program (Canada)
NCIPP:	National Critical Infrastructure Protection Program (Canada)
NCO-T	National Continuity Consultation Platform Telecommunications (The Netherlands)
NCPG:	National Contingency Planning Group (Canada)
NCS:	National Communications System (United States)
NCSA:	National Cyber Security Alliance (United States)
NCSC:	National Cyber Security Center (Korea)
NCSD:	National Cyber Security Division (United States)
NCSP:	National Cyber Security Partnership (United States)
NCTC:	National Counter-Terrorism Committee (Australia)
NCTP:	National Counter-Terrorism Plan (Australia)
NDMS:	National Disaster Mitigation Strategy (Canada)
NeGP:	National e-Governance Action Plan (India)
NERC:	North American Electricity Reliability Council (United States)
NERS:	National Emergency Response System (Canada)
NES:	Federal Office for National Economic Supply/Bundesamt für Wirtschaftliche Landesversorgung (BWL) (Switzerland)
NESA:	National Emergency Supply Agency (Finland)
NEST:	National Emergency System (Singapore)
NGO:	Non-Governmental Organizations
NHTCC:	National High Tech Crime Center (The Netherlands)
NHTCU:	National Hi-Tech Crime Unit (United Kingdom)

NIAC:	National Infrastructure Advisory Council (United States)
NIB:	National Information Board (India)
NIC:	National Informatics Centre (India)
NII:	National Information Infrastructure
NIPC:	National Infrastructure Protection Center (United States)
NIPP:	National Infrastructure Protection Plan (United States)
NIRA:	National Infrastructure Risk Assessment (Canada)
NIRT:	National Incident Response Team (Japan)
NISA:	National Information Security Alliance (Korea)
NISC:	National Information Security Center (Japan)
NISCC:	National Information Security Coordination Cell (India)
NISCC:	National Infrastructure Security Co-ordination Centre (United Kingdom)
NISER:	National ICT Security and Emergency Response Centre (Malaysia)
NIST:	National Institute of Standards and Technology (United States)
NITA:	National IT Agenda (Malaysia)
NITAS:	National Information Technology Alert Service (Australia)
NITC:	National Information Technology Council (Malaysia)
NLIP:	Branchevereniging van Nederlandse Internet Providers/Consortium of Dutch Internet Providers (The Netherlands)
NOC:	Network Operation Centre (Russia)
NPA:	National Police Agency (Japan)
NPB:	Swedish National Police Board (Sweden)
NPSI:	National Plan for Information Infrastructure Protection (Germany)
NRC:	Canadian National Research Council (Canada)
NSA:	National Security Agency (United States)
NSAC:	National Security Advice Centre (United Kingdom)
NSCS:	National Security Council Secretariat (India)
NSCS:	National Security Council Secretariat (India)
NSD:	Industry Security Delegation (Sweden)
NSM:	Norwegian National Security Authority (Norway)
NSRI:	National Security Research Institute (Korea)
NSSC:	National Strategy to Secure Cyberspace (United States)
NZCS SigSec:	Computer Society Special Interest Group on Security (New Zealand)
NZSA:	New Zealand Security Association (New Zealand)
NZSIS:	New Zealand Security Intelligence Service (New Zealand)
NZSIT:	New Zealand Security of Information Technology (New Zealand)
OASD/NII:	Office of the Assistant Secretary of Defense for Networks and Information Integration (United States)
OCIIP:	Office of Computer Investigations and Infrastructure Protection (United States)
OCSI:	Organismo die Certificazione della Sicurezza Informatica (Italy)
ODESC:	Officials Committee for Domestic and External Security Co-ordination (New Zealand)
OEA:	Office of Energy Assurance (United States)
OECD:	Organisation for Economic Co-operation and Development

OFCOM:	Federal Office for Communication (Switzerland)
OGIT:	Office of Government Information Technology (Australia)
OGO:	Office for Government On-line (Australia)
OKOKRIM:	National Authority for Investigation and Prosecution of Economic and Environmental Crime (Norway)
PAGSI:	Government Action Program for an Information Society (France)
PB&C:	Planning Board and Committee (NATO)
PBIST:	Planning Board for Inland Surface Transportation (NATO)
PBOS:	Planning Board for Ocean Shipping (NATO)
PCCIP:	Presidential Commission on Critical Infrastructure Protection (United States)
PCII:	Protected Critical Information Infrastructure Programm (United States)
PCIS:	Partnership for Critical Infrastructure Security (United States)
PDD:	Presidential Decision Directives (United States)
PKI:	Public Key Infrastructure
PPO:	Planning and Partnerships Office (PPO)
PSD:	Protective Services Divison (United States)
PSEPC:	Public Safety and Emergency Preparedness Canada (Canada)
PSS:	Public Safety and Security (Sweden)
PSYOP:	Psychological Operations
PTS:	Swedish National Post and Telecom Agency (Sweden)
R&D:	Research and Development
RAKEL:	Radio Communication for Efficient Command (Sweden)
RANS:	Russian Association of Networks and Services (Russia)
RBNET:	Russian Backbone Network
RCMP:	Royal Canadian Mounted Police (Canada)
RegTP:	Regulatory Authority for Telecommunications and Posts (Germany)
RIPN:	Russian Institute of Public Networks
RMA:	Revolution in Military Affairs
RU-CERT:	Computer Emergency Response Team of Russia (Russia)
S&T:	Science and Technology (United States)
SAI:	Centro Virtuale di Simulazione e Analisi delle Interdipendenze/Interdependencies Simulation and Analysis Center (Italy)
SÄPO:	Swedish Security Service (Sweden)
SBA:	Vulnerability Assessment/SårBarhetsAnalys (Sweden)
SCADA:	Supervisory Control and Data Acquisition
SCEPC:	Senior Civil Emergency Planning Committee (NATO)
SCNS:	Secretaries' Committee on National Security (Australia)
SCOs:	Sectoral Cyber Security Officers (India)
SCSSI:	Service Central de la Sécurité des Systèmes d'Information (France)
SEI:	Software Engineering Institute (United States)
SEMA:	Swedish Emergency Management Agency (Sweden)
SFU:	Strategische Führungsübung/Strategic Leadership Exercise (Switzerland)
SGDN:	General Secretariat of National Defense (France)

SigG:	Electronic Signature Law (Austria)
SIGINT:	Signals Intelligence
SII:	Strategic Infrastructure Initiative (Canada)
SIS:	Center for Information Security (Norway)
SITIC:	Swedish IT Incident Centre (Sweden)
SLT:	Strategic Leadership Training (Switzerland)
SMEs:	Small and Medium Enterprises
SMS:	Short Message Service
SNZ:	Standards New Zealand (New Zealand)
SONIA:	Sonderstab Information Assurance/Special Task Force on Information Assurance (Switzerland)
SPG:	Security Police Law/Sicherheitspolizeigesetz (Austria)
SSI:	Security of Information Systems (France)
StGB:	Austrian Penal Code (Austria)
STQC:	Standardization Testing & Quality Certification (India)
SWANs:	State Wide Area Networks (India)
SWITCH:	Swiss Education and Research Network (Switzerland)
Tekes:	National Technology Agency (Finland)
TIEKE:	Finnish Information Society Development Centre (Finland)
TISN:	Trusted Information Sharing Network for Critical Infrastructure Protection (Australia)
TKG:	Telekommunikationsgesetz (Austria)
TNO:	Netherlands Organization for Applied Scientific Research (The Netherlands)
TSA:	National Communications Security Group (Sweden)
TSWG:	Technical Support Working Group (UN)
UN:	United Nations
UNIDIR:	United Nations Institute for Disarmament Research (UN)
UNIRAS:	Unified Incident Reporting and Alert Scheme (United Kingdom)
UNITAR:	United Nations Institute for Training and Research (UN)
USA PATRIOT:	(Act) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (United States)
US-CERT:	United States Computer Emergency Response Team (United States)
V&W:	Ministry of Transport, Public Works, and Water Management (The Netherlands)
VAHTI:	Steering Committee for Data Security in State Administration (Finland)
VDI:	Warning System for Digital Infrastructure (Norway)
VEC:	Veilige Elektronische Communicatie (The Netherlands)
VROM:	Ministry of Housing, Spatial Planning, and the Environment (The Netherlands)
VWS:	Ministry of Health, Welfare and Sport (The Netherlands)
WARP:	Warning, Advice, and Reporting Point (United Kingdom)
WPISP:	Working Party on Information Security and Privacy (OECD)
WSIS:	World Summit on the Information Society (ITU/UN)
ZAS:	Zentrales Ausweichsystem (Austria)

Introduction

Background

Contrary to widespread belief, concerns about cyber-security are not a phenomenon that arose in the 1990s. Viruses and worms have been part of the background noise of cyberspace since its earliest days: In the 1986 movie War Games, a young teenager hacks his way into the computer that handles command and control for the US nuclear arsenal and almost triggers World War III. In the real world, the famous Cuckoo's Egg incident in the mid-1980s raised the awareness that intelligence services had found new ways to obtain highly classified information.[1] So what is new today? On the one hand, the technological environment and substructure is new: Since the early 1990s, information technology has evolved from modest use of mainly stand-alone systems in closed networks to the development of the internet and other networks connecting businesses, governments, consumers, and any "wired" individual or organization. Access devices have multiplied and diversified to include a variety of portable and wireless accesses. Increased vulnerability seems to manifest itself in the increase of cyber-incidents in recent years: According to CERT (Computer Emergency Response Team) statistics, 9'859 incidents were reported in 1999, 52'658 in 2001, and 137'529 in 2003.[2]

Even if we are highly skeptical about the usefulness and accuracy of statistics, we can also identify a qualitative difference in addition to a quantitative increase in cyber-incidents. This qualitative difference concerns the gravity of the threat: In the mid-1990s, the issue of cyber-security was catapulted onto the security political agendas when it was persuasively linked to both terrorism and critical infrastructure protection (CIP). A critical infrastructure (CI) is an infrastructure or asset the incapacitation or destruction of which would have a debilitating impact on the national security and the economic and social welfare of a nation.[3] Protection concepts for strategically important infrastructures and objects have been part of national defense planning for decades, though

1 Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage (New York: Pocket Books, 1990).

2 CERT/CC Statistics 1988-2005. http://www.cert.org/stats/cert_stats.html#incidents.

3 The definition of critical infrastructure varies from country to country. The Handbook shows in detail how each country defines critical infrastructure and what sectors are included under this category.

at varying levels of importance. Towards the end of the Cold War and for a couple of years thereafter, the possibility of infrastructure discontinuity caused by attacks or other disruptions played a relatively minor role in the security debate — only to gain new impetus around the mid-1990s.[4]

During that time, it was established that key sectors of modern society, including those vital to national security and to the essential functioning of industrialized economies, rely on a spectrum of highly interdependent national and international software-based control systems for their smooth, reliable, and continuous operation. This critical information infrastructure (CII) underpins many elements of the CI, as many information and communication technologies (ICT) have become all-embracing, connecting other infrastructure systems and making them interrelated and interdependent. Not only are information systems exposed to failures, they are also potentially attractive targets for malicious attacks. The CI delivers a range of services that individuals, and society as a whole, depend on. Any damage to or interruption of the CI causes ripples across the technical and societal systems — a principle that has held true in the past, and even more so today due to much greater interdependencies. Attacking infrastructure therefore has a "force-multiplier" effect that allows even a relatively small attack to achieve a great impact. For this reason, CI structures and networks have historically proven to be appealing targets for a whole array of actors.[5]

Part I Survey of National Protection Policies

The US — due to its leading role as an IT nation, among other factors — was the first state to address the problem of CIP in earnest. This new interest in infrastructure protection was augmented by the enhanced threat perception after the Oklahoma City bombing of 1995. After the attack on the Alfred P. Murrah Federal Building in Oklahoma City, government officials realized that the loss of a seemingly insignificant federal building, outside the "nerve center" of Washington, was able to set off a chain reaction that affected an area of the economy that would not have normally been linked to the functions of

4 Cf. Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver. "Critical Infrastructure Protection in The Netherlands: A Quick-scan". In: Gattiker, Urs E., Pia Pedersen, and Karsten Petersen (eds.). EICAR Conference Best Paper Proceedings 2003. http://www.tno.nl/instit/fel/refs/pub2003/BPP-13-CIP-Luiijf&Burger&Klaver.pdf.

that federal building. The idea was that, beyond the loss of human lives and physical infrastructure, a set of processes controlled from that building had also been lost (i.e., a local bureau of the FBI, a payroll department, etc.), with a hitherto unimaginable impact on other agencies, employees, and/or the private sector down the supply chain and far beyond the physical destruction of the building. This made clear that interdependency between infrastructures and their vulnerability were major issues.

One direct outcome of the Oklahoma City bombing was Presidential Decision Directive 39 (PDD-39), which directed the attorney-general to lead a government-wide effort to re-examine the adequacy of the available infrastructure protection. As a result, Attorney-General Janet Reno convened a working group to investigate the issue and report back to the cabinet with policy options. The review, which was completed in early February 1996, particularly highlighted the lack of attention that had been given to protecting the cyber-infrastructure of critical information systems and computer networks. Thus, the topic of cyber-threats was linked to the topics of critical infrastructure protection and terrorism. Subsequently, President Bill Clinton started to develop a national protection strategy with his Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996.[6]

The PCCIP concluded in 1997 that the security, economy, way of life, and perhaps even the survival of the industrialized world were now dependent on the combination of electrical energy, communications, and computers. The commission found that advanced societies rely heavily upon critical infrastructures, which are susceptible to classical physical disruptions as well as to new virtual threats.[7] Following the PCCIP's publication, US President Bill Clinton started initiatives to increase the protection of critical infrastructure in the US, on the premise that a joint effort by government, society, organizations,

5 Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP). Threat Analysis No. TA03-001 (2003). http://www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf.

6 President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures (Washington, October 1997). Publication quoted in the following as PCCIP.

7 Ibid.

and critical industries was needed to prepare for defending these vital assets.[8] Following the example of the US and driven by a growing concern for the potential vulnerability of their own networked societies, numerous countries have thereafter begun to draft protection policies of their own.

On the one hand, the CIIP Handbook focuses on these national governmental efforts to protect critical information infrastructure and provides an overview of CII protection practices in a range of countries: The initial eight surveys of the 2002 edition (Australia, Canada, Germany, the Netherlands, Norway, Sweden, Switzerland, and the United States) have been substantially updated and supplemented by six additional surveys in the 2004 edition (Austria, Finland, France, Italy, New Zealand, and the United Kingdom). In the current 2006 edition, we add an additional six surveys to the existing fourteen, with a distinct focus on Asia (India, Japan, the Republic of Korea, Malaysia, Russia, and Singapore).

For each survey, five focal points of high importance covering conceptual and organizational aspects of CIIP are considered:

1 The definition of critical sectors: The first section lists the critical sectors identified by the specific country and provides definitions of CII and CIIP, where available.
2 Past and present CIIP initiatives and policy: The second section gives an overview of the most important steps taken at the governmental level since the late 1990s to handle CIIP. The focus is on initiatives and the main elements of CIIP policy. This includes descriptions of specific committees, commissions, task forces, and working groups, the main findings of key official reports and fundamental studies, and important national programs.
3 Organizational structures: The third section gives an overview of important public actors in the national CIIP organizational framework. It only characterizes the specific responsibilities or public actors at the state (federal) level (such as ministries, national offices, agencies,

8 Clinton, William J., Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue. Version 1.0 (Washington, 2000); Clinton, William J., Executive Order 13010 on Critical Infrastructure Protection (Washington, 15 July 1996). http://www.info-sec.com/pccip/web/eo13010.html; Clinton, William J., Protecting America's Critical Infrastructures: Presidential Decision Directive 63 (Washington, 22 May 1998). http://www.fas.org/irp/offdocs/eo13010.htm.

coordination groups, etc.). Public actors at the lower state level and private actors (companies, industry, etc.) are omitted. Due to the growing importance of public-private partnerships, the most important of these are presented.

4 Early warning and public outreach: The forth section describes national organizations responsible for CIIP early warning, namely CIIP-related information-sharing organizations such as CERTs (Computer Emergency Response Teams), ISACs (Information Sharing and Analysis Centers), etc. Reference is made to plans for the development of comprehensive early warning alert and incident report structures. Moreover, public outreach initiatives are depicted.

5 Law and legislation: The fifth section lists important legislation enacted for the promotion of CIIP. This includes acts defining the responsibilities of the government authorities in case of emergencies as well as legislation dealing with issues such as technical IT security, data protection, damage to data, fraudulent use of a computer, the handling of electronic signatures, etc.

To cover some of the important topics in more detail, this volume is supplemented by a second volume on "Analyzing Issues, Challenges, and Prospects", in which various experts express their view on issues of high relevance in the field of CIIP.

Part II Survey of International Protection Policies

It is well known that threats to CIP/CIIP do not respect functional or geographic boundaries, and that the various sectors share cross-border vulnerabilities and interdependencies. This is especially true as all infrastructures rely on energy and telecommunications for support. All of the above factors strengthen the case for making CIP/CIIP an international co-operative effort: strong international partnerships between governments and critical infrastructure owners and operators are becoming essential. The security of cyberspace has become an important consideration in most countries, and governments worldwide are already putting a fair amount of effort into cyber-security. The 2003 WSIS

Declaration of Principles[9] and two succeeding UN resolutions[10] rightly state that a global culture of cyber-security is a prerequisite for the development of the information society and for building confidence among users of ICTs.

Many international organizations are dealing with this challenge and have taken steps to raise awareness, establish international partnerships, and agree on common rules and practices. In its second part, this edition of the CIIP Handbook looks at protection policies by international organizations and institutions, namely the European Union (EU), the G8 Group, the North Atlantic Treaty Organisation (NATO), the Organisation for Economic Co-operation and Development (OECD), the United Nations (UN), and the World Bank Group.

Methodology

The surveys were compiled in a three-step procedure.

1. First, open-source material was collected from online resources, publicly available government papers, workshops, and conference proceedings. This information was used to write a first draft of the country surveys. However, the availability of this open-source information, and especially the availability of documents on the internet, varies considerably in quantity and quality from country to country. Additionally, much of the relevant information is only available in the original language. [11]
2. The second and most important step was the collaboration with the national experts from government and government-related organiza-

9 World Summit on the Information Society (WSIS). Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium. Document WSIS-03/GENEVA/DOC/4-E, (12 December 2003). http://www.itu.int/wsis/docs/geneva/official/dop.html; World Summit on the Information Society. Plan of Action. Document WSIS-03/GENEVA/DOC/5-E, (12 December 2003). http://www.itu.int/wsis/docs/geneva/official/poa.html.

10 In UN Resolution 57/239 of December 2002, the UN General Assembly outlined elements for creating a global culture of cyber-security, inviting member states and all relevant international organizations to take account of them in their preparations for the Summit. In December 2003, UN Resolution 58/199 further emphasized the promotion of a global culture of cyber-security and the protection of critical information infrastructures.

11 All links last checked on 30 January 2006.

tions in the field. Whenever possible, at least two experts per country were consulted for reviews. The experts were asked to correct, complete, and update the draft country surveys.[12]

3 Finally, all of the national experts' input was worked into the final version of the country studies.

Since expert input was crucial for all country surveys, it is obvious that the individual perspectives and viewpoints of the consulted experts had a significant impact on the end result. This is also one of the major reasons why the individual surveys differ considerably in focus and general direction, and in their understanding of the nature of CIIP.

The Handbook includes an extensive appendix, which contains a bibliography for each country, a collection of links, and a list of experts involved. In addition, the "Countries at a Glance" pages provide a quick overview of the most important actors and documents in each country.

The Handbook is aimed mainly at security policy analysts, researchers, and practitioners. It can be used either as a reference work for a quick overview of the state of the art in CIIP policy formulation, or as a starting point for further, in-depth research. As the information revolution is an ongoing and dynamic process that is fundamentally changing the fabric of security and society, continuing efforts to understand these changes are necessary. This requires research into information-age security issues, the identification of new vulnerabilities, and new ways for countering threats efficiently and effectively. The International CIIP Handbook is a small contribution towards this ambitious goal.[13]

12 The authors tried to include all the opinions of the persons contacted. In the final version, however, the Handbook represents solely the authors' views and interpretations. Without the invaluable support and help of these experts, however, this work would not have been possible. The deadline for information-gathering and expert input was 30 November 2005. More recent developments could not be considered in this edition.

13 The entire publication is available on the internet at http://www.crn.ethz.ch. We kindly ask the reader to inform us of any inaccuracies or to submit any comments regarding the content.

Part I
CIIP Country Surveys

Australia

Critical Sectors

The Australian government takes an all-hazards approach to the protection of critical infrastructures, whether information-based or not. It defines critical infrastructures as "infrastructure which, if destroyed, degraded or rendered unavailable for an ext ended period, would significantly impact on social or economic well-being or affect national security or defence".[14] Australia's national information infrastructure (NII) is defined as "a subset of the critical infrastructure which comprises the electronic systems that underpin critical services such as telecommunications, transport and distribution, energy and utilities, and banking and finance".[15] The prime minister has defined the aim of critical information infrastructure protection (CIIP) as "to assure Australians

* The Country Survey of Australia 2006 was reviewed by Alex Webling and Patrick Drake-Brockman, Attorney-General's Department, Australian government.

14 Attorney-General's Department National Security Website (http://www.ag.gov.au/). http://www.nationalsecurity.gov.au/www/nationalsecurityHome.nsf/Web+Pages/5C51DE424EB541C2CA256C95000A8DDA?OpenDocument.

15 Attorney-General's Department, Protecting Australia's National Information Infrastructure. Report of the Interdepartmental Committee on Protection of the National Information Infrastructure. (Canberra, December 1998), pp. 7–8.

that both the physical safety of key assets as well as the information technology systems on which so many of them depend are protected".[16]

The scope of Australian critical infrastructure includes the following items:[17]

- Communications (Telecommunications (Phone, Fax, Internet, Cable, Satellites) and Electronic Mass Communications),
- Energy (Gas, Petroleum Fuels, Refineries, Pipelines, Electricity Generation and Transmission),
- Banking and Finance (Banking, Finance, and Trading Exchanges),
- Food Supply (Bulk Production, Storage, and Distribution),
- Emergency Services,
- Health (Hospitals, Public Health, and Research and Development Laboratories),
- Icons and Public Gatherings (Buildings (e.g., Sydney Opera House), Cultural, Sport, and Tourism),
- Transport (Air Traffic Control, Road, Sea, Rail and Inter-modal (Cargo Distribution Centers)),
- Utilities (Water, Waste Water, and Waste Management).

Past and Present Initiatives and Policies

National Counter-Terrorism Plan (NCTP)

The "National Counter-Terrorism Plan (NCTP)"[18] of June 2003 and its second edition of September 2005 both contain a special section dealing with critical infrastructure protection (CIP). The latter says that the NCTC has primary responsibility for the oversight of the protection of critical infrastructures from terrorism. In general, however, CIP is a shared responsibility of business and the

16 Media release from Australian Prime Minister John Howard's office, see: http://www.pm.gov.au/news/media_releases/2001/media_release1367.htm.
17 Attorney-General's Department National Security website, with additions.
18 Ibid.

Australian federal, state, and territory governments. In the field of CIIP, it is stated that the Attorney-General's Department coordinates arrangements.[19]

The government's aim is to ensure adequate levels of protective security for critical infrastructure in place, to minimize the number of individual points of failure, and to provide rapid recovery arrangements. The Australian government takes actions in the following fields:

- Identifying Australia's critical infrastructure and determining broad areas of risk;
- Assisting businesses in mitigating their risk through business-government partnerships, e.g., the Trusted Information Sharing Network (TISN) and Infrastructure Assurance Advisory Groups (IAAGs), and through state and territory governments;
- Promoting domestic and international best practices in CIP.[20]

Organizational Overview

Public Agencies

The e-Security Coordination Group (ESCG) is the standing interdepartmental committee with responsibility for e-security policy, whilst another standing interdepartmental committee, the Information Infrastructure Protection Group (IIPG), examines NII strategic policy.

e-Security Coordination Group (ESCG)

In November 2000, in recognition of the increasing reliance of government, business, citizens, and consumers on networked technologies, the scope of

19 National Counter-Terrorism Plan (2nd ed.), September 2005 (Commonwealth of Australia, 2005). http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/(5738DF09EBC4B7EAE52BF217B46ED3DA)~NCTP_Sept_2005.pdf/$file/NCTP_Sept_2005.pdf.

20 Australian Government, Protecting Australia against Terrorism, p. 32–33. http://www.pmc.gov.au/publications/protecting_australia/docs/protecting_australia.pdf.

Commonwealth security policy was broadened to encompass a national approach to e-security.

The ESCG, chaired by the Department of Communications, Information Technology & the Arts (DCITA), is the Commonwealth's policy coordination body on e-security matters. It is attended by government policy and law enforcement agencies and is concerned with e-security issues affecting the broader economy and the community.

- The ESCG addresses a range of issues, including:
- Awareness-raising,
- Authentication,
- e-Security skills,
- Research and development,
- Biometrics.

Department of Communications, Information Technology & the Arts (DCITA)

The Department of Communications, Information Technology & the Arts (DCITA) participates in the Australian government's CIP activities through TISN. It chairs and provides secretariat support to the IT Security Expert Advisory Group (ITSEAG). The ITSEAG provides advice to the Trusted Information Sharing Network (TISN) on current and emerging security issues affecting owners and operators of critical infrastructure, including:

- Voice over Internet Protocol (VoIP) enterprise systems,
- Supervisory Control and Data Acquisition (SCADA) systems,
- Wireless services.

DCITA also provides the secretariat for the Communications Sector Infrastructure Assurance Advisory Group (CSIAAG) of the TISN, which has developed an all-hazards risk management framework for the national critical communications infrastructure.

Australian Government Information Management Office (AGIMO)

The Australian Government Information Management Office (AGIMO), located within the Department of Finance and Administration, provides strategic advice, activities, and representation relating to the application of ICT to government administration, information, and services.
AGIMO's functions and responsibilities include:

- Promoting improved government services through technical interoperability and the integration of business processes across Australian government services and with state/territory and local authorities;
- Developing and enhancing government e-procurement processes;
- Promoting comprehensive telecommunications arrangements for the entire government;
- Identifying and promoting the development of ICT infrastructure necessary to implement emerging strategies for the entire government;
- Developing an e-government Authentication Framework to assist people in verifying electronic communications.

In cooperation with other government bodies, AGIMO manages international contacts and represents Australia in world forums on ICT related issues. AGIMO also manages the gov.au domain in consultation with state and territory governments.[21]

Information Infrastructure Protection Group (IIPG)

The Information Infrastructure Protection Group (IIPG) is an interdepartmental committee of the Australian government responsible for providing policy coordination and/or technical response in relation to threats to the National Information Infrastructure (NII). The IIPG is chaired by the Attorney-General's Department, and its members include the Defence Signals Directorate (DSD), the Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP), the Department of the Prime Minister and Cabinet (PM&C), the Australian Government Information Management Office (AGIMO), the Attorney-General's Department's (AGD), the Department of Communications,

21 http://www.agimo.gov.au.

Information Technology and the Arts (DCITA), the Department of Transport and Regional Services (DOTARS), and the Department of Foreign Affairs and Trade (DFAT).

Defence Signals Directorate (DSD)

The Defence Signals Directorate (DSD) is Australia's national authority on information security and signals intelligence. DSD plays an integral role in the protection of Australia's official communications and information systems. It does so by providing expert assistance to Australian agencies in relation to cryptography, network security, and the development of guidelines and policies on information security.

The activities of the DSD's Information Security Group (INFOSEC) include information and incident collection, analysis and warning services, setting awareness and certification standards, and defensive measures, including protective security measures, response arrangements, and contingency planning. In addition to its support for Australian government departments and authorities, INFOSEC also plays an important role working with industry towards the development of new cryptographic products.[22]

Australian Security Intelligence Organisation (ASIO)

The Australian Security Intelligence Organisation (ASIO) is Australia's national security service. Its functions are set out in the Australian Security Intelligence Organisation Act 1979 (the ASIO Act). ASIO's main role is to gather information and produce intelligence that will enable it to warn the government about activities or situations that might endanger Australia's national security. The ASIO Act defines "security" as the protection of Australia and its people from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defense system, and acts of foreign interference. Some of these terms are further defined in the ASIO Act.[23]

22 http://www.dsd.gov.au.
23 http://www.asio.gov.au.

The Australian Federal Police (AFP)

The introduction of the Cybercrime Act (2001) prompted the Australian Federal Police (AFP) to join forces with state and territory police to create a national organization to address the threat of cyber-crime. The distinction between cyber-crime and cyber-terrorism is blurred because many of the tools and techniques are common to both activities. Consequently, the creation of the Australian High Tech Crime Centre (AHTCC) was a major and important CIIP measure. The AHTCC provides a national coordinated approach to dealing with instances of high-tech crime affecting the Australian jurisdiction, including the investigation of electronic attacks against the National Information Infrastructure.[24]

Public-Private Partnerships

The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN)

Building on the recommendations of the first Consultative Industry Forum (CIF),[25] the prime minister in November 2001 announced the formation of the Business-Government Task Force on Critical Infrastructure. The task force recommended replacing the CIF with a "learning network" to share information about critical infrastructure protection. In 2002, the government announced the creation of a Trusted Information-Sharing Network for Critical Infrastructure Protection (TISN).[26] The TISN and its Critical Infrastructure Advisory Council (CIAC) were established on 29 November 2002.[27]

The TISN is a forum in which the owners and operators of critical infrastructure work together to share information on security issues that affect critical infrastructure. The TISN is made up of nine Infrastructure Assurance Advisory Groups (IAAGs) for different business sectors and three expert advisory groups that focus on IT Security, future issues, and the built environment. Each IAAG is represented on the CIAC, which is chaired by the

24 http://www.ahtcc.gov.au.
25 This Forum resulted from the government's first report in the CIIP field, NII Report 1998, op. cit.
26 http://www.cript.gov.au.
27 Ibid.

Attorney-General's Department, and also includes representation from the states and territories and relevant Australian government agencies.

Infrastructure Assurance Advisory Groups (IAAGs)
TISN IAAGs have been formed for the key sectors of communications, energy, banking and finance, iconic landmarks and public gathering places, transportation, the food chain, health, water services, and emergency services. The IAAGs were created to allow the owners and operators of critical infrastructure to share information on shared threats, vulnerabilities, and appropriate measures and strategies to mitigate risk.

The participation of government agencies in the sector groups will assist in a greater understanding of issues by the government, and allow industry to be briefed on government activity. The Attorney-General's Department assists the IAAGs in collaborating on issues related to common threats, vulnerabilities, and interdependence.[28]

Early Warning and Public Outreach

There are two key organizations that provide comprehensive early-warning services for cyber-attacks in Australia. The Defence Signals Directorate (DSD) has the remit to assist Federal and State/Territory IT networks, and the Australian Computer Emergency Response Team (AusCERT) provides some similar services to private sector operators of CI. In addition, the Australian government has launched the OnSecure website, run by DSD.

Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS)

The Defence Signals Directorate (DSD) manages the Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS). The function of the ISIDRAS is the collection of information on security incidents that affect the security or operability of Australian Commonwealth Government computer and communication systems.

28 http://www.pmc.gov.au/publications/protecting_australia/docs/protecting_australia.pdf.

The ISIDRAS facilitates high-level analysis of information security incidents with the aim of improving knowledge of both threats and vulnerabilities to Australian government information systems and about how to protect these systems more effectively. ISIDRAS provides regular reporting of incidents. Information derived from these reports is used as a basis for threat assessments and security advice.

OnSecure Website

OnSecure is a joint initiative between the Defence Signals Directorate (DSD) and the Australian Government Information Management Office (AGIMO) to assist Australian government agencies in dealing with information security breaches and incidents. Government agencies are able to report any information security incidents online via the OnSecure website. DSD manages the website and also analyses incident reports.

OnSecure compliments the Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS) that collects reports by Australian government agencies on information security incidents. The website also has a public view that allows the general public access to resources on information security.[29]

Australian Computer Emergency Response Team (AusCERT)

The Australian Computer Emergency Response Team (AusCERT) is a non-profit organization located at the University of Queensland. It provides an important information security service to the private sector and to some government agencies on a fee-for-service basis. AusCERT's aims are to reduce the probability of successful attacks, to reduce the direct costs of security to organizations, and to lower the risk of consequential damage.[30] In May 2003, the Australian government announced the launch of AusCERT's National Information Technology Alert Service (NITAS),[31] which is sponsored by the federal government. NITAS provides a free service to subscribers, who are mainly owners and operators of the NII.[32]

29 http://www.onsecure.gov.au.
30 http://www.auscert.org.au, and NII Report 1998, p. 2.
31 http://www.nationalsecurity.gov.au/www/attorneygeneralHome.nsf/0/64534A395BA69AF4CA256D24007BDCA2?OpenDocument.
32 http://www.national.auscert.org.au.

Law and Legislation

Electronic Transactions Act 1999

The Electronic Transactions Act of 1999 creates a light-handed regulatory regime for using electronic communications in transactions. It facilitates electronic commerce in Australia by removing existing legal impediments under Commonwealth law that may prevent a person using electronic communications. The Act gives business and the community the option of using electronic communications when dealing with government agencies.[33]

Cybercrime Act 2001

The Cybercrime Act of 2001 amended the Criminal Code Act 1995 (Cth). It also amended the Crimes Act 1914 and the Customs Act 1901 to enhance the applicability of the existing search-and-seizure provisions relating to electronically stored data. It gives federal law enforcement agencies the authority to investigate and prosecute groups who use the internet to plan and launch cyber-attacks (such as hacking, computer virus propagation, or denial-of-service attacks) that could seriously interfere with the functioning of the government, the financial sector, and industry. The offenses and investigation powers were drafted in a manner to make them consistent with the draft of the Council of Europe's Cybercrime Convention.
The act covers:

- Unauthorized modification of data to cause impairment;
- Unauthorized impairment of electronic communication;
- Unauthorized access to, or modification of, restricted data;
- Unauthorized impairment of data stored on a computer disk, etc.;
- Possessing, producing, supplying, or obtaining data with intent to commit a computer offense;
- Causing an unauthorized computer function with intent to commit a serious offense.

33 http://www.ag.gov.au/agd/WWW/securitylawHome.nsf/Page/e-commerce_Electronic_Transactions_Act_-_Advice_for_Commonwealth_Departments.

The offenses were drafted in a way that recognizes the inter-jurisdictional character and extend to situations where:

- The conduct occurs wholly or partly in Australia;
- The result of the conduct occurs wholly or partly in Australia; or
- The offender was an Australian citizen or Australian company.

Security Legislation Amendment (Terrorism) Act 2002

The Security Legislation Amendment (Terrorism) Act 2002[34] amended the Criminal Code Act 1995 to:

- Create a new offense of engaging in a terrorist act and a range of related offenses;
- Modernize Australia's treason offense; and
- Create offenses relating to membership in or other specified links with a terrorist organization.

An organization can be listed in regulations if the attorney-general is satisfied that the organization is a terrorist organization and that the organization has been identified in a decision of the United Nations Security Council relating to terrorism. A court may also find that an organization is a terrorist organization.[35]

The act also specifically outlawed cyber-terrorism: "The action or threat of action which seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to information, telecommunications and financial systems […]. The action is done or the threat is made with the intention of: advancing a political, religious or ideological cause; and coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country (or part of)."[36]

34 Security Legislation Amendment (Terrorism) Act 2002, No. 65, 2002. An Act to enhance the Commonwealth's ability to combat terrorism and treason, and for related purposes. http://scaleplus.law.gov.au/html/comact/11/6499/pdf/0652002.pdf.

35 http://www.nationalsecurity.gov.au/agd/www/NationalSecurityHome.nsf/Page/RWPA41035442ED47EF7CA256D6A001215A5?OpenDocument.

36 Security Legislation Amendment (Terrorism) Act 2002, op. cit.

Spam Act 2003

Australia's anti-spam legislation was introduced in 2003 in response to concerns about the impact of spam on the effectiveness of electronic communication and the costs imposed on end-users. The Spam Act 2003 prohibits the sending of spam, which is defined as a commercial electronic message sent without the consent of the addressee via e-mail, short message service (SMS), multimedia message service (MMS), or instant messaging. The requirements under the Spam Act apply to all commercial electronic messages, including both bulk and individual messages. The Australian Communications and Media Authority (ACMA) has enforcement responsibility for the Spam Act.

In September 2005, the minister directed the Department of Communications, Information Technology and the Arts to initiate a review of the Spam Act, as required by legislation.[37]

37 http://www.dcita.gov.au/ie/spam_home.

Austria

Critical Sectors

The origins of today's dangers and risks to the state, the society, and the individual may be found in the fields of politics, the economy, the military, society, the environment, culture and religion, and information technology. Information and communication technology has acquired a dimension of its own in security policy because it links all other security aspects, thus becoming a power factor in its own right and leaving room for many options. Austria as a modern society[38] and as a small state is particularly vulnerable in the area of information. This includes both the military and the civilian sectors,[39] and increasingly business and industry as well.[40]

* The Country Survey of Austria 2006 was reviewed and updated by Thomas Pankratz, Austrian Federal Ministry of Defense, Bureau for Security Policy. His contribution was written in his private capacity and does not reflect the official position of the Austrian Ministry of Defense. Dr. Pankratz would like to express his gratitude for the research assistance of Nieves Kautny and Ralph Schöllhammer, University of Vienna. In addition, Gerald Trost, Stabsstelle IKT-Strategie des Bundes, Federal Chancellery of the Republic of Austria and Otto Hellwig, former official of the Federal Chancellery, provided valuable input.

38 According to a study, more than 50 per cent of the Austrian population use the internet; the use of the internet within the EU is around 47 per cent. In: Der Standard, 12 November 2005.

39 As in many other states, most of the Critical Infrastructure and Critical Information Infrastructure (around 80–90 per cent) is in the possession of private owners.

40 Resolution by the Austrian parliament: Security and Defense Doctrine: Analysis – Draft expert report of 23 January 2001.

Until now, there is no clear definition of Critical Infrastructure (CI) or Critical Infrastructure Protection (CIP) in Austria. To arrive at such definitions will be part of a strategy for the protection of critical infrastructure. Most probably, a future Austrian definition will be consistent with the definition elaborated by the EU (see chapter on the EU in this book). According to the European Union Green Paper on a European Programme for CIP, critical infrastructures include the following sectors and services:

- Energy (Oil and Gas Production, Refining, Treatment and Storage, including Pipelines; Electricity Generation; Transmission of Electricity, Gas and Oil; Distribution of Electricity, Gas and Oil),
- Information and Communication Technologies (Information System and Network Protection; Instrumentation Automation and Control Systems (Supervisory Control and Data Acquisition SCADA etc.), Internet; Provision of Fixed Telecommunications; Provision of Mobile Telecommunications; Radio Communication and Navigation; Satellite Communication; Broadcasting),
- Water (Provision of Drinking Water; Control Water Quality; Stemming and Control of Water Quantity),
- Food (Provision of Food and Safeguarding Food Safety and Security),
- Health (Medical and Hospital Care; Medicines, Serums, Vaccines and Pharmaceuticals; Bio-Laboratories and Bio-Agents),
- Financial (Payment Services/Payment Structures (private); Government Financial Assignment),
- Public and Legal Order and Safety (Maintaining Public and Legal Order; Safety and Security; Administration of Justice and Detention),
- Civil Administration (Government Functions; Armed Forces; Civil Administration Services; Emergency Services; Postal and Courier Services),
- Transport (Road Transport; Rail Transport; Air Traffic; Inland Waterways Transport; Ocean and Short-Sea Shipping),
- Chemical and Nuclear Industry (Production and Storage/Processing of Chemical and Nuclear Substances; Pipelines of Dangerous Goods (Chemical Substances)),
- Space and Research (Space; Research).[41]

Past and Present Initiatives and Policies

Following the "Security and Defense Doctrine of 2001", which can be seen as the guideline of Austria's security and defense policy, security in all its dimensions is the basic prerequisite for the existence and functioning of a democracy as well as for the economic welfare of the community and its citizens. Therefore, security must be conceived and implemented within a comprehensive security policy.[42]

There have been several organizational and procedural efforts since the 1990s to manage CIP/CIIP in Austria. The issue of CIIP has been addressed by the government, especially by the Ministry of Internal Affairs, the Ministry of Defense, the Ministry of Traffic, Infrastructure and Technology, and the Federal Chancellery, which has taken the leadership and is the central point in different projects.

Although there have been such initiatives, there is still no stringent, congruent, coordinated CIP/CIIP concept designated as such in a narrow sense in Austria. In autumn of 2005, the Federal Chancellery started an initiative to develop a strategy for the protection of critical infrastructure. All relevant ministries are involved in the process of developing this strategy. The sub-strategy will contain and define the following: Political and legal basics, definition of critical infrastructure, actors and responsibilities, risks and scenarios, strategic aims, procedures, organizational framework, and measures. The strategy will follow a comprehensive approach (all-hazards approach). Therefore, it aims at the protection of the entire infrastructure and will not focus exclusively on the protection of the critical information infrastructure.

On the European level, Austria takes part in all relevant EU activities regarding the protection of critical infrastructures, such as the "European Program for the Protection of Critical Infrastructure (EPCIP)" and the "Critical Infrastructure Warning Information Network (EUCIWIN)". Austria, like most other EU member states, shares the opinion that the protection of critical infrastructures has to follow the so-called "subsidiarity principle", which means that the protection of the critical infrastructure is primarily the task of the member states. Activities of the EU are seen as complementary measures.

41 Commission of the European Communities. Green Paper on a European Programme for Critical Infrastructure Protection, (Brussels, 17 November 2005), COM(2005) 576 final, p. 24.

42 Analysis – Draft expert report of 23 January 2001, op. cit., p. 4.

Security and Defense Doctrine 2001

According to the principle of comprehensive security, the "Security and Defense Doctrine"[43] recommends the development of the existing "Comprehensive National Defense Program" into a system of "Comprehensive Security Provision" by focusing on the new risks and threats and by amending legal provisions.[44] One can therefore deduce that this will also include all measures referring to CIIP.[45] This doctrine clearly stresses that for small states, full and unimpaired access to the information they require is a basis for their freedom of action in security matters.[46]

The implementation of Austria's security policy within the framework of the "Comprehensive Security Provision" relies on systematic co-operation among various policy areas on the basis of appropriate sub-strategies.

e-Government Program

The government program for the year 2000 recommended the implementation of e-government in Austria. This is an essential part of the already mentioned ICT sub-strategy and consists of the following projects: the citizen card, ELAK (Electronic File), and the seal of e-government approval. "e-Government"[47] refers to two channels of communication: First, electronic communication between citizens and the public administration (G2C),[48] and secondly, communication between different branches of the public administration (G2G). Referring to

43 http://www.bka.gv.at/2004/4/18/doktrin_e.pdf.

44 Security and Defense Doctrine, op. cit.

45 The concept of "Comprehensive National Defense" as developed from 1961 onwards was embedded in the Constitution in 1975. Under Article 9a of the Austrian Constitution, the role of Comprehensive National Defense is to "maintain [Austria's] independence from external influence as well as the inviolability and unity of its territory, especially to maintain and defend permanent neutrality". Together with the constitutional amendment, the Austrian parliament unanimously adopted a resolution in 1975 "on the fundamental formulation of Comprehensive National Defense in Austria" (defense doctrine). These were the foundations of the national defense plan, which was adopted by the Austrian government in 1983 and identified the "protection of the country's population and fundamental values from all threats" as a basic goal of Austrian security policy.

46 Security and Defense Doctrine, op. cit.

47 On the implementation of e-government in Austria, see: http//www.bka.gv.at and http://www.cio.gv.at/egovernment.

48 On the methodology, basic principles, structure, and examples of this topic, see: Hollosi, Arno. Sicherheit mit offenen Standards für die Verwaltung (Vienna, 2002).

G2C, the target was to make all administrative channels accessible by electronic communication until the end of 2005. In concrete terms, this means that official forms no longer need to be downloaded, filled out, and physically returned to the responsible department. Instead, it should be possible to fill out forms directly on screen, and send them to the department concerned with an electronic signature.[49] Another aim in this field is to offer all citizens and companies one virtual point of contact that supplies them with the required information, and also takes care of transmitting the necessary administrative procedures to the responsible department.[50]

To make the Austrian e-government secure, the Austrian seal of approval for e-government was developed by the ICT board.[51] This seal of approval is only issued by the Federal Chancellor Office under certain conditions, which must be fulfilled for three years. After that period, approval can be renewed. One essential part of the whole project is the guideline paper on "Network Safety in the Field of e-Government".[52]

At the G2G level, Austria has also made big steps forward, and its ranking is at the top of the EU states. Thanks to the introduction of the so called ELAK,[53] it is possible for different ministries or other public offices to work simultaneously on the same record using electronic forms instead of paper. Since the end of 2005, the Ministry of Defense and other departments are connected to this system, and the harmonization process completed.

IT Strategy of the Government

The IT strategy of the government was formulated in July 2001, based on a decision of the Council of Ministers of 6 June 2001 referring to the "New Structuring of the IT Strategy of the Government". It was located at the Ministry of Public Service and Sports and moved to the Federal Chancellery in 2003. The strategy consists of the following three service types: Administration and Public Relations, Techniques and Standards, and Project Management and International Affairs.

49 http://www.cio.gv.at/egovernment.
50 This is the so-called "One Stop Principle".
51 http://www.cio.gv.at/egovernment.
52 "Netzwerksicherheit im Bereich e-Government".
53 "Elektronischer Akt" (electronic file).

A special body, the ICT Board, was established to guarantee a strategic co-ordination of ICT within the framework of the public government. This board comprises all chief information officers of all ministries and is located at the Federal Chancellery.

Citizen Card

The aim of this project, which was launched in January 2003, is to reconsider the concept of a Citizen Card.[54] This is a chip card with encrypted information from the central registration office. The test run was initiated by the national provider of digital signature cards[55] (a.trust), the Austrian Computer Society, and the ICT board of the Federal Chancellery.[56] The citizen card is seen as a mixture of official identification document and an electronic signature for verifying electronic administration procedures. Together with the G2C concept, it is possible for the officials to identify the citizen in electronic communication. However, it has not yet met with the expected response from the official institutions.[57]

ICT Security Sub-Strategy

According to the Security and Defense Doctrine, the government had to work out sub-strategies for all areas relevant to security policy based on the recommendations on security and defense policy. These sub-strategies, which are adopted by the end of 2005, should be continuously reviewed, coordinated, and, if necessary, adjusted in accordance with the international framework conditions.[58] In particular, the sub-strategies should relate to the areas of foreign

54 For more information, see: http://www.buergerkarte.at/index.html.

55 The digital signature became legally valid in 2003.

56 Kurier, 28 November 2002.

57 One of the reasons could be investment incurred by citizens who had to buy a card-reading machine and to pay a registration fee and a regular fee each year, in addition to the cost of upgrading a bank card, which is free until the end of 2005. By the beginning of 2005, only 30,000 people – mostly in the business sector – had signed on as users. But expectations are still high: 200,000 new users are expected by the end of 2005, and for 2007 the number should rise to 800,000. Cf. http://futurezone.orf.at/futurezone.orf?read=detail&view=bw&id=261340, 20 November 2005. By this date, buying cigarettes from a vending machine should only be possible by paying with a bank card on which the birth date of its carrier should be stored, thus preventing people younger than 16 years of age from buying tobacco from machines.

58 These sub-strategies are: Teilstrategie Verteidigungspolitik (Defense Policy), Teilstrategie Innere Sicherheit (Internal Security), Teilstrategie ICT-Sicherheit (Information and Communication

policy, defense policy, and internal security. References to CI/ CII can be found in nearly all of these sub-strategies.

The Federal Chancellery and the Ministry of Internal Affairs cooperated to elaborate a special sub-strategy on ICT security. This sub-strategy is divided into four parts:

- Overview of the status quo of IT security,
- Risk analysis,
- Strategies,
- Measures.[59]

Zentrales Ausweichsystem (ZAS)

After a fire at the National Library at the end of the 1970s, the government decided to establish an alternative replacement system for the data stock of the government. This system is located in the so-called "Einsatzzentrale Basisraum" (EZB) in St. Johann/Salzburg. Due to its coordinative function in the procurement of IT technologies, the Federal Chancellery has been responsible for the development of the EZB.[60]

The "Zentrale Ausweichsystem" (ZAS) has been a central part of the governmental crisis prevention system since the 1980s and has been fully operational on a day-to-day basis ever since. Some fundamental and very important systems (like the law information system/RIS) are run by this system. It has been continually modernized and adapted. However, a comprehensive storage of public data has never been achieved, and it has only been used continually by the regional government of Salzburg. It has been suggested to offer this system to private users, but this idea is still under discussion.[61]

Technology Security), Teilstrategie Verkehrs- und Infrastrukturpolitik (Traffic and Infrastructure Policy), Teilstrategie Wirtschaftspolitik (Economy Policy), Teilstrategie Landwirtschaftspolitik (Agriculture Policy), Teilstrategie Finanzpolitik (Financial Policy), Teilstrategie Außenpolitik (Foreign Policy), Teilstrategie Bildungs- und Informationspolitik (Education and Information Policy).

59 http://www.bmi.gv.at and http://www.austria.gv.at.

60 The ZAS is located on an installation of the Austrian military; therefore, not much is publicly known about the institution itself.

61 Interview with a representative of the Federal Chancellery.

Official Austrian Data Security Website

The Official Austrian Data Security Website,[62] which is coordinated by the Federal Chancellery, serves as an information desk for citizens in important matters such as data security, the Schengen Information System, Europol, etc. It also informs the public about the work of the Commission on Data Protection, whose reports are available on the website. It also serves as a complaint board for citizens who want to report violations of their data privacy.

Organizational Overview

Public Agencies

At the public level, no single central authority is responsible for CII/CIIP, which is considered to be a cross-agency task. However, the Federal Chancellery fulfils a coordinating task. CIIP is mainly addressed by the Ministry of Internal Affairs, the Ministry of Defense, and the Ministry of Traffic, Innovation, and Technology.

The Austrian Parliament and the Ministries

All ministries have their own specific security measures and special departments for ICT technologies. A chief information officer leads these departments.[63] The security concept of the ministries is based on two pillars: Pillar 1 refers to organizational and procedural measures for the internal network in general. Pillar 2 refers to technical means for the protection of sensitive data. This is guaranteed by three safeguards: Firewalls, virus protection, and intrusion detection systems.[64] These measures are especially important in the ministries dealing with national security and/or personal or other sensitive data, such

62 http://www.dsk.gv.at/indexe.htm.

63 The IT Security Handbook of the government provides guidelines for CII security measures; these measures are implemented and realized by the ministries at their own discretion.

64 Interview with a representative of the Ministry for Social Security, Generations and Consumer Protection.

as the Ministry of Defense, the Foreign Ministry, or the Ministry of Internal Affairs.

The Austrian parliament, as well as most other public or semi- public institutions, is also taking a number of measures to prevent any unauthorized use of its data.

Ministry of Internal Affairs (BMI)

Several divisions of the Ministry of Internal Affairs (BMI) deal with CIIP, especially with aspects of data security and cyber-crime. The Criminal Police's homepage issues information on internet security. The Center for the Fight against Internet Crime was established in August 1999 under the auspices of the BMI.[65] The Austrian Cyberpolice represent Austria in the European Network of Forensic Science Institutes on Computer Crime (ENFSI).[66]

The Federal Agency for State Protection and Counter-Terrorism (BVT) is part of the Ministry of Internal Affairs. Division 3 of the BVT is responsible for the coordination of personal security and the security of objects. In addition, it evaluates and develops the ability to provide protection on a permanent basis with regard to possible new threat scenarios. Responsibility for advanced security and examinations also rests with Division 3.

The BMI also serves as point of contact for European initiatives concerning Critical Infrastructure Protection.

Ministry of Defense

In the framework of the Ministry of Defense, Department II (also known as the "control department") is responsible for all aspects of information warfare. It fulfills its duties in close cooperation with the Leadership Support Command[67] and the two military intelligence services.[68] One of these, the "Abwehramt",

65 The Center for the Fight against Internet Crime has been part of the Federal Criminal Office since 2001.

66 http://www.bmi.gv.at.

67 The Austrian armed forces and the Ministry of Defense are currently undergoing reform, so that a change in responsibilities is possible.

68 "Heeresnachrichtenamt" and "Heeresabwehramt". Interview with a representative of the Ministry of Defense.

which is responsible for the protection of the army itself, also has a special department called "Electronic Defense".[69]

The Austrian Federal Constitution and the Defense Law determine the cooperation between the army and civil authorities in crisis situations if the latter are not able to guarantee the maintenance of public order and inner security themselves. Part of this is the protection of civilian installations against interference by unauthorized third parties, including the protection of critical information infrastructures.

The final report of the Politico-Military Commission,[70] which was released in autumn 2004, recommends that the Austrian armed forces be given an important role in the protection of the vital, civilian ICT, as well as the capacity to provide redundant systems in case of catastrophes or threats.[71]

These protective measures have been tested in several exercises held in close co-operation with the civilian institutions. The largest maneuver of this kind in Austria took place in the federal states of Carinthia and Styria from 13–16 April 2004. The "Schutz 2004" maneuver was planned and executed as a security assistance mission under the leadership of the civil authorities.

Ministry for Traffic, Innovation and Technology (BMVIT)

The Ministry for Traffic, Innovation, and Technology (BMVIT) is responsible for the safety of the public critical infrastructure. It operates a coordinating center for private owners and operators of critical infrastructure, and a center for security research. One of its recent activities has been to order an ICT master plan that would analyze the strengths and weaknesses and the state of the art of Austria's critical infrastructure. Another part of this mandate consisted in presenting options for measures, targets, missions, and visions.[72] The BMVIT is also coordinating the Austrian Security Research Program, in which critical infrastructure protection plays an essential part.[73]

69 The chief of this department, Colonel Walter J. Unger, published several articles concerning IT security and cyberterrorism. See for example: Unger, Walter J. and Heinz Vetschera. "Cyber War und Cyber Terrorismus als neue Formen des Krieges". In: Österreichische Militärische Zeitschrift, No. 2 (2005), pp. 203–211; Unger, Walter J., "Angriff aus dem Cyberspace I-III". In: Truppendienst No. 2 (2004), pp. 143–147; No.3 (2004), pp. 271–275; No. 4 (2004), pp. 382- 386.

70 Bundesheerreformkommission.

71 Bundesheerreformkommission. Endbericht (Vienna, 2004), pp. 49–50.

72 http://www.bmvit.gv.at.

73 http://www.kiras.at/wDeutsch/index.php and http://www.bmvit.gv.at/innovation/sicherheitsforschung/index.html.

Board of Information and Communication Technology Strategy (ICT Board)

The Board for Information and Communication Technology Strategy[74] (ICT Board) was established in July 2001 as part of the Chief Information Office and was based on a decision of the Council of Ministers of 6 June 2001 referring to a "restructuring of the government's IT strategy". It is located at the Federal Chancellery. Its core efforts include coordinating the implementation of information and communication technologies, the coordination of electronic information transfer, and the evaluation of the application of those technologies in terms of profitability, usefulness, and austerity.[75]

Government Headquarters for Information and Communication Technology Strategy

The Government Headquarters for Information and Communication Technology Strategy was established in July 2001. The main task of this institution is the coordinated implementation of e-government at all levels of the public administration. It is also responsible for IT security in these areas. Several working groups are tasked with analyzing and advancing awareness of these topics.

The Government Board for Information and Communication Technology Strategy publishes the IT Security Handbook. This handbook gives an overview of IT security in general and informs readers in a broad and comprehensive way about fundamental aspects and measures in the field of IT. The handbook was updated twice in 2003 and 2004, based on the idea that security is a continuous process. It consists of two parts: "IT Security Management", which offers concrete instructions in this field; and "IT Security Measures", which describes standard security measures for IT systems requiring a medium security level.[76]

74 Stabsstelle IKT-Strategie des Bundes.
75 http://www.cio.gv.at/faq/ikt-board.
76 The complete handbook is available at: http:www.cio.gv.at/securenetworks/sihb.

Commission on Data Protection (DSK)

The Commission on Data Protection (DSK) serves as independent control authority that deals with data processing in the public and private sectors.[77] The DSK is located at the Federal Chancellery. All citizens have the right to appeal to this commission if their rights in the field of data security are violated. The commission verifies these claims and takes measures to remedy confirmed violations. The Council on Data Protection has exclusive consultative agendas and periodically publishes the "Report on Data Security".

Public-Private Partnerships

Center for Secure Information Technology Austria (A-SIT)

The Center for Secure Information Technology Austria (A-SIT) was founded in May 1999 as an association supported by the Austrian National Bank, the Ministry of Finance, and the University of Technology in Graz. Its tasks include general monitoring issues of IT security[78] and the evaluation of encryption procedures,[79] as well as supporting the introduction of the Citizen Card, supporting public institutions, and developing a security policy for all important electronic payment systems for the Austrian National Bank. It is also a member of the Computer Incident Response Coordination Austria (CIRCA).

Early Warning and Public Outreach

Austria has an early-warning system for nuclear catastrophes[80] and natural and technical disasters that is based primarily on bilateral treaties and national (public and private) efforts.[81] However, to date, no comprehensive and coordinated

77 For more information, see: http://www.dsk.gv.at/indexe.htm.
78 A-SIT offers tools and demonstration examples on its homepage: http://demo.a-sit.at.
79 http://www.a-sit.at/asit/asit.htm.
80 This is primarily provided by the "Strahlenfrühwarnsystem" (Radiation Early Warning System), which comes under the responsibility of the Ministry of Life (Lebensministerium).
81 The central institution is the Federal Emergency Operations Center, located at the Ministry of Internal Affairs.

early-warning system for attacks on the critical information infrastructure is in place or planned.

Computer Incident Response Coordination Austria (CIRCA)

The Computer Incident Response Coordination Austria (CIRCA) is Austria's main organization in the field of IT early-warning systems. It is a public-private partnership whose main actors are the Federal Chancellery, the Federation of the Austrian Internet Service Providers (ISPA), and the Center for Secure Information Technology Austria (A-SIT). Other members are representatives of the social partners (economic interest groups), the federal states, and of other critical infrastructure providers. It is a web of trust between Internet Service Providers (ISPs), IP network operators from the public and private sectors, and enterprises in the field of IT security. The electronic communication network of the private sector is run by ISPA, whereas the Federal Chancellery has the lead in the public sector.

The aim of this Austrian security net is to provide an early-warning system against worms, viruses, distributed denial-of-service attacks, and other threats that endanger IP networks and their users. Therefore, CIRCA issues alerts and risk assessments and provides information about precautionary measures. It works with a proactive and a reactive strategy, which means a continuous exchange of information and news between the Federal Chancellery and CIRCA.

Law and Legislation

There is a broad variety of legal acts and laws dealing with CII/CIIP in a very broad sense. Most of them refer to the processing, the collection, the transfer, and the protection of (personal) data through or by public agencies (e.g., the police, security agencies).

The general responsibilities of governmental authorities are laid out in the Bundesministeriengesetz (Federal Ministry Law), which defines the agendas of each ministry.

The following can be regarded as the central and most relevant legislative acts:

Information Security Law and Information Security Order

With the Information Security Law[82] and the Information Security Order[83], Austria guarantees the secure use of classified information within the jurisdiction of the federal government according to international law. They regulate the access, transmission, identification, electronic processing, registration, and preservation of classified information. In accordance with international law, information regarding security arrangements within the EU or with other states qualifies as classified information. The Information Security Law specifies four types of classified information:

- "Limited": if the unauthorized transmission of information would be contrary to the interests mentioned in Article 20, paragraph 3 of the Federal Constitution;
- "Confidential": If the information has to be kept secret according to additional federal laws and if maintaining secrecy is in the public interest;
- "Restricted": If the information is confidential and its publication would harm the interests mentioned in Article 20, paragraph 3 of the Federal Constitution;
- "Top Secret": If the information is secret and its publication could seriously damage the interests mentioned in Article 20, paragraph 3 of the Federal Constitution.

Consequently, every type of classification is connected to a certain security infrastructure (building, organizational structures, and personnel).

The Data Security Law therefore only grants access to Confidential, Restricted, and Top Secret information to individuals who have completed an advanced security examination according to paragraphs 55 to 55b of the Security Police Act. In the civilian sphere, this security examination is provided by the Federal Office for Constitutional Protection and Counter-Terrorism.

82 BGBl I Nr. 23/2002.
83 BGBl II Nr. 548/2003.

Data Security Law

The Data Security Law (DSG)[84] contains extensive regulations on the processing of personal data. With this law, Austria adopted the EU guideline for data security of the year 1995. The DSG 2000 stresses the importance of data-security measures and measures to enhance confidentiality for personal data. As a rule, the user of personal data is responsible for ensuring that the information is used in a correct manner, that no unauthorized persons have access to data, that the data is not destroyed, and that its secure storage is guaranteed. The DSG lists the following as civil rights: The fundamental right to a secure processing of personal data; the right of information; the right to have incorrect or wrong data corrected; and the right to have data deleted. Another important part of the DSG's activities is the duty to report. This means that with certain exceptions (e.g., for reasons of national security), all applications for personal data must be reported. Additionally, the Data Security Website contains all necessary information, forms, and addresses for rapid reporting.

Security Police Law

The Security Police Law (SPG)[85] defines the duties and authority of the civilian security services. Several articles and/or sections refer to the collection, transfer, storage, and deletion of personal data,[86] as well as measures to prevent the unauthorized use of data. It also provides special rights for individuals whose privacy has been violated by the security services.[87]

Together with this law, the office of a "legal protection agent"[88] was established as a controlling institution. The main duty of the legal protection agent is to protect the rights of citizens by ensuring that investigations of threats as well as observation and surveillance stay within legal rules.

84 BGBl 165/99; see the explanations given by the Ministry of Internal Affairs; http://www.bmi.gv.at.

85 BGBl 566/91 idF BGBl 85/2000.

86 Cf. especially section 4 of the law "Verwenden personenbezogener Daten im Rahmen der Sicherheitspolizei".

87 Cf. especially section 6 of the law "Besonderer Rechtsschutz".

88 "Rechtsschutzbeauftragter" (ombudsman in charge of protecting the rights of the citizen).

Military Competence Law

In analogy to the Security Police Law, the Military Competence Law (MBG)[89] regulates the tasks and duties of the Austrian armed forces, including the two military intelligence services.[90] The MBG regulates the collection, transfer, and deletion of personal data. Paragraph 55 regulates the rights of citizens in case of disregard of data security measures**.** The MBG also provides for the establishment of the institution of a "legal protection agent" who monitors the legality of measures undertaken by the intelligence services.[91]

Telecommunication Law

The Telecommunication Law[92] (TKG) includes extensive and detailed regulations referring to data security in general, and specific regulations regarding communication exchange. Furthermore, these regulations stipulate confidentiality of telecommunication.[93] The law also states that the suppliers of communication lines are responsible for securing all data. Paragraph 89 obliges the suppliers of communication lines to place all technical means necessary for the surveillance of telecommunication at the disposal of the security agencies.

Austrian Penal Code (StGB)

Several articles of the Austrian Penal Code (StGB) refer to CII/CIIP. Some new regulations were introduced to the Penal Code in 2002:[94]

Paragraph 118a: Unlawfully accessing a computer system: "Unlawfully accessing a computer system" is punishable with a prison sentence up to six months or a fine. It applies not only to illegal access, but also to unauthorized registration on a computer system or to those who offer these possibilities to another person, make them public, or use them to gain benefit. The law also applies to cases where users who are authorized to use part of the system have accessed other parts that are off-limits to them. But an essential element is that a violation of security measures has to have occurred. Thus, if no security

89 BGBl 86/ 2000.
90 Second Section of the Law on Intelligence Services.
91 Paragraph 57 of the law.
92 Telekommunikationsgesetz, BGBl 100/ 1997 idF BGBl 134/ 2002.
93 Chapter 12, "Fernmeldegeheimnis, Datenschutz"; paragraphs 87–101.
94 http://www.cybercrimelaw.net/countries/austria.html.

measures are in place, unauthorized access is not a crime. It is worth mentioning that the perpetrator will only be prosecuted with authorization from the injured party.

Paragraph 119: Infraction of the confidentiality of telecommunications: "Infraction of the confidentiality of telecommunications" is defined in a similar way to violations of the privacy of correspondence. The punishments and the requirement for the prosecution are the same as in paragraph 118a.

Paragraph 119a: Improper interception of data: "Improper interception of data" is punished and prosecuted. It is essential that the intercepted data not be intended for the intercepting person. It does not matter whether the perpetrators intend to use the data for themselves, to make it public, or to offer it to another party. The law makes no distinction between the methods applied.

Paragraph 126b: Disturbance of the operability of computer systems: The elements of the crime of "Disturbance of the operability of computer systems" are directly connected with paragraph 126a. It outlaws the disturbance of systems by introducing or sending data. The authorization of the injured party is not needed for prosecution, because this law applies to the diffusion of viruses, worms, etc.

Paragraph 126c: Abuse of computer programs or access data: This article is a very complex one. It prohibits the abuse of computer programs or access data, such as passwords. It is generally intended to cover Trojans and spy programs, as well as accessing and distributing passwords and access codes for various purposes. However, the maximum punishment is not higher than in the other articles.

Penal Procedure (StPO)

The Penal Procedure (StPO) regulates the special investigation methods for combating organized crime. These methods are provisions for optical and acoustic surveillance by civilian security institutions. The law also regulates the installation of a legal protection agent who monitors the legality of the special investigation methods. According to the StPO, the Minister of Justice is obliged to report annually on the use of special investigation methods to the DSR, the DSK, and the Austrian parliament.[95]

95 Cf. Bundesministerium für Justiz, Gesamtbericht über den Einsatz besonderer Ermittlungsmethoden im Jahr 2001, (Vienna 2002).

In 2004, Austria introduced the European arrest warrant into its Penal Procedure System. It is an EU regulation that simplifies the extradition of persons for trial or for the enforcement of sentences. It comprises a catalog of 32 crimes where no close examination is required for extradition. A major problem is that these 32 offenses are not defined properly. One of these crimes is "cyber-crime", which has given rise to a lot of controversy, because each of the 25 member states may define it in a different way. In the Austrian penal code, for example, there is no such offence as "cyber-crime".

Electronic Signature Law (SigG) 1999

Since 1999, the Electronic Signature Law (SigG)[96] has regulated the admission of electronic signatures in the Austrian legal system. The controlling board is the Austrian Telecom Control Commission, which gives the suppliers the necessary certificates. It also informs its constituency about security measures related to electronic signatures.[97] Since 24 September 2002, it has been fully operational with the Public-Key-Infrastructure (PKI).

96 Signaturgesetz BGBl 1999/ 190.
97 http://www.signatur.rtr.at.

Canada

Critical Sectors

In Canada, critical infrastructure (CI) consists of "those physical and information technology facilities, networks and assets, which if disrupted or destroyed would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada."[98]

Canada's CI is made up of ten sectors with sub-sectors. The identification of these sectors was the result of a dynamic dialog involving domestic stakeholders and the exchange of information on the international scene. The sectors are the following:

- Communications and Information Technology (Telecommunications, Software, Hardware, Networks (Internet)),

* The Country Survey of Canada 2006 was reviewed by Claudia Zuccolo, Public Safety and Emergency Preparedness Canada (PSEPC). In addition, Janet Bax, Phil Beahen, Robert Corley, Peter Hill, Andrew McAllister, Craig Oldham, Julie Spallin, and Suki Wong (PSEPC) provided valuable input.

98 http://www.psepc-sppcc.gc.ca/prg/em/nciap/about-en.asp.

- Energy and Utilities (Electrical Power, Natural Gas, Oil Production and Transmission Systems),
- Finance (Banking, Securities, Investment),
- Food (Food Safety, Agriculture and Food Industry, Food Distribution),
- Government (Government Facilities, Government Services (e.g., Meteorological Services), Information Networks, Assets, Key National Symbols (Cultural Institutions and National Sites and Monuments)),
- Health Care (Hospitals, Health Care and Blood Supply Facilities, Laboratories, Pharmaceuticals),
- Manufacturing (Chemical Industry and Defense Production, Defense Industrial Base),
- Safety (Chemical, Biological, Radiological, and Nuclear Safety; Hazardous Materials; Emergency Services (Police, Fire, Ambulance), Search and Rescue, Dams),
- Transportation (Air, Rail, Marine, Surface),
- Water (Drinking Water, Wastewater Management).[99]

Past and Present Initiatives and Policies

Public Safety and Emergency Preparedness Canada (PSEPC) develops initiatives and programs aimed at assuring the continuation of essential services to Canadians in the event that any part of the nation's critical infrastructure is disrupted or destroyed.

Given the interdependencies and connectedness between critical infrastructures, the interruption of any one service could have a cascading effect and disrupt other essential services or systems. For example, during the North American Power Outage of 2003, large segments of rural and urban communities were in the dark: traffic and street lights were out; banking and government services were interrupted; fuel distribution was disrupted. The disruption in one sector - electricity - affected a score of others, interrupting the delivery of important services upon which Canadians depend.

99 Ibid.

PSEPC promotes a national partnership among private and public-sector stakeholders. Since most of Canada's infrastructure is privately owned, the government of Canada fosters cooperation and communication to provide the best possible assurance of a resilient and viable infrastructure. One component of the PSEPC mandate addresses cross-border systems and networks, including the internet, banking networks, and gas and oil pipelines.

While individual sectors, provincial, territorial, and municipal governments may have their own assurance programs, PSEPC provides national coordination to assure the continuity of services across all sectors. PSEPC encourages dialog among owners and operators of critical infrastructure to help prevent undue interruption of essential services in the wake of disasters or disruptions.

Canadian cyber-protection activities focus on awareness and the resilience of information technology systems and assets. This includes components such as telecommunications, computers and software, the internet, and satellites, as well as interconnected computers and networks and the services they provide.

Policies and programs are in place or under development to ensure that Canada is prepared for attacks and has the ability to recover key services as quickly as possible. These initiatives enable the government of Canada to identify threats, to minimize the exploitation of vulnerabilities, and to mitigate disruptions as early as possible, allowing it to quickly issue warnings and provide guidance to owners and operators of critical infrastructures.

To provide credible national leadership, the government of Canada ensures an adequate level of protection for its own portion of the national critical infrastructure (in the physical realm and in cyberspace). This means having emergency plans, contingency plans, and business continuity plans for government systems, processes, and assets. The Government Security Policy prescribes the application of safeguards (physical and virtual) for federal departments and agencies.

Canada's National Security Policy 2004

In April 2004, the government of Canada issued its first comprehensive statement on national security. "Securing An Open Society: Canada's National

Security Policy"[100] is a strategic framework and action plan designed to ensure that the government of Canada can prepare for and respond to current and future threats. The policy adopts an integrated approach to security issues across government sectors, employs a model that can adapt to changing circumstances, and reflects Canadian values.

In its National Security Policy, the government recognizes the need for a more modern, integrated national emergency management system. In Canada, effective emergency management comprises several phases: mitigation and prevention, preparedness, response, and recovery. The national capacity must be bolstered for all of these phases, and policies and operations must be made seamless across jurisdictions. The National Security Policy assesses the threats to Canadians, articulates national security interests, and outlines an integrated management framework that integrates emergency management, critical infrastructure protection, and national security. It provides a blueprint for action in six key areas: intelligence, emergency management, public health, transportation, border security, and international security.

National Critical Infrastructure Protection Strategy

As announced in the National Security Policy, PSEPC published a "Position Paper on a National Strategy for Critical Infrastructure Protection" in November 2004. The Position Paper helped to stimulate a national discussion on the key elements required for greater protection of the national critical infrastructure, and provided a basis for national consultations. During the spring of 2005, PSEPC hosted a series of national consultations with other levels of government and the owners and operators of Canada's national critical infrastructure to determine measures currently under way to better protect critical assets and services and to explore the gaps and challenges to protection measures.

As a result of these consultations, PSEPC will release a National Critical Infrastructure Protection Strategy[101] that outlines the priority areas for CIP, such as: ways to share and protect information better; ways to understand interdependencies better; and roles and responsibilities for undertaking pro-

100 Canada, Privy Council Office. Securing an Open Society: Canada's National Security Policy (April 2004). Available at: http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf.

101 Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection (November 2004).

tective actions. Other important topics that will be addressed in the strategy paper include the identification of vulnerabilities and risks; risk management; threats and warnings; research and development; international cooperation; and governance mechanisms. Following the release of the strategy, an implementation plan will be developed that further details the initiatives to address those priorities. PSEPC continues to work with key government departments, with provinces and territories, and with the private sector in all ten sectors of Canada's critical infrastructure to ensure that work progresses efficiently. This partnership is indispensable for ensuring better protection for the infrastructure on which all Canadians rely for their health and safety.

Mitigation and Response Review

PSEPC is currently developing two initiatives of great importance to the goal of a seamless emergency management system: the "National Disaster Mitigation Strategy (NDMS)", which aims to prevent and reduce the risks, impacts, and spiraling costs of natural disasters, and the "National Emergency Response System (NERS)". The NERS is the mechanism whereby the government will respond to and manage the initial impact of an emergency. In any emergency that involves critical infrastructure, whether cyber or physical, PSEPC intends to provide leadership and ensure a harmonized national response to events that affect, or have the potential to affect those national interests. This aim is achieved by coordinating federal mandates, by providing effective federal, provincial, and territorial coordination, and through the incorporation of all stakeholder actions into a national response.[102]

Government-on-Line (GoL)

The government plans to implement a technology and policy framework that protects the security and privacy of Canadians in their electronic dealings with their government. This is part of the Government-on-Line (GoL)[103] policy. Canadians will be able to transmit applications and financial transactions securely online and in real-time. GoL must address the principal security requirements for electronic transactions (data integrity, data confidentiality, availability, authentication, and non-repudiation).

102 Information provided by expert from PSEPC.
103 http://www.gol-ged.gc.ca/index_e.asp.

The secure channel is a major component of the technology infrastructure that will allow citizens to access federal services over the internet reliably and securely, and is a key part of the government's plan to get government programs and services on-line by the end of 2005.[104]

Joint Infrastructure Interdependencies Research Program (JIIRP)

PSEPC and the Natural Sciences and Engineering Research Canada have collaborated to announce funding for academic research projects that will study the interdependencies of Canada's major infrastructure systems. Known as the Joint Infrastructure Interdependencies Research Program (JIIRP),[105] it is the first research program of its kind in Canada and is designed to help infrastructure owners and operators better understand the extent of their dependencies on other sectors for delivering their services and goods, and how the risks resulting from these interdependencies can be mitigated.

Information Technology Systems Research and Development Initiative

Several federal government agencies have research and development expertise in the area of information infrastructure protection. These include the Public Safety and Emergency Preparedness (PSEPC), Defence Research and Development Canada, the Communications Security Establishment, and Industry Canada's Communications Research Centre. These agencies have formed a joint working group to collaborate on information infrastructure research projects and to develop a joint long-term research agenda. This initiative is expected to expand to include other Canadian government departments, as well as to develop international linkages to other research councils.

Information-Sharing

Information-sharing is arguably one of the most significant issues in CIIP. Canada has been working to identify better ways to achieve this goal. Information-sharing can be viewed as a means to manage actions that can

104 http://www.tbs-sct.gc.ca/si-as/performance/performance01_e.asp.
105 http://www.psepc.gc.ca/prg/em/jiirp/index-en.asp.

help deter, prevent, mitigate, and respond to the impact of a threat, as well as a tool to manage risk.

Canada is working towards establishing a comprehensive information-sharing framework. This framework will provide a clear structure for the process of establishing information-sharing relationships, and encouraging consistent approaches among participants, while ensuring that such processes are workable for and relevant to all key stakeholders. The primary goals of Canada's information-sharing framework are assessing threats and vulnerabilities, improving warning and reporting capabilities, and analyzing attacks to develop better defenses and responses.

Organizational Overview

Public Agencies

Public Safety and Emergency Preparedness Canada (PSEPC)

In Canada, the lead portfolio dealing with CIP/CIIP is Public Safety and Emergency Preparedness Canada (PSEPC).[106] Industry Canada also contributes to CIIP programs and initiatives in particular.

On 12 December 2003, the prime minister announced the creation of PSEPC, which integrated the former Department of the Solicitor General, the National Crime Prevention Centre, and the former Office of Critical Infrastructure Protection and Emergency Management. The prime minister created PSEPC to close further security gaps and to maximize emergency preparedness and response measures to any kind of threat, thereby ensuring that national interests and citizens are protected. Public Safety and Emergency Preparedness also includes the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), the Correctional Service of Canada, the National Parole Board, the Canada Firearms Centre, the Canada Border Services Agency, and three review bodies. Through partnership-building, the government of Canada also works together with the private sector and provincial/territorial governments focusing on developing a seamless, well-coordinated approach to CIP.

106 http://www.psepc.gc.ca.

The PSEPC provides policy leadership and delivers programs and services in the areas of national security, emergency management, policing, border security, corrections, and crime prevention. It also ensures policy cohesion among the six agencies that report to the minister.

PSEPC continues the mandate given to the Office of Critical Infrastructure Protection and Emergency Preparedness to combine critical infrastructure protection and emergency preparedness responsibilities in one organization. This approach reflects the new risk environment, where the physical and virtual dimensions of infrastructures are increasingly interconnected. Combining critical infrastructure protection and emergency management resources and policy tools with acquired knowledge and experience in emergency preparedness should ensure a stronger, more integrated and effective national security posture. Critical infrastructure protection and emergency management are not seen as separate endeavors, but as part of the assurance and protection continuum.

PSEPC is the focal point for coordinating, analyzing, and sharing information related to physical and virtual threats to the Canadian critical infrastructure. Therefore, it receives Joint Department of Homeland Security/ Federal Bureau of Investigation Information Bulletins on a variety of threats and security topics. Once it has received notification, the Government Operations Center assesses the threat to Canada and further distributes the bulletin and assessment to critical infrastructure owners and operators as well as emergency management contacts in Canada.

Integrated Threat Assessment Centre (ITAC)

The Integrated Threat Assessment Centre (ITAC)[107] was created to facilitate the integration of intelligence from various sources into comprehensive threat assessments. These are based on intelligence and trend analysis evaluating both the probability and potential consequences of threats. Such assessments are aimed at assisting the government of Canada to more effectively coordinate activities in response to specific threats in order to prevent or mitigate risks to public safety.

Several federal government departments feed into ITAC, including: PSEPC, the Canadian Security Intelligence Service, the Department of

107 http://www.csis-scrs.gc.ca/en/itac/itac.asp.

National Defence, the Canada Border Services Agency, Foreign Affairs Canada, Transport Canada, the Royal Canadian Mounted Police, the Communications Security Establishment, Ontario Provincial Police, and the Privy Council Office. The focus of the threat assessments is on domestic and international terrorism-related events and trends. Although the assessments are related to national security issues, they are produced at various levels of classification allowing for a broader distribution. ITAC assessments are currently distributed to the federal government and foreign partners through the center; law enforcement agencies receive the assessments through the Royal Canadian Mounted Police; and the private sector and provinces and territories receive the assessments through PSEPC.

Federal Provincial High-Level Forum on Emergencies

Major emergencies require extremely close cooperation between the federal government, provinces and territories, municipalities, and first responders. The government has therefore invited provinces and territories to establish a permanent high-level forum on emergencies in order to allow for regular strategic discussion of emergency management issues among key national players. The government is also very committed to moving ahead on the co-location of federal, provincial, and territorial emergency operations centers.[108]

Cross-Cultural Roundtable on Security

A key element of the National Security Policy was the establishment of the Cross-Cultural Roundtable on Security,[109] created to engage Canadians and the government of Canada in a long-term dialog on matters related to national security as they affect a diverse and pluralistic society.

The government needs the help and support of Canadians to make its approach to security effective. The Roundtable will provide a forum to discuss emerging trends and developments emanating from national security matters, and it will serve to better inform policy-makers.

The Roundtable will accomplish its mandate by:

108 http://www.psepc-sppcc.gc.ca/pol/ns/secpol05-en.asp.
109 http://www.psepc.gc.ca/roundtable/index_e.asp.

- Providing insights on the potential impact of national security measures on Canada's diverse communities;
- Promoting the protection of civil order, mutual respect, and common understanding;
- Facilitating a broad exchange of information between the government and communities on the impact of national security issues consistent with Canadian rights and responsibilities.

The Roundtable works with the minister of PSEPC and the minister of justice, who will consider its input in matters relating to national security.

Public-Private Partnerships

The Canadian private sector, which owns and operates almost 85 per cent of the nation's infrastructure, plays a key role in securing cyberspace. National sector associations such as the Canadian Electricity Association (CEA), the Canadian Bankers Association (CBA), the Canadian Telecommunications Emergency Preparedness Association (CTEPA), and others have been active in promoting enhanced CIP efforts. Currently, Canada's CI sectors are working to enhance information-sharing among their members, with government, and between sectors.

It is increasingly recognized that information on threats, vulnerabilities, corrective measures, and best practices should be shared widely, across sectors and with governments. Canadian industry and governments at all levels are working together to improve information-sharing and analysis efforts. Industry sectors have identified a variety of challenges, including such issues as timeliness and relevancy of threat information. As industry efforts to increase cooperation and information-sharing mature, so will the national ability to respond to and manage cyber-incidents and attacks.

National Critical Infrastructure Assurance Program (NCIAP)

The overall aim of the National Critical Infrastructure Assurance Program (NCIAP)[110] is to promote a more resilient and viable national critical infrastructure through partnership between governments and the private sector.

110 http://www.ocipep.gc.ca/critical/nciap/synopsis_e.asp.

Such partnership will enable two-way information exchange and more directed research and development. It will also develop the means to better assess risks, vulnerabilities, threats, and interdependencies that can affect the continuity of the NCI.

The NCIAP is currently a framework for cooperative action. The short-term goal is to bring together organizations with a stake in better assuring CI/CII, so that an approach can be jointly developed and the exact nature of the partnership and methods of information exchange can be designed. The NCIAP will evolve with the emergence of new needs and the changing risk environment. Through consultation and planning, the NCIAP will evolve from its current framework status to a fully operational program with a powerful, yet flexible charter.

Early Warning and Public Outreach

Canadian Cyber Incident Response Centre (CCIRC)

PSEPC's Canadian Cyber Incident Response Centre (CCIRC)[111] provides national and international leadership in cyber-readiness and response. CCIRC is Canada's national focal point for coordinating cyber-security incident response and monitoring the cyber-threat environment 24 hours a day, seven days a week.

CCIRC leverages the IT security capabilities of the federal government to provide the following services to critical infrastructure sectors:[112]

- Incident response, coordination and support;
- Monitoring and analysis of the cyber-threat environment;
- IT security-related technical advice;
- National awareness and education (training, standards, best practices).

111 http://www.ocipep.gc.ca/ccirc/index_e.asp.
112 http://www.ocipep.gc.ca/critical/index_e.asp.

When warranted, PSEPC issues cyber-alerts and advisories, as well as other cyber-related information products to respond to potential, imminent, or actual threats, vulnerabilities, or incidents affecting Canada's critical infrastructure. This information is made available to all levels of government, as well as to non-government organizations.

CCIRC will build upon PSEPC's existing international relationships and is designed for improved interoperability with its allied partners.

Government Operations Centre (GOC)

PSEPC is home to the Government Operations Centre (GOC).[113] The GOC operates 24 hours a day, seven days a week. Its purpose is to provide strategic-level coordination and direction on behalf of the government of Canada in response to an emerging or occurring event affecting the national interest. It also receives and issues information dealing with any emerging or occurring threat to the safety and security of Canadians and Canada's critical infrastructure.

Information received by the GOC is quickly verified, analyzed, and distributed to the appropriate response organizations. This is made possible through PSEPC's close linkages with other government departments and agencies; provincial, territorial, and municipal governments; and the private sector.

Calling upon resources and experts in various fields, the GOC helps to ensure that the right resources are in the right place at the right time. It coordinates the response to calls for help from other government departments and agencies; provincial, territorial, and municipal governments; and the private sector.

Law and Legislation

Canadian Criminal Code Sections

342.1 (1) Every one who, fraudulently and without color of right, (a) obtains, directly or indirectly, any computer service, (b) by means of an elec-

113 http://www.psepc-sppcc.gc.ca/prg/em/goc/index-en.asp.

tro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly , any function of a computer system, (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

342.2 (1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section, (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or (b) is guilty of an offence punishable on summary conviction.

430. (1.1) Every one commits mischief who willfully (a) destroys or alters data; (b) renders data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of data; or (d) obstructs, intercepts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.[114]

Two key laws are involved in the organization of the government of Canada for emergency management and in securing the public's safety: The Department of Public Safety and Emergency Preparedness Act (DPSEPA) and the Emergency Preparedness Act.

The Emergencies Act 1988

The Emergencies Act[115] enables the government of Canada to fulfill its constitutional responsibility to provide safety and security for Canadians during national emergencies.

114 http://www.cybercrimelaw.net/countries/canada.html.
115 http://www.psepc.gc.ca/pol/em/em_act-en.asp.

The Emergencies Act includes fully safeguarded and appropriately limited exceptional powers to deal with four types of national emergencies. It ensures that the exceptional powers granted by parliament will be no more than what is needed for the specific emergency at hand. The four types of emergencies are:

- Public Welfare Emergencies: severe natural disasters or major accidents affecting public welfare, which are beyond the capacity or authority of a province or territory to handle;
- Public Order Emergencies: crises that constitute threats to the security of Canada, and are so serious as to be national emergencies and are beyond the capacity or authority of a province or territory to handle;
- International Emergencies: emergencies that arise from acts of intimidation or coercion or the use of serious force or violence that threatens the sovereignty, security, or territorial integrity of Canada or any of its allies;
- War Emergencies: war or other armed conflict, real or imminent, involving Canada or any of its allies.

Safeguards place a number of constraints on the government of Canada's use of special temporary powers. These safeguards include the provision that, in the case of a public-welfare or a public-order emergency where the effects of the emergency are confined to a single province, the federal government may only declare an emergency after the province concerned has indicated that its capacity to cope has been exceeded.

The Emergencies Act applies only to national emergencies. The Preamble to the Act defines a "national emergency" as "an urgent and critical situation of a temporary nature that seriously endangers the lives, health or safety of Canadians and is of such proportions or nature as to exceed the capacity or authority of a province to deal with it, or seriously threatens the ability of the government of Canada to preserve the sovereignty, security and territorial integrity of Canada, and cannot be effectively dealt with under any other law of Canada."

The definition ensures that the application of the Act will be confined only to those very serious emergencies that are considered under the "emergency doctrine" to fall within the responsibility of the government of Canada.

The Emergency Preparedness Act, companion legislation adopted by parliament at the same time as the Emergencies Act, provides a statutory basis for the planning and preparedness programs necessary for dealing effectively with emergencies of all kinds.

The Emergency Preparedness Act 1988

The Emergency Preparedness Act[116] provides a statutory basis for effective civil emergency preparedness in Canada, and for co-operation between federal and provincial or territorial governments in this area.

This legislation establishes the requirement that the government of Canada be in a position to respond to the needs of Canadians in emergencies in an increasingly complex social and technological environment. The legislation establishes a government-wide mandate for all federal departments and agencies to develop and coordinate programs to deal with unforeseen and potentially disastrous events.

Specifically, the Emergency Preparedness Act:

- Sets out the responsibilities and functions of the Minister Responsible for Emergency Preparedness with respect to the coordination and support of civil emergency plans, the enhancement of public awareness, and the conduct of training and education related to civil preparedness for emergencies;
- Establishes the emergency preparedness responsibilities of all federal ministers in their respective areas of accountability;
- Explicitly recognizes the interests of the provinces in relation to federal assistance provided during a provincial emergency;
- Provides the legal basis for the Governor in Council to declare a provincial emergency to be of concern to the federal government, and to provide financial and other assistance requested by the affected province(s).

The Minister Responsible for Emergency Preparedness is supported by PSEPC in her responsibility to administer the Act.

116 http://www.psepc.gc.ca/pol/em/epa-en.asp.

However, events in recent years have challenged governments and the private sector, stretching their ability to cope with emergencies. These events have been studied extensively to derive lessons learned and propose remedial action. As a result, the federal government has decided to review the Emergency Preparedness Act to better meet the range of events facing Canadians and provide specific previsions to deal with new areas such as critical infrastructure protection. As a result, a new act, called the Emergency Management Act (C-78), was tabled in the House of Commons for first reading on 16 November 2005.

C-78 - Emergency Management Act 2005

The purpose of the new Emergency Management Act (EMA) is to strengthen the readiness posture of the government of Canada to prepare for, mitigate the impact of, and respond to all hazards in Canada. It recognizes that emergency management in an evolving risk environment requires a collective and concerted approach between all jurisdictions, including the private sector and non-governmental organizations. The new act will reflect a comprehensive, all-hazards approach to emergency management.

The proposed EMA sets out the duties and responsibilities of the minister in providing national leadership by coordinating emergency planning for the government of Canada. The EMA also sets out the responsibilities of other ministers. While the PSEP minister has broad authorities for public safety and emergency preparedness, the proposed EMA specifically outlines how the PSEP minister will exercise her leadership role for emergency management. In particular, this involves:

- Coordinating the federal response to emergencies in Canada and the US;
- Establishing standardized elements for emergency plans within the GoC;
- Monitoring, evaluating, and testing the robustness of EM plans of government institutions;
- Enhancing cooperation with other jurisdictions and entities by promoting common standards and information-sharing.

The EMA also outlines the responsibilities of other federal ministers in carrying out their emergency management responsibilities.

The Department of Public Safety and Emergency Preparedness Act 2005

The Department of Public Safety and Emergency Preparedness Act is PSEPC's enabling legislation that sets out the general powers, duties, and functions for the department. The act establishes the PSEPC minister's powers and authorities to secure public safety and emergency preparedness, and to provide leadership at the national level.

Finland

Critical Sectors

Finland aims to ensure society's ability to function in all circumstances by securing the functioning of both official infrastructures and those administered by individual citizens and businesses. Consequently, as an information society,[117] Finland can only function smoothly if its critical information infrastructure is fully operational, because any disruptions may result in dramatic consequences.

Protective actions are based on both the "Security of Supply Act" and the "Decree of the National Emergency Supply Agency (NESA)" of 1992.[118] Subsequently, the Finnish government set official goals for the development

* The Country Survey of Finland 2006 was reviewed by Ilkka Kananen, Veli-Pekka Kuparinen, and Hannu Sivonen, National Emergency Supply Agency (NESA).

117 An Information Society is a society where information technology is essential for productivity and the economy. For example, in 1994, the report by Martin Bangemann on Europe and the global information society recommended actions to the European Council in order to carry Europe forward to the Information Society. http://www.cyber-rights.org/documents/bangemann.htm.

118 The Security of Supply Act is the legal basis for ensuring supplies of various basic materials in the case of emergency situations. Based on this act, the National Emergency Supply Agency (NESA), a subordinate agency to the Ministry of Trade and Industry, was founded in 1993 for the development and maintenance of security of supply. NESA is the national stock-holding agency of Finland.

of security of supply in 2002. According to this decision, the most critical sectors in Finland are:

- Energy Networks and Supply,
- Telecommunication Networks,
- Information Systems and ICT Maintenance,
- Electronic and Print Media,
- Financing Services,
- Payment Systems and Currency Supply,
- Water Supply and Other Municipal Utilities,
- Transportation, Storage, and Distribution Systems,
- Food Supply,
- Social Services and Public Health,
- Defense-Related Industry and System Maintenance.

The government focuses on safeguarding society's critical infrastructure. The objective is to protect fundamental structures by using non-critical technology and organizations, even during disturbances and emergency situations. Accordingly, an essential aspect of safeguarding the technology is ensuring the system's ability to recover.

Past and Present Initiatives and Policies

Governmental Support for the Information Society

From the early 1990s on, the Finnish government has worked continuously on new programs aimed at promoting the Information Society, its infrastructure, and the protection of the infrastructure. On the basis of their reports, several ministries have produced action plans and provided funding for Information Society projects.

In 2000, the Ministry of Finance published a report of the Information Society Advisory Board (1999–2003) entitled "Finland as an Information Society".[119] This report aimed at outlining the development of the Information

Society and at evaluating the social and economic effects of the Information Society. The report also dealt with the domestic regulatory framework and discussed measures and programs in the public sector for the promotion and development of the Information Society. In 2001, the same ministry published a report on "Finland in eEurope", where the following areas were identified as important to Finland: facilitating the ability of the public to participate in the Information Society, the securing of networks, and the acceleration of e-commerce and e-government.[120]

In 2005, the Information Society Council published a report "Towards a Networked Finland".[121] In the report, the council reviews the current development of the Information Society and the ensuing challenges in Finland. It also outlines measures to address these challenges. According to the report, 80 per cent of the Finnish population is familiar with the internet, and nearly half of these people use it every day. Ninety per cent of internet users consider on-line bank services secure. The report concentrates on business and competition challenges for the Finnish Information Society. It sees information security as an important positive challenge and opportunity for business.

Also in 2005, the Finnish government issued a strategy resolution, which includes an "Information Society Programme".[122] This program promotes information society development in the areas of telecommunication infrastructure, digital television, citizens' skills to utilize the Information Society, research and development, and ICT in public administration and business. Special emphasis has been put on the security of networks so that the citizens can trust the electronic services.

119 Information Society Advisory Board. Finland as an Information Society (Helsinki 2000). http://www.innovazione.gov.it/ita/intervento/banda_larga/fin1.pdf.

120 Ministry of Transport and Communications. Finland in eEurope (2001).

121 The Information Society Council. Towards a Networked Finland (February 2005). http://www.tietoyhteiskuntaohjelma.fi/tietoyhteiskuntaneuvosto/en_GB/information_society_council/_files/11233297000012864/default/TietoYnRap-Eng-7-6-05.pdf.

122 The Finnish Government. Information Society Programme (April 2005). http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/11233297000000607/default/tietoyhteiskuntaojelma_en_2005.pdf.

Strategy for Securing the Functions Vital to Society

In 2003, the Finnish government issued a "Strategy for Securing the Functions Vital to Society".[123] The strategy paper divides the vital functions into seven broad areas: state leadership, the external capacity to act, national military defense, internal security, the economy and the society, the population's livelihood and capacity to act, and mental crisis endurance.

Electronic information and communication systems are recognized as an important part of a well-functioning society. It is vital to secure electronic communication networks and their information security, to determine basic security levels for services and technical systems, and to ensure that the regulations on construction and maintenance of systems are observed. In addition, it is critical to coordinate the development of networks used by the authorities, to safeguard the state's information-processing capacity, and to provide guidelines for public electronic services, the public data administration, and information security. Among vital threats to society, the strategy paper lists threats to information and communication systems first.

Updated versions of this strategy paper are due in 2006 and 2010. This development process is due to become an integral part of activity planning and economic planning in the government departments.

Security and Defense Policy 2004

The Finnish government submits a Security and Defense Policy report to parliament every three or four years. In 2004,[124] the report emphasized the growing importance of electronic information and communications technology systems for the functioning of modern society. It is no longer possible to shift to the use of manual reserve systems.

Along with the rest of society, criminals also use networks and systems. Therefore, specific chapters in this policy paper are devoted to combating cyber-crime and to securing society's electronic communications and information systems. According to the report, the capacity of the police for protecting

123 The Finnish Government. Strategy for Securing the Functions Vital to Society (2003). http://www.defmin.fi/index.phtml/page_id/369/topmenu_id/7/menu_id/369/this_topmenu/368/lang/3.

124 The Finnish Government. Finnish Security and Defence Policy (2004). http://www.defmin.fi/chapter_images/2574_2160_English_White_paper_2004%5B1%5D.pdf.

information systems, telecommunication connections, and electronic transactions, as well as for combating cyber-crime, will be expanded. Cooperation between the police and the Finnish Communications Regulatory Authority (FICORA) will raise the level of information systems protection required in an open network environment.

The security level of communication networks is being increased. ICT used by major government agencies, security authorities, and vital industries are safeguarded by prioritization and by the construction of communication networks and data systems for special use. One example is Finland's Public Authority Network VIRVE.[125]

On data networks, individuals are to have an unmistakable electronic identity in order to prevent online identity theft and identity fraud. Public support measures will be applied in order to speed up the distribution of the state-approved electronic identity card.

National Information Security Bodies

In 2001, the government set up an Advisory Committee for Information Security (ACIS) under the Finnish Communications Regulatory Authority (FICORA) as a point of contact for citizens, companies, organizations, and authorities on information security issues.

In 2002, ACIS published the "Information Security Review",[126] which deals with the most important information security threats affecting Finland, and recommends steps to be taken by all parties to promote information security. The committee expressed its vision — to be attained by the year 2010 — as follows: "Finland will be an information-secure society that everyone can trust and that enables all parties to manage and communicate information safely."

Also in 2002, ACIS released its "National Information Security Strategy Proposal",[127] which was approved by the government in 2003. The paper states

125 Finland's Public Authority Network VIRVE, based on TETRA (Terrestrial Trunked Radio) technology is being expanded by increasing the number of users. Among the users are fire and rescue services, police, border guards, customs, the military, and health services. http://www.virve.com/englanti/englanti_etusivu.htm.

126 Finnish Communications Regulatory Authority (FICORA). Information Security Review related to the National Information Security Strategy (May 2002). http://www.ficora.fi/englanti/document/review.pdf.

127 Advisory Committee for Information Security. National Information Security Strategy Proposal (2002). http://www.ficora.fi/englanti/document/infos.pdf.

that risk management for improving information security will be developed by improving society's ability to cope with disruptions, and by advanced recognition of information security risks, as well as by protecting the critical infrastructure. The paper lists detailed policy objectives and measures to be implemented as well as the responsibilities of the various stakeholders.

In order to monitor the implementation of this strategy, the government set up a National Information Security Advisory Board[128] for the period 2004–2007. The members of this board are representatives of the authorities and of business organizations.

The priority areas of implementation in 2006 will be to secure electronic services, to secure biometric identification, to protect critical infrastructure, to combat cyber-crime, to protect the national information assets, to enhance information security awareness by promoting the annual national information security day, and to improve awareness in business enterprises. Supporting activities will take place in the areas of information security in public services, international cooperation, and strategy communication.

eFinland

The website eFinland[129] provides daily updated information on Finnish IT know-how and the Finnish Information Society, in particular e-business, e-government, e-education, e-culture, mobility, and research and development. eFinland was built and is maintained in co-operation with the Ministry for Foreign Affairs, the Ministry of Finance, the Ministry of Transport and Communications, the National Technology Agency (Tekes), and the TIEKE Finnish Information Society Development Center.

128 National Information Security Advisory Board. Creating a Safer Information Society (2004). http://www.mintc.fi/oliver/upl501-NISAB%20report%20(lowres).pdf.

129 http://e.finland.fi.

Organizational Overview

Public Agencies

In Finland, there are three major public agencies dealing with CIIP. The Finnish Communications Regulatory Authority (FICORA) promotes the Information Society, as well as technical regulation and standardizations; the National Emergency Supply Agency (NESA) analyzes threats and risks against critical (information) infrastructures; and finally, the Steering Committee for Data Security in State Administration (VAHTI) develops policy guidelines and practical guides for the security of information systems.

Finnish Communications Regulatory Authority (FICORA)

The Finnish Communications Regulatory Authority (FICORA)[130] belongs to the Ministry of Transport and Communications. FICORA is a general administrative authority for issues concerning electronic communications and Information Society services. Its mission is to promote the development of the Information Society in Finland. The specific duty of FICORA is to safeguard the functionality and efficiency of the communications markets in order to ensure that consumers have access to competitive and technically advanced communications services that are affordable as well as of good quality.

FICORA's mission includes issuing technical regulations and coordinating standardization at the national level. It also oversees the protection of privacy and securing data in electronic communications. In addition, FICORA encourages national and international co-operation.

FICORA also ensures that telecommunications operators are prepared for emergencies. The operators must report significant information security incidents as well as any threats, faults, or disturbances in telecommunication networks and services to FICORA. FICORA checks the operators for compliance with the "Communications Market Act" and the "Act on the Protection of Privacy in Electronic Communications" and monitors compliance with the relevant technical regulations and standards. In pursuing this task, FICORA collects information from the operators and conducts inspections.

130 http://www.ficora.fi/englanti/esittely/n2483.htm.

Finally, FICORA operates the national Computer Emergency Response Team (CERT-FI), which is tasked with the detection and resolution of data security infringements.

National Emergency Supply Agency (NESA)

The National Emergency Supply Agency (NESA)[131] is the cross-administrative operative authority for the security of supply in Finland. NESA works under the auspices of the Ministry of Trade and Industry. In addition, NESA serves to develop cooperation between the public and private sectors in the field of economic preparedness, in coordinating preparations within the public administration, and in developing and maintaining the security of supply.

NESA and the National Board of Economic Defense (NBED) analyze threats and risks that may affect the critical infrastructure. NESA itself conducts research and finances research commissioned by outside organizations. NESA and NBED formulate plans and guidelines for public authorities and businesses with respect to the management and control of such threats and risks.

NESA has a growing role in securing the critical national infrastructure by developing and financing both technical backup systems and electromagnetic pulse (EMP)-secure premises for systems. Finland's vital communication and IT systems are located in the capital region. This is a risky concentration. Therefore, a National EDP Backup Center was established far from the capital to secure society's critical IT systems in exceptional conditions. A second center is now under construction.

The National Fixed Line Telephone Backup Network is a digital, nationwide separate network that was built to secure the lines of communication of vital public organizations, as well as other key subscribers, in exceptional situations and crises. The Ministry of Transport and Communications and NESA are jointly developing the network so that it can also secure other telecommunication services than voice services. NESA is involved in the development and maintenance of Finland's Public Authority Network VIRVE.

In addition, NESA has financed several projects to secure the communication and broadcast systems. These projects and activities are related to

131 http://www.nesa.fi.

reserve systems, emergency and warning message broadcasting systems, and the construction of circuitous routes for critical nodes of networks.[132]

Steering Committee for Data Security in State Administration (VAHTI)

The central government's data-security and information-management policies are steered and developed by the Ministry of Finance. Guidelines are developed by the Steering Committee for Data Security in State Administration (VAHTI),[133] a broad group of experts.

For the central government, the issue of data security includes a number of areas such as the use of the internet, data management outsourcing, remote work, e-mail, protection from viruses, personnel security, physical security, data communication security, and database security. The Ministry of Finance works in close cooperation with other ministries and agencies to support and facilitate cooperation in the development of e-government and electronic services in the state sector.

VAHTI has published an extensive collection of practical guides (some of them in English) for information system security. The guides are intended for the state administration, but they are also used by many private organizations.

Public-Private Partnerships

National Board of Economic Defense (NBED)

Established in 1955, the National Board of Economic Defense (NBED),[134] under the auspices of the Ministry of Trade and Industry, supports and assists NESA activities. NBED also plans and coordinates economic preparations for implementation in case of exceptional circumstances in Finland.

NBED is a network of committees consisting of the leading experts from both the public administration and the business world. Its tasks are to analyze threats against the country's security of supply, to plan measures to control

132 Information provided by representatives of the Finnish National Emergency Supply Agency (NESA).

133 http://www.vm.fi/vm/liston/page.lsp?r=2685&l=en.

134 http://www.nesa.fi.

these threats, and to promote readiness planning in individual industrial sites.

NBED's areas of responsibility include the Information Society, transport logistics, food supply, energy supply, and healthcare services. Financial service pools and industrial pools that contribute to national defense come under the direct responsibility of the central section of NBED. NBED members include representatives of ministries, government agencies, the private economy, and various industrial organizations. Approximately 800 people work within the NBED.

NBED has several planning bodies in the area of information infrastructure. They have prepared instructions and basic plans for the ICT sector as well as for other vital branches of the infrastructure. In addition, NBED studies and follows up on risks and threats to the security of supply. Databases and methods have been developed to support and improve the level of readiness to act in exceptional situations.

Finnish Information Society Development Centre (TIEKE)

Since 1998, the Finnish Information Society Development Centre (TIEKE)[135] has had a key role in the public and private sectors in Finland. TIEKE's goal is to create viable tools and expertise for use in the Information Society. Specifically, TIEKE's main focus is on the development of networking and interoperability.

TIEKE's membership includes more than 100 organizations and companies involved in the information society. The members operate in the areas of trade, industry, and public administration, and thus also serve individual citizens.

Information Society Council

The Information Society Council[136] is a negotiating body for steering the development of the Information Society and for coordinating cooperation between administrative branches and between administration and business life. The

135 http://www.tieke.fi/in_english/about_tieke.

136 http://www.tietoyhteiskuntaohjelma.fi/tietoyhteiskuntaneuvosto/en_GB/information_society_council.

government appointed the Information Society Council in 2003. It is composed of the prime minister, a number of cabinet ministers, and representatives of key private companies and state agencies that have a special interest in developing the Information Society.

The council discusses the main policies regarding the development of the Information Society. It anticipates, monitors, and assesses the development of the information society and related impacts, possibilities, and threats. Additionally, the Information Society Council puts forward initiatives to promote cooperation across sectors, follows and discusses horizontal initiatives and legislative proposals relating to information society development, and monitors their implementation. The council also follows international developments affecting the Information Society, puts forward proposals on Finland's policies, and develops interaction between business life and administration in development projects that benefit the information society. Finally, the Council assesses the "Information Society Programme" and its progress, and reports to the government on the state of Finland's Information Society development.

Early Warning and Public Outreach

Computer Emergency Response Team Finland (CERT-FI)

FICORA's CERT-FI[137] group prevents, observes, and solves information security violations and gathers information on threats to information security. CERT-FI cooperates with national and international CERT actors and representatives of trade and industry. It is in contact with suppliers of equipment, networks, and software as well as with the police and other authorities.

CERT-FI receives notifications from telecommunications operators concerning information security incidents and threats. In addition, CERT-FI continuously follows up current global events related to information security, security problems of information systems, security incidents, and responses to them.

137 http://www.ficora.fi/englanti/tietoturva/cert.htm.

In 2005, 3'500 individuals and companies subscribed to the CERT-FI-ALERT e-mail service. The information security helpline for customers operates during business hours, but the threats and incidents are supervised around the clock, seven days a week.

Law and Legislation

Act on the National Board of Economic Defense (NBED) 1960

The Act on the National Board of Economic Defense (NBED) (238/1960)[138] obliges the NBED to plan and organize activities needed to secure the economy and the livelihood of the population in exceptional situations. NBED has the legal right to obtain, from enterprises and other important actors, information that is necessary for performing the planning and organizational tasks.

Emergency Powers Act 1991

In case of serious disturbances and in emergencies, public authorities need special powers to safeguard society's essential activities. The most important provisions are contained in the Emergency Powers Act (1080/1991).[139] In crisis situations, this law empowers the government to issue provisions concerning the critical infrastructures and other functions of society. The government's decisions are examined by parliament, which has the power to repeal them.

Security of Supply Act 1992/2005

Critical infrastructure protection actions are based on both the Security of Supply Act (1390/1992)[140] and the Decree of the National Emergency Supply

138 The official texts of Finnish legislation have been published in Finnish and Swedish. Some laws have an unofficial English translation. Unless otherwise indicated, we refer to the official texts. Act on the National Board of Economic Defence (NBED) (238/1960). http://www.finlex.fi/fi/laki/alkup/1960/19600238.

139 Emergency Powers Act (1080/1991) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/1991/en19911080.pdf.

140 Security of Supply Act (1390/1992). http://www.finlex.fi/fi/laki/ajantasa/1992/19921390.

Agency (NESA) (1391/1992).[141] The Finnish government specified the development of security of supply as one of the official goals for 2002.[142] The Security of Supply Act was amended in 2005 (688/2005).[143] The amendment refers to severe disturbances in otherwise normal circumstances (not only in crisis situations as defined in the Emergency Powers Act). The amendment emphasizes the securing of technical systems.

Finnish Penal Code

In the Finnish Penal Code, Chapter 38, Amendment 578/1995[144] specifically outlaws computer intrusions and disturbances of the telecommunications system.

Act on Television and Radio Operations 1998

This act (744/1998)[145] obliges television or radio broadcasters to ensure that they can continue transmitting with minimum disruption even in the exceptional circumstances referred to in the Emergency Powers Act. Additionally, broadcasters must transmit information from the authorities to the public if it is necessary to save human life, or protect property, or safeguard the functioning of the society.

Act on Provision of Information Society Services 2002

This act (458/2002)[146] defines the rules of offering e-services and the possibilities of the authorities to limit the services if they constitute threats to consumers or to public security.

141 The Decree of the National Emergency Supply Agency (NESA) (1391/1992). http://www.finlex.fi/fi/laki/ajantasa/1992/19921391.

142 Government decision on the Goals of Security of Supply (2002), http://www.finlex.fi/fi/laki/alkup/2002/20020350.

143 The Amendment of the Security of Supply Act (688/2005), http://www.finlex.fi/fi/esitykset/he/2005/20050044.

144 Penal Code Chapter 38 Amendment (578/1995) (unofficial English translation). http://www.finlex.fi/pdf/saadkaan/E8890039.PDF.

145 Act on Television and Radio Operations (744/1998) (unofficial English translation). http://www.finlex.fi/fi/laki/kaannokset/1998/en19980744.pdf.

146 Act on Provision of In formation Society Services (458/2002) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/2002/en20020458.pdf.

Communications Market Act 2003

This act (393/2003)[147] obliges the communications operators to ensure the functioning of their services, regardless of whether the disturbances occur during normal times, exceptional situations, or in times of crises. The act assures the telecommunications operators that any extra expenses incurred through such preparatory measures will be reimbursed to the operators by the National Emergency Supply Agency (NESA).

Act on the Protection of Privacy in Electronic Communications 2004

This Act (516/2004)[148] states that telecommunications operators or service providers must secure their services and inform the authorities about any violations. The operator or provider has the right to eliminate any programs that threaten information security. They may also limit or stop the traffic when necessary for the protection of information security.

147 Communications Market Act (393/2003) (unofficial English translation). http://www.mintc.fi/www/sivut/dokumentit/viestinta/tavoite/CommunicationsMarketAct_upto518_2004.pdf.

148 Act on the Protection of Privacy in Electronic Communications (516/2004) (unofficial English translation). http://www.mintc.fi/www/sivut/dokumentit/viestinta/tieto/Sahköisen_viestinnan_tietosuojalaki_20041213_en.pdf.

France

Critical Sectors

All infrastructures that are vital to the maintenance of primary social and economic processes are considered critical sectors in France. These critical sectors are the following:[149]

- Banking and Finance,
- Chemical and Biotechnological Industries,
- Energy and Electricity,
- Nuclear Power Stations,
- Public Health,
- Public Safety and Order,
- Telecommunication,
- Transport Systems,
- Water Supply.

* The Country Survey of France 2006 was partly reviewed by Isabelle Valentini, Secretary-General for National Defense (SGDN).

149 Haut Comité Francais pour la Défense Civile. Livre Blanc HCFDC: 20 ans, 20 constats et propositions (2003), p. 18.

Past and Present Initiatives and Policies

Government Action Program for an Information Society (PAGSI)

In August 1997, the prime minister of France designated the information and communication society as a priority for government action. The objective was to build an information society for all, to prevent a digital divide, and to help France catch up with other countries in terms of internet usage. Making government services available online has been the main goal of the formation of the "Government Action Program for an Information Society (PAGSI)"[150] (adopted at the meeting of the Inter-ministerial Committee for Information Society (CISSI) in January 1998). In addition to the improvement of general public services, standardization, and training for civil servants, PAGSI supports projects in the fields of education, culture, electronic commerce, and research and innovation, and establishes appropriate regulations for the safer use of information technologies and networks. Two of the main priorities of the PAGSI action plan are managing the "Security of Information Systems (SSI)" and combating cyber-threats.[151]

Expression of the Needs and Identification of Security Objects (EBIOS)

In 1997, the Central Information Systems Security Division (DCSSI) developed and published the first version of the guide "Expression of the Needs and Identification of Security Objects (EBIOS)".[152] It outlines a method for risk analysis concerning the security of information systems.

150 http://www.internet.gouv.fr.

151 Service d'Information du Gouvernement. Four years of Government measures to promote the information society (August 2001).

152 Prime Minister's Office, Service Central de la Sécurité des Systèmes d'Information. Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS): Technical Guide - English version (February 1997, version 1.02.)

State Information System Security Reinforcement Plan (2004–2007)

The director of the French Prime Minister's Office instructed the ministerial departments and the General Secretariat of National Defense to prepare a specific plan of action by October 2003 to "secure the main central and local governmental networks, and those used for vital infrastructure management." This plan of action was approved on 16 December the same year. The so-called "State Information System Security Reinforcement Plan"[153] has the following four objectives:

- To secure communication channels for senior state officials: that is, to ensure, under all circumstances, the security of all protected communication means for the use of senior authorities, based on supervision under the direct control of state authorities;
- To secure government information systems: that is, to secure the new e-government functions in accordance with the ADAE[154] strategic e-government plan and guidelines, and to explain security policies;
- To set up operational capabilities to respond to computer attacks;
- To include the French information system security policy within the scope of the French security policy in the EU.

In order to reach these goals, various measures in the following areas are planned: Training and skills; awareness-raising; organization; equipment; and the legal framework.[155]

Organizational Overview

In France, the Secretary-General of National Defense (SGDN), a secretary attached to the Prime Minister's Office, bears complete responsibility for organizing CIP. Furthermore, within the Ministry of Defense, the key organiza-

153 Prime Minister's Office. State Information System Security Reinforcement Plan (2004–2007) (10 March 2004). http://www.ssi.gouv.fr/site_documents/PRSSI/PRSSI-en.pdf.

154 Agence pour le Dévéloppement de l'Administration Électronique (ADAE). http://www.adae.gouv.fr/adele.

155 Ibid.

tions responsible for CIP/CIIP are the Central Information Systems Security Division (DCSSI) and its Inter-Ministerial Commission for the Security of Information Systems (CISSI) and the Advisory Office, whereas the Central Office for the Fight Against Hi-Tech Crime plays a lead role within the Ministry of the Interior.

Public Agencies

General Secretariat for National Defense (SGDN)

The Secretary-General for National Defense (SGDN) deals with national and international security affairs. The organization was first called into action for Y2K, when a specific network of contacts among different bodies from the public and private sectors became involved under the coordination of the SGDN. The SGDN is directly subordinated to the French prime minister and assists him in the co-ordination of the preparation, implementation, and follow-up of the government's decisions regarding defense and security policy, including the security of information systems.

The SGDN promotes and co-ordinates the activities between ministries involved in CIIP. This includes responsibility for the security of information systems (since 1996) and chairing the Inter-Ministerial Commission for the Security of Information Systems (CISSI),[156] as well as responsibility for the protection of classified and sensitive military information. The SGDN deals with the impact of the scientific and technical revolution on defense and security policy, focusing on securitization of information and communication technology relating to military as well as civilian matters. In this area, the SGDN works closely together with DCSSI.[157]

Central Directorate for Information Systems Security (DCSSI)

The Central Information Systems Security Division (DCSSI) was instituted by Decree No. 2001–693 of 31 July 2001 under the authority of the SGDN. It succeeded to the Central Information Systems Security Division as the state's focal center for Information Systems Security.

156 Commission Interministérielle pour la Sécurité des Systèmes d'Information (CISSI).
157 http://www.premier-ministre.gouv.fr/fr/p.cfm?ref=6467&txt=1#contenu.

DCSSI has two main objectives: To guarantee the security of the information systems of the French state (in the administration, critical infrastructures, including time of crisis); and to create a trusted environment to promote and facilitate the development of the Information Society. DCSSI's principal missions are:

- To contribute to interdepartmental and international definitions of governmental policy as regards IT security (Infosec);
- To serve as a national regulatory authority for Infosec by issuing approvals, guarantees, and certificates for national information systems, encryption processes, and products used by public bodies and services; and by controlling information technology security evaluation centers (CESTI);
- To assist public services in Infosec (consult, audit, issue warnings, and conduct incident management, including crisis management);
- To develop scientific and technical expertise in the field of Infosec for the benefit of the administration and public services;
- To run training courses and increase awareness in Infosec (Information Systems Security Training Centre/CFSSI).

The DCSSI also administers the Security of Information Systems (SSI) website[158] and co-ordinates its activities. The SSI website comprises information on the Computer Emergency Response Team (CERTA),[159] information on regulation, certification, authorization, electronic signatures, and cryptography, and provides technical advice.[160]

Information Systems Security Training Center (CFSSI)
Attached to DCSSI, the Information Systems Security Training Center's (CFSSI) objectives are to increase awareness on information systems security, and to train experts capable of designing, evaluating, and making recommendations on the following aspects of information systems security:

158 http://www.ssi.gouv.fr/en/index.html.
159 Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques. http://www.ssi.gouv.fr/fr/index.html.
160 Ibid.

- Communications security,
- Protection against compromising parasite signals,
- Computer security.

The CFSSI continues training actions undertaken by the CESSSI (Center for Training and Advanced Studies on Information Systems Security) since 1986. It will become the central player in a network designed to increase awareness on information systems security problems and provide training in the various aspects of this area, for the benefit of all government authorities.

The CFSSI also develops partnerships with higher education and further training centers. The activities of the CFSSI and the education it provides are controlled and monitored by an Improvement Committee chaired by the General Secretary for National Defense and composed of civil servants and military staff.[161]

Advisory Office

A core operational part of the DCSSI is the Advisory Office (le bureau conseil), which assists the administration in CIIP matters. If it is in the overall interest of France's security, the Advisory Office also advises and collaborates with the private sector. In addition, the Advisory Office publishes methodological and technical guides to clarify concepts presented in the "Information Technology Security Evaluation Criteria (ITSEC)".[162]

Central Office for the Fight Against Hi-Tech Crime

In May 2000, the Ministry of the Interior opened the Central Office for the Fight against Cyber-Crime.[163] It co-operates with Interpol and deals with unauthorized intrusions and crime in the field of information and communication technologies and supports legal investigations in this field. The Central Office has nation-wide jurisdiction in this matter and works closely together with the national police as well as the private sector. It provides assistance to all agencies responsible for fighting computer crime, such as the police and gendarmerie, and sensitizes the actors.[164]

161 http://www.ssi.gouv.fr/en/formation.html.
162 http://www.ssi.gouv.fr/fr/dcssi/conseil.html.
163 http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic/missions.

Public-Private Partnerships

Strategic Advisory Board on Information Technologies (CSTI)

The Strategic Advisory Board on Information Technologies (CSTI)[165] was created in July 2000 at a meeting of the government committee on the Information Society. It is chaired by the French prime minister. The CSTI is composed of business and industry executives and leading representatives of the research and development community. It is responsible for recommendations to government concerning CIIP topics and the French contribution to the 6th European Framework Research and Development Program. The CSTI, in particular, has the following duties:

- To communicate opinions and recommendations to the government on the studies and documents commissioned,
- To maintain a permanent dialog with representatives of industry and to improve co-ordination between private and public researchers (and the industry),
- To define national priorities and to select areas where more action is required,
- To provide general monitoring and warning services in the area of CIIP.

French Dependability Institute (ISDF)

The French Dependability Institute (ISDF) provides a forum for the private sector to discuss CIIP issues across a variety of industries. It is strongly supported by the Department of Industry as well as representatives from the automotive, military, and space industries and from professional organizations. ISDF fosters connections on information exchange with the industry and aims at becoming the official representative of France in international organizations in the field of CIIP.[166]

164 Ibid. Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (L'O.C.L.C.T.I.C.).

165 Conseil Stratégique des Technologies de l'Information: http://www.csti.pm.gouv.fr.

166 Dependability Development Support Initiative (DDSI). European Dependability Policy Environments, Country Report France (September 2002), p. 108.

Every year since 1990, ISDF has launched a set of projects in connection with the activities of its members. These projects reflect current issues in the field of securing information systems, such as reliability, availability, maintainability, safety, and security. As there are about 25 technical working groups at ISDF, gathered into seven colleges (management; methods and tools; maintainability; the human factor; safety; education and standards; software and systems dependability), the propositions embrace the whole spectrum of safety and dependability topics.[167]

Early Warning and Public Outreach

Computer Emergency Response Teams (CERTs)

In France, there are three different Computer Emergency Response Teams (CERTs) addressing three different constituencies: CERT-RENATER, CERTA, and CERT-IST.

- CERT-RENATER, founded in 1993, specifically addresses research centers and academic institutions. CERT-RENATER gathers and provides information about information security and is dedicated to the membership of GIP RENATER, the National Network of Telecommunications for Technology, Education, and Research.[168]
- The Computer Emergency Response Team CERTA[169] has been hosted by DCSSI since 2000. CERTA deals in particular with the French administration services. As a center of expertise, it evaluates CIIP threats and gives advice, issues warnings, and provides information on how to prevent, respond to, and handle an attack against information systems. High-level staff, mainly engineers, work at CERTA.
- CERT-IST (CERT-Industry, Services, and Tertiary) was launched in 1999 by Alcatel (a telecom company), CNES (the French Space Agency), France Telecom, and the TotalFinaElf energy group. It serves France's private sector as a contact point for security incident response.

167 http://www.bull.com/fr/isdf/pgena.htm.
168 http://www.renater.fr.
169 http://www.certa.ssi.gouv.fr.

CERT-IST provides alerts and means of protection against computer attacks aimed at French enterprises. It also helps the association members with incident handling.[170] CERT-IST interacts with the French national security organizations SGDN and DCSSI, in conjunction with CERT-RENATER and CERTA.[171]

CLUSIF (Club de la Sécurité des Systèmes d'Information Français)

The Club de la Sécurité des Systèmes d'Information Français (CLUSIF), created in 1984, is a non-profit organization of over 600 members representing 300 corporations or administrative organizations. CLUSIF fosters the sharing of information and experiences between its members, keeps users informed about new IT security material, and provides IT security information and whitepapers. Furthermore, it is involved in CIIP activities related to education, raising awareness, and security threat analysis.[172]

The Secretary-General of National Defense (SGDN) is also an early-warning actor, to the extent that the office coordinates the ministerial officials known as High Functionaries of Defense (Hautes fonctionnaires de Défense).[173]

170 http://www.cert-ist.com.

171 DDSI – Dependability Overview, op. cit., p. 107.

172 https://www.clusif.asso.fr/en/clusif/present.

173 Présentation des nouvelles orientations de l'Etat en sécurité des systèmes d'information. Séminaire DCSSI-AFNOR (27 March 2003). http://www.ssi.gouv.fr/fr/actualites/afnor-dcssi-270303/pdf/AFNOR270303.pdf.

Law and Legislation

French Penal Code 2004

Amended as Law no.2004-575 of 21 June 2004, entered into force on 23 June 2004.

Article 323-1
Fraudulent accessing or remaining within all or part of an automated data processing system is punishable by a sentence not exceeding two years' imprisonment and a fine. Where this behavior causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence shall not exceed three years' imprisonment and a fine.

Article 323-2
Obstruction or interference with the functioning of an automated data processing system is punished by a sentence not exceeding five years' imprisonment and a fine.

Article 323-3
The fraudulent introduction of data into an automated data processing system or the fraudulent suppression or modification of the data that it contains is punished by a sentence not exceeding five years imprisonment and a fine.

Article 323-3-1
Fraudulently, and without legitimate motive, importing, holding, offering, selling or making available any equipment, tool, computer program or any data designed or particularly adapted to commit one or more offences provided for by articles 323-1 to 323-3, is punishable by the sentences prescribed for offences in preparation or the one that carries the heaviest penalty.[174]

174 http://www.cybercrimelaw.net/countries/france.html.

Germany

Critical Sectors

The main assumption underlying CIP/CIIP in Germany is that both the government and society as a whole depend heavily on a secure infrastructure. All elements of the infrastructure whose failure would result in supply shortages or other dramatic consequences for large parts of the population are defined as critical. According to the German constitution, it is the state's task to guarantee public security and order and to ensure that the population is provided with essential goods. The state therefore has a responsibility to ensure the protection of critical infrastructures.

The following are the principal infrastructure sections defined as critical in Germany:

- Transportation and Traffic (Aviation, Sea Traffic, Rail Traffic, Local Traffic, Inland Water Transportation, Road System, Postal System),
- Energy (Electricity, Mineral Oil, Gas, Nuclear Power Stations),

* The Country Survey of Germany 2006 was reviewed by Susanne Jantsch, Consultant.

- Hazardous Materials (Chemical and Biological Substances, Hazardous Material Transportation, Defense Industry),
- Telecommunications and Information Technology,
- Finance and Insurance (Banking, Finance, Financial Service Provider, Stock Markets),
- Services (Emergency Services, Health Care Services, Civil Protection, Food and Water Supply, Waste Management),
- Public Administration and Justice System (Government, Government Agencies, Public Administration, Police, Customs, and Federal Armed Forces),
- Other (Media, Major Research Establishments, Outstanding or Symbolic Buildings, Cultural Assets) .[175]

Past and Present Initiatives and Policies

In the past five to ten years, many activities have been undertaken that were directly or indirectly related to the issue of critical infrastructure protection. They emerged from inter-ministerial activities begun in 1997 at the initiative of the federal minister of the interior, motivated in part by the study produced by the "US President's Commission on Critical Infrastructure Protection". The events of 11 September 2001 added urgency to ongoing efforts and, as part of the campaign against terrorism, contributed to widening the scope of national activities and intensifying the international dialog.

The presentation of two key documents in 2005 can be seen as the first result of these activities: The "National Plan for Information Infrastructure Protection (NPSI)",[176] enacted by a cabinet decision of the federal government, and the "Baseline Protection Concept for Critical Infrastructure Protection".[177] The NPSI aims at strengthening IT security in the nation's IT-dependent infrastructures and at enabling swift responses to IT-related crises,

175 http://www.bsi.bund.de/fachthem/kritis/kritis_e.htm.

176 http://www.bmi.bund.de/cln_028/Internet/Content/Nachrichten/Archiv/Pressemitteilungen/2005/08/Information__Infrastructure__en.html.

177 Bundesministerium des Innern. Schutz Kritischer Infrastrukturen – Basisschutzkonzept, (Berlin, August 2005). http://www.bmi.bund.de/cln_012/nn_122052/Internet/Content/Common/Anlagen/Broschueren/2005/Basiskonzept__kritische__Infrastrukturen,templateId=raw,property=publicationFile.pdf/Basiskonzept_kritische_Infrastrukturen.

while the "Baseline Protection Concept for Critical Infrastructure Protection", developed in close cooperation between the Federal Ministry of the Interior (BMI), the Federal Office for Civil Protection and Disaster Response (BBK), the Federal Criminal Police Agency (BKA),[178] and the private sector, provides guidance for the analysis of potential hazards such as terrorist attacks, criminal acts, and natural disasters, as well as recommendations for adequate protective measures.

AG KRITIS

Initiated by the report of the "President's Commission on Critical Infrastructure Protection (PCCIP)" in the US, an inter-ministerial working group on CI (AG KRITIS) was established in 1997 by the federal minister of the interior.[179] It consisted of the ministerial representatives, a steering committee, and a permanent office at the Federal Office for Information Security (BSI). The mandate of AG KRITIS was to:

- Describe possible threat scenarios for Germany,
- Conduct a vulnerability analysis of Germany's crucial sectors,
- Suggest countermeasures,
- Sketch an early-warning system.

In the first half of 1998, AG KRITIS conducted a survey of the federal public administration with a focus on the identification of the specific CII situation in the individual administrative agencies, an analysis of the IT dependency of each infrastructure sector, and an assessment of possible risks. Here is an overview of the main results:

- The awareness of IT threats varied heavily from agency to agency;
- There was a strong reluctance among the interviewees to reveal vulnerabilities in the IT security structure;
- Generally, hacking and unauthorized access to data are seen as the main threats for IT systems.

178 http://www.bka.de.

179 AG KRITIS. Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland. Kurzbericht der Ressortarbeitsgruppe KRITIS. (Entwurfsversion 7.95, December 1999). http://www.iwar.org.uk/cip/resources/Kritis-12-1999.html. The report itself was never published.

The creation of AG KRITIS was an important basis for all further activities of public agencies in Germany. Other agencies, e.g. the Federal Office for Information Security (BSI), are continuing its work.[180]

Situational Analysis of Threats and Hazards

The report of the AG KRITIS was handed over to the Federal Ministry of the Interior in 2000. Although not released to the public, the report resulted in further analysis of threats and hazards. These activities were intensified after the events of 11 September 2001 and after the floods of the Danube, Oder, and Elbe rivers in the following years. The following sections provides summaries of reports and recommendations.

Comprehensive Reports on Threats and Hazards

In autumn of 2001, the Ministry of the Interior published a second comprehensive threat analysis for Germany.[181] The IT section in this report is an attempt to answer the questions identified by the AG KRITIS study. Besides other threats, information security is defined as crucial for the security of the German society and for the success of its economy. It states that all measures, techniques, and instruments necessary for the protection of the vital infrastructure systems that rely on information technology are available. Rigorous application of those measures would eliminate a vast proportion of the threat. The risk-management approach to information security proposed in this report delegates the responsibility to the individual company providing information infrastructure services.

Kirchbach Report

The Kirchbach Commission, established after the devastating flood of 2002 in the Free State of Saxony, analyzed the overall structure of the German

180 http://www.bsi.bund.de.

181 Federal Ministry of the Interior. Zweiter Gefahrenbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bevölkerung bei Grosskatastrophen und im Verteidigungsfall (Berlin, October 2001). http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Broschueren/2001/Zweiter__Gefahrenbericht__der__Id__62160__de.html.

Emergency Protection System. Besides the focus on the flood disaster, it included a comprehensive analysis of existing facilities, and recommendations for future capacities to secure information and communications technology in cases of emergency.[182] This disaster and the conclusions of the Kirchbach report triggered a broad range of measures in a variety of ministries and agencies.

Report on the IT Security Situation in Germany

In July 2005, the BSI published a report on the "IT Security Situation in Germany"[183] that provides a survey of current threats to information and information systems, of the challenges to be met to secure information infrastructures, and of trends related to new information technologies and evolving threats.

Critical Infrastructure Protection – Baseline Protection Concept

The "Baseline Protection Concept for Critical Infrastructure Protection",[184] developed in close cooperation between the BMI, the BBK,[185] the BKA,[186] and the private sector, was published in September 2005. The concept aims at reducing the vulnerability of critical infrastructures with respect to natural incidents or accidents, but also to terrorist attacks or criminal acts. The concept recommends a process for analyzing infrastructures and planning adequate measures, and it provides a checklist to support this process.

CIIP in Germany

Since 2001, several departments at the Federal Office for Information Security (BSI) have been expanded and given additional tasks to support critical infrastructure protection.

On its website, the Federal Office for Information Security (BSI) regularly updates information and practical advice[187] for providers of critical in-

182 Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung. Flutkatastrophe 2002 (2nd ed., 2003). http://home.arcor.de/schlaudi/Kirchbachbericht.pdf.

183 Federal Office for Information Security (BSI). The IT Security Situation in Germany in 2005 (2005). http://www.bsi.de/english/publications/securitysituation/lagebericht2005_englisch.pdf.

184 Basisschutzkonzept, op. cit.

185 http://www.bbk.bund.de.

186 http://www.bka.de.

187 http://www.bsi.de/fachthem/kritis/index.htm.

frastructures. In October 2005,[188] the BSI published a set of methods and tools to enhance IT security in critical infrastructures,[189] several of which are available in English.[190]

Infrastructure Analysis Studies

In mid-2002, the BMI and the BSI commissioned a series of systematic studies of the CI/CII sectors. These studies have been completed and are currently being used to build a database for instant information access in case of an emergency related to information infrastructures, and for continuous situation evaluation. The database is still in the making and may become the foundation for interdependency research in and between different CI/CII sectors. This database contains basic information on the infrastructure sector gained through interviews, workshops, and a standardized questionnaire.[191]

Campaign for "Security in the Internet"

The campaign for "Security in the Internet"[192] is a combined initiative undertaken by the BMI, the Ministry of Economics and Labor, and the BSI. Its main objective is to provide small and medium-sized enterprises with a sound basis of information that encourages the use of the internet and internet-based services, and with adequate attention to all relevant IT security issues.[193]

IT Security Guidelines

The "IT Security Guidelines" published by the BSI are intended to satisfy the needs of small and medium-sized businesses, providing a compact overview of the most important IT security measures that is intelligible to the non-expert. The focus is on organizational safeguards and on illustrating threats through practical examples.[194]

188 http://www.bsi.de/presse/kurzmeldung/051005kritis.htm.
189 http://www.bsi.de/fachthem/kritis/hilfsmittel.htm.
190 http://www.bsi.de/fachthem/kritis/utilities.htm.
191 http://www.bsi.de/fachthem/kritis/index.htm.
192 http://www.sicherheit-im-internet.de. Note: the initiative was re-launched with the current focus on support for small and medium-sized enterprises at the end of 2003.
193 A similar initiative is: http://www.sicher-im-netz.de.
194 Federal Office for Information Security (BSI). IT Security Guidelines: IT Baseline Protection in brief (Bonn: 2004). http://www.bsi.bund.de/english/gshb/guidelines/guidelines.pdf.

National Plan for Information Infrastructure Protection (NPSI)

The National Plan for the Protection of Information Infrastructures (NPSI) is the federal government's strategy for a comprehensive approach to the protection of IT systems.[195] The NPSI pursues three strategic objectives:

- Prevention – protecting information infrastructures adequately;
- Reaction – effective acting during IT security incidents;
- Sustainability — strengthening IT security expertise and promoting international standards.

This strategy addresses public authorities as well as businesses and individuals. The development of processes for the implementation of the NPSI throughout the federal government agencies, under the lead of the Ministry of the Interior (BMI) and in cooperation with all other federal ministries, will be completed in 2006. The various ministries will then be responsible for implementing the agreed measures in their area of accountability.

The BMI will invite providers of critical infrastructure and IT security professionals to join in the development of guidelines for the implementation of the NPSI objectives.

For citizens, timely updates of information campaigns such as "BSI for the citizen",[196] "Security in the Internet", and other initiatives will be available.

Awareness and Support for the Citizen

The internet service "BSI for the citizen"[197] aims to provide easy-to-understand background information on IT security and the internet, and offers guidance on how to surf the internet and use internet-based applications securely. The information includes up-to-date warnings on new internet threats and a newsletter.

195 A succinct overview in English with several links to relevant documentation (only German, as of September 2005) is available at: http://europa.eu.int/idabc/en/document/4591/194.

196 „BSI für Bürger": http://www.bsi-fuer-buerger.de.

197 Ibid.

International Outreach

A joint initiative of the German Ministry of the Interior[198] and the US Department of Homeland Security[199] at the ministerial level has established the basis for future cooperation for enhancing the protection of computer systems and networks. As a mid-term measure, a joint early-warning system will be created. This bilateral initiative complements the already ongoing counter-terrorism efforts. Furthermore, both parties agreed to foster regular consultations in international organizations in order to enhance multilateral cooperation. Multilateral conferences such as the International Watch, Warning and Incident Response Workshop held in Berlin in October 2004 are aimed at developing and improving methods for multinational cooperation.

Secure e-Government and BundOnline 2005

The e-government initiative aims at a consistent use of modern information and communications technology in order to make administrative processes more efficient and to facilitate an exchange between the business community, the public, and the administration.

The objective of the BundOnline 2005 initiative – to make all suitable government services available to the public through the internet — was successfully concluded in August 2005. The BSI was tasked with developing the basic IT security component and with setting up the data security competence center. The BSI also publishes the "e-Government Manual" covering all aspects of secure e-government and presenting pragmatic approaches. In addition, the BMI has established a knowledge management system for BundOnline 2005.[200]

198 http://www.bmi.bund.de.
199 http://www.dhs.gov.
200 http://www.wmsbundonline.de.

Organizational Overview

The overall responsibility for, and coordination of, major CIP- and CIIP-related activities rests with the Federal Ministry of the Interior (BMI), together with several of its subordinated agencies, such as the Federal Office for Information Security (BSI)[201], the Federal Agency of Civil Protection and Disaster Response (BBK)[202], the Federal Law Enforcement Agency (BKA), and the Federal Police (BPOL).[203] For coordination within the ministry and the subordinated agencies, a task force for critical infrastructure protection (PG KRITIS) was established at the BMI in 1999.[204] Strategy development and implementation are also coordinated with other federal ministries, especially the Federal Ministry of Economics and Technology, the Office of the Chancellor of the Federal Republic of Germany,[205] the Federal Ministry of Justice, the Federal Ministry of Foreign Affairs, the Federal Ministry of Defense, and other relevant agencies, such as the Federal Network Agency.[206] Furthermore, strategic partners from the private sector are consulted.[207]

Public Agencies

Federal Ministry of the Interior (BMI)

As the government agency responsible for ensuring Germany's internal security, the Federal Ministry of the Interior (BMI) is closely involved with CIP/CIIP. This is where the relevant topics are dealt with and coordinated, such as physical protection within the context of civil protection and disaster response, threat prevention within the context of law enforcement, and all areas of IT and IT dependence. The authority in charge of IT-related issues with regard to CIP is

201 "Bundesamt für Sicherheit in der Informationstechnik". http://www.bsi.bund.de.
202 "Bundesamt für Bevölkerungsschutz und Katastrophenhilfe". http://www.bbk.bund.de.
203 "Bundespolizei": http://www.bundespolizei.de; formerly "Bundesgrenzschutz".
204 See, e.g., the brochure on CIIP in Germany at: http://www.bsi.bund.de/fachthem/kritis/ciip_en.pdf, p. 2.
205 "Bundeskanzleramt".
206 "Bundesnetzagentur": http://www.bundesnetzagentur.de/enid6c28cf7e908c093de1d8973191d1ed59,0/xn.html.
207 http://www.bmi.bund.de/cln_012/nn_163922/sid_8482804BA61AD772670A96F56684C062/nsc_true/Internet/Content/Themen/Informationsgesellschaft/Einzelseiten/IT__sicherheitskultur__2.html.

Department IT 3 (Security of Information Systems) under the Federal Ministry of the Interior's Chief Information Officer.

Germany participated in the OECD survey on the IT security culture in member states. The Ministry of the Interior (BMI) has summarized the answers on ten topics and published these on its website.[208]

The Federal Office for Information Security (BSI)

The Federal Office for Information Security (BSI), one of the agencies under the Federal Ministry of the Interior, plays an especially important role in CIP. The BSI deals with all areas related to security in cyberspace and takes preventive action by analyzing IT weaknesses and developing protective measures, including the following:

- Internet security: analyses, concepts, advice (including the IT Baseline Protection Manual);[209]
- Management of the computer emergency response team (CERT) and virus center;
- Network security and cryptology, public key infrastructure (PKI), and biometrics;
- Critical infrastructure;
- e-Government.

The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and develops solutions. Even in technically secure information and telecommunications systems, risks and damage can still occur. In order to minimize or avoid these risks, the BSI's services address a wide audience: it advises manufacturers, distributors, and users of information technology. It also analyses developments and trends in information technology.

The BSI is organized in four divisions, one central and three specialized divisions:

208 http://www.bmi.bund.de/cln_012/nn_163922/Internet/Content/Themen/Informationsgesellschaft/DatenundFakten/IT__Sicherheitskultur__0.html.

209 http://www.bsi.bund.de/english/gshb/manual/index.htm.

- Security of Applications, Critical Infrastructure, and Internet Division,
- Cryptography, Cryptographic Technology, and Scientific Foundations Division,
- Counter-Eavesdropping, Certification, Approval, Accreditation Division.[210]

Federal Office for Civil Protection and Disaster Response (BBK)

In order to facilitate cooperation between the different levels of public authority, a Federal Office for Civil Protection and Disaster Response (BBK) was established on 1 May 2004 within the Ministry of the Interior.[211] One of the main functions of this agency is information-sharing and resource allocation in case of an emergency. A public-relations and information website has been established.[212] This German Emergency Preparedness Information System (deNIS) provides general information about organizations, emergency potentials, and web links on emergency precaution and preparedness.[213]

Moreover, decision-makers at the federal and state levels will be able to pool, process, and distribute resources in cases of wide-ranging catastrophes. In particular, securing the energy and food supply and a smooth functioning of the information infrastructure are regarded as elementary. In a further stage of development, a secure and classified system called deNIS II will be established.[214] Every international request for emergency support from Germany will be handled through deNIS.[215]

The BBK has a special focus on CIP. It operates in close cooperation with the BSI and the Regulatory Agency for Telecommunication and Post (RegTP) in the field of CIIP and evaluates the vulnerabilities and redundancies of ICT services as well as their interdependencies. Moreover, contingency plans and appropriate measures will be developed according to case studies.[216]

210 http://www.bsi.de/english/functions.htm.

211 http://www.bbk.bund.de/cln_007/nn_398002/DE/00__Home/homepage__node.html__nnn=true.

212 http://www.denis.bund.de.

213 Zentralstelle für Zivilschutz, Leistungspotenziale im Zivilschutz. Deutsches Notfallvorsorge-Informationssystem, (Februar 2003). http://www.denis.bund.de/imperia/md/content/intern/1.pdf.

214 Ibid.

215 http://www.denis.bund.de.

216 http://www.bbk.bund.de/cln_027/nn_398882/DE/02__Themen/06__SchutzKritischerInfrastrukturen/01__Themen/02__InformationstechnikundTelekommunikation/InformationstechnikundTelekommunikation__node.html__nnn=true.

The Federal Criminal Police Agency (BKA)
The Federal Criminal Police Agency (BKA)[217] is responsible in the first instance for prosecuting crimes against the internal or external security of the Federal Republic of Germany and crimes involving damage to or the destruction of critical infrastructures that could result in a serious threat to life, health, or the functioning of society. Further, the BKA is the central agency for investigating crimes involving information and communications technology.

Federal Ministry of Economics and Technology (BMWi)

With more than 90 per cent of Germany's critical infrastructure being privately owned, the Federal Ministry of Economics and Technology (BMWi)[218] also plays a role, as its brief includes economic policy. With regard to the energy sector, one of the BMWi's tasks is developing the framework for securing the energy supply. According to Article 87f of the German constitution, the BMWi is also responsible for ensuring the availability of adequate telecommunications infrastructure and services.

Federal Network Agency
In July 2005, the Regulatory Authority for Telecommunications and Posts was renamed the Federal Network Agency. The Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway is a separate higher federal authority within the scope of business of the Federal Ministry of Economics. The Federal Network Agency's task is to provide, by liberalization and deregulation, for the further development of the electricity, gas, telecommunications, and postal markets and, as of January 2006, of the railway infrastructure market as well.[219]

Other ministries involved

The Federal Ministry of Justice (BMJ)[220] is responsible for relevant legislation, in particular for ensuring that national laws comply with the cyber-crime agreement of 23 November 2001.

217 http://www.bka.de.
218 http://www.bmwi.de.
219 http://www.bundesnetzagentur.de/enid/0a888f9d9a85f3748b2d8fb635f752e7,0/xn.html.
220 http://www.bmj.bund.de.

The Federal Ministry of Defense (BMVg)[221] is involved in the context of its responsibility for national defense and for maintaining troop readiness and performance.

The Federal Chancellery plays a coordinating role at the ministerial level. Additional ministries with specific areas of responsibility are also involved in CIP.

Responsibilities are also shared among the agencies within the remit of the various ministries. The Federal Intelligence Service (BND) and the Federal Office for the Protection of the Constitution (BfV) provide important information regarding the threat situation and possible domestic targets.

Public-Private Partnerships

The prevalent assumption in Germany is that cooperation between the public and the private sectors is the best strategy. There are several cooperation initiatives in Germany between public and private actors related to CIIP.

Initiative D21

Initiative D21[222] is the largest public-private partnership in Germany. This economic initiative also deals with information security. Initiative D21 is a neutral platform, independent of party allegiance and of individual industrial sectors. D21 is a model of an "activating government" with about 400 participants representing all sectors of industry (not only ICT providers), institutions, and politics. Initiative D21 pursues a steadily growing number of projects. Initiative D21 is organized into four subject areas (steering groups):

- Education, Qualification and Equality of Opportunity,
- e-Government/Security and Trust in the Internet,
- Information and Communications Technologies in Healthcare,
- Growth and Competitiveness, with the focal issues being broadband technology and the mobile society.[223]

221 http://www.bmvg.de/C1256F1200608B1B/vwContentByKey/W2653DJT532INFOEN.
222 http://www.initiatived21.de/english/index.php.
223 Ibid.

Working Group on Infrastructure Protection (AKSIS)

Based on the assumption that the increasing dependability of society on CII means the associated risks must be studied in a comprehensive approach, the Working Group on Infrastructure Protection (AKSIS)[224] was established in 1999 at the initiative of the Center for Strategic Studies (ZES),[225] which belongs to the IABG (Industrieanlagen-Betriebsgesellschaft) company. The main purpose of AKSIS is to provide a forum for information exchange to analyze and assess the dependability of CI/CII sectors. AKSIS has no official government or industry mandate. It is purely voluntary and informal. It holds two meetings per year, bringing together representatives of the public and private sectors (ministries, armed forces, police, telecommunication, energy, transport, banks, academia, etc.). Models for close cooperation between the government's CII protection initiative and AKSIS are currently being discussed.

Early Warning and Public Outreach

CERT-Bund

The CERT-Bund Unit was established on 1 September 2001 at the Federal Office for Information Security (BSI). CERT-Bund is a central contact point charged with protecting the security of data processors and networks of the federal public administration. CERT-Bund also offers some of its services to clients from the private sector. However, several services are only available to the federal administration (e.g., incident response).[226] CERT-Bund's main tasks include warning and information-sharing, data collection, analysis and processing of information, documentation and dissemination, sensitization of IT decision-makers, and cooperation with existing CERTs.[227]

224 Arbeitskreis zum Schutz von Infrastrukturen, AKSIS: http://www.aksis.de.

225 Zentrum für Strategische Studien (ZES).

226 Ennen, Günther. "CERT-Bund – eine neue Aufgabe des BSI". In: KES Zeitschrift für Kommunikations- und EDV-Sicherheit. Bundesamt für Sicherheit in der Informationstechnik (BSI). (Bonn, June 2001), p. 35. See also http://www.bsi.bund.de/certbund/index.htm.

227 Ennen, CERT-Bund, op. cit., p. 35.

Mcert

The study "Security and Trust in the Internet", a product of the project CERT Infrastructure Germany,[228] was published in January 2002. It determined that a CERT addressing the needs of small and middle enterprises (SMEs) was required in addition to the existing CERTs (such as dCERT,[229] DFN-CERT,[230] S-CERT,[231] secu-CERT,[232] Telekom-CERT, and CERT-Bund[233]). This gap was closed with the collaborative establishment of Mcert[234] between the Federal Ministry of Economics and Technology, the Ministry of the Interior, and the non-profit organization BITKOM[235] in 2003. Some major IT players in Germany are already members and sponsors of this new body. Mcert offers a basic and a professional package, where the first addresses SMEs without in-house IT departments or security resources and provides them with a suitable warning service, while the professional package offers support for companies with an in-house IT organization.

CERT-Network

The "CERT-Verbund" (CERT Network) is an alliance of German security and computer emergency teams.[236] The alliance provides a common base for cooperation between the teams and also allows the pursuit of the overarching objectives, namely to ensure the protection of national IT networks or to prepare for swift and coordinated reaction in case of larger IT security incidents.

228 http://www.initiative21.de/druck/news/publikationen2002/doc/24_1053502570.pdf .
229 http://www.dcert.de/index_e.html.
230 http://www.cert.dfn.de.
231 http://www.s-cert.de.
232 http://www.secunet.de.
233 http://www.bsi.de/certbund/index.htm.
234 http://www.mcert.de.
235 http://www.bitkom.org.
236 http://www.cert-verbund.de.
237 http://www.iid.de/iukdg/gesetz/Signaturg_engl.pdf.

IT Crisis Response Center

To be prepared for national crisis situations affecting information infrastructures, Germany plans to establish an IT Crisis Response Center. This center is foreseen as a non-standing organization located at the BSI, closely related to a control and analysis center tasked with continually providing a reliable assessment of the IT security situation in Germany. Situational changes indicating a crisis will activate IT crisis response functions to warn and alarm potentially affected parties. Moreover, the center supports a coordination board for IT security of the federal ministries in organizing timely response to minimize and to contain damage, and to return swiftly to the safe and secure operation of affected information infrastructures.

Law and Legislation

Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations

The purpose of this law is to create the conditions for the use of electronic signatures. This law deals with issues such as technical security, voluntary accreditation, supervision, liability, and data protection.[237]

Information and Telecommunications Services Act 1997

The Information and Telecommunications Services Act of 1997[238] was the starting point for the liberalization of the German telecommunications market.[239] This act is a bundle of laws comprising the Electronic Signature Act and the Teleservices Act (TDG).[240]

238 http://www.iid.de/iukdg/gesetz/iukdge.html.
239 Interview with a representative of the consulting company Industrieanlagen-Betriebsgesellschaft (IABG), May 2002.
240 http://www.iukdg.de/english.html.

Electronic Signature Act 2001/2005

In May 2001, this act (which conforms to EU regulations) replaced the existing pioneer Digital Signature Act of 1997. The main purpose of the act is to define a framework for the handling of electronic signatures.[241] The act was further amended as of 11 January 2005.

Act on the Utilization of Teleservices

This act will be the basis for the establishment of uniform economic conditions for the various applications of electronic information and communication services.[242]

Teleservices Data Protection Act

The purpose of this act is to define provisions to protect the personal data of teleservice users within the framework of the Act on the Utilization of Teleservices, which governs the collection, processing, and utilization of such data by service providers.[243]

German Penal Code

Section 202a. Data Espionage

(1) Any person who obtains without authorization, for himself or for another, data that are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine.
(2) Subsection 1 only applies to data stored or transmitted electronically or magnetically or in any form not directly visible.

241 http://bundesrecht.juris.de/index.html.
242 http://www.iid.de/iukdg/aktuelles/fassung_tdg_eng.pdf.

Section 303a. Alteration of Data

(1) Any person who unlawfully deletes, suppresses, renders useless, or alters data (section 202a(2)) shall be liable to imprisonment for a term not exceeding two years or to a fine.
(2) The attempt shall be punishable.

Section 303b. Computer Sabotage

(1) Any person who interferes with data processing that is of essential importance to another business, another enterprise, or an administrative authority by:

1. Committing an offense under section 303a(1), or
2. Destroying, damaging, rendering useless, removing, or altering a computer system or a data carrier,

shall be punished by imprisonment not exceeding five years or a fine.

(2) The attempt shall be punishable.[244]

243 http://www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf.
244 http://www.cybercrimelaw.net/countries/germany.html; and http://www.iukdg.de.

India

Critical Sectors

In India, the following sectors are considered critical:

- Banking and Finance,
- Insurance,
- Civil Aviation,
- Telecommunications,
- Atomic Energy,
- Power,
- Ports,
- Railways,

* The Country Survey of India 2006 was reviewed by Subimal Bhattacharjee, Argus Integrated Systems. Luthra & Luthra Law Offices reviewed and contributed substantially to the section on Law and Legislative Action.

- Space,
- Petroleum and Natural Gas,
- Defense,
- Law Enforcement Agencies.

These 11 critical sectors were identified by the National Task Force on Y2K a few years ago, taking into account the extent of penetration of information technology in these sectors and the impact that a disruption of any of these sectors would have.[245]

Past and Present Initiatives and Policies

In India, many efforts in the field of CIIP were triggered by the governments' goal of making the country a leading knowledge-driven global economy by boosting IT and e-business. In 1998, the prime minister of India announced a drive to make India an IT superpower and one of the largest generators and exporters of software in the world within the next ten years. The government of India has recognized the potential of IT for rapid national development.[246] Therefore, a National Task Force on Information Technology and Software Development[247] and a Department of Information Technology (DIT), also dealing with CIIP, have been set up.[248]

National Task Force on Information Technology & Software Development and Information Technology Action Plan

The Indian government has given top priority to developing an appropriate action plan for the country to emerge as a global leader in the field of IT. As a first step, the National Task Force on IT and Software Development[249] was set up by Prime Minister Shri Atal Behari Vajpayee on 22 May 1998, under

245 Mishra, Vineeta. "Critical sectors to be Y2K ready in time: govt report". In: India Times, 19 October 1999. http://www.apnic.net/mailing-lists/s-asia-it/archive/1999/10/msg00050.html.
246 National Task Force on Information Technology and Software Development. Information Technology Action Plan, Preamble, 4 July 1998. http://it-taskforce.nic.in/prem.htm.
247 http://it-taskforce.nic.in.
248 http://mit.gov.in.
249 http://it-taskforce.nic.in.

the chairmanship of the deputy chairman of the planning commission. This task force had a mandate to formulate the draft of a "National Informatics Policy", including:

- To recommend an appropriate institutional mechanism to implement this policy as a national mission with the participation of the central and state governments, industry, academic institutions, and society at large;
- To prepare a vision statement that will excite and energize the people of India, creating the faith in them that information technology aids personal and national growth. The task force will also suggest a strategy for the effective articulation and dissemination of that vision, so as to create an ethos, an ambiance, a mindset, and a work culture that is consistent with the needs of the emerging knowledge-driven global civilization;
- To prepare a blueprint for the nationwide adoption of information technology, with a network of task forces at all governmental and non-governmental levels.[250]

The IT Task Force submitted its first report in the form of an "Information Technology Action Plan" to the prime minister on 4 July 1998. The report contains a special section on "IT for all by Year 2008", the centerpiece of which is a major national campaign called "Operation Knowledge", focusing on spreading of IT and IT-based education at all levels.[251]

The establishment of the Task Force is a clear indication that information technology is an area where India wants to achieve global pre-eminence. It is hoped that IT, fostered by these government policies, will prove immensely useful in all areas of national economy — especially industry, trade, and services — and will contribute significantly to making India a global economic power.[252]

250 http://informatics.nic.in/archive/inf98jul/cover.htm.

251 The IT Action Plan included, among others the following measures: Ministries and departments to earmark 1–3 per cent of their budget for IT; IT literacy requirement for government/public-sector employment; software and IT to be treated as priority sector by banks; zero tax on all IT products by Year 2002; access to internet through cable TV; early introduction of IT legislation; networking of all engineering/medical colleges and universities before 2000. http://it-taskforce.nic.in/index.html.

252 Ibid.

National e-Governance Plan (NeGP)

The government of India has approved the National e-Governance Plan (NeGP) for the years 2003–2007. The plan should lay the foundation and provide the impetus for long-term growth of e-governance within the country. The plan is intended to create the right government and institutional mechanisms, to set up the core infrastructure and policies, and to make the public administration more responsive to the needs of citizens and businesses.

The NeGP has started to realize three important elements of the e-Governance Plan that form the core infrastructure for effective service delivery: Data processing centers, State Wide Area Networks (SWANs), and Common Services Centres (CSCs).[253] In addition, the various state governments are also implementing large-scale e-governance projects across the country.

Core Group on Standards for e-Governance

Under the NeGP, standards for e-governance are crucial to ensure integration and interoperability of data and e-applications. The Department of Information Technologies (DIT) has therefore constituted a Core Group on Standards for e-Governance[254] to develop an institutional mechanism and processes, and to recommend key areas for standardization. Some of the priority areas for standardization are:

- Technical standards,
- Localization standards,
- Quality and documentation,
- Security standards,
- Metadata and data standards for various application domains.

253 Department of Information Technology. Annual report 2004–2005, p. 2. http://www.mit.gov.in/annualreport2004-05.zip.

254 http://egov.mit.gov.in.

An apex body has been constituted under the chairmanship of the secretary of the DIT with senior representatives from the government, the National Association of Software and Service Companies (NASSCOM),[255] the Bureau of Indian Standards (BIS), and others with a mandate to approve, deliver notification of, and enforce the standards formulated by various working groups and to ensure that they are in accordance with international practices.

The National Informatics Centre (NIC)[256] publishes whitepapers on all the desired standards, which serve as discussion papers for the working groups that develop the standards. The working groups with representatives of the DIT, associations, industry, academia, and central and state governments etc. will be constituted with the approval of the DIT.

The standards approved by the apex body will be released on the web by the Standardization Testing & Quality Certification (STQC) Directorate, an office attached to the DIT. The STQC will further ensure conformance and certification (where required) of these standards. The e-Governance Division of the NIC and the STQC will function in tandem with the e-Governance Programme Management Unit at DIT.[257]

Organizational Overview

Public Agencies

In the Indian government, the National Information Board (NIB) is at the very top of the national information security structure. Directly linked to the NIB are the National Technology Research Organization (Technical Cybersecurity) and the National Information Security Coordination Cell (NISCC) which

255 http://www.nasscom.org.

256 The National Informatics Centre (NIC) of the Department of Information Technology provides network backbone and e-governance support to the central government, state governments, administrations, districts, and other government bodies. It offers a wide range of ICT services, including a nationwide communication network for decentralized planning, improvement in government services, and greater transparency of national and local governments. The NIC closely collaborates with central and state governments in implementing IT projects. See http://home.nic.in.

257 Information provided by Indian expert involved.

is part of the National Security Council Secretariat (NSCS). The NIB has instructed the NSCS to coordinate cyber-security activities across the country. The NISCC provides necessary input for the consideration of the NIB. It works through the Sectoral Cyber Security Officers (SCOs).

Directly below the NIB are the Information Infrastructure Protection Centre (IIPC), followed by state cyber police stations; and the Computer Emergency Response Team India (CERT-In), followed by state- and sectoral-level CERTs. Various ministries' coordinators of special functions are also situated at this level, as is the Development and Promotional Section of the Ministry of Communications and Information Technology (MOC).

National Information Board (NIB)

The set up of the National Information Board (NIB) was recommended by a group of ministers. It consists of 21 members. The national security advisor is the chairman of the board, while the deputy national security adviser serves as its member secretary. The NIB acts as the highest policy formulation body at the national level and periodically reports to the Cabinet Committee on Security of the Government of India, headed by the prime minister. The NIB is at the very top of the information security structure.[258]

National Information Security Coordination Cell (NISCC)

The NIB has charged the National Security Council Secretariat (NSCS) with coordinating cyber-security activities across the country, covering both the public and the private sectors. NISCC, which is part of NSCS, provides necessary input to NIB for its consideration. It works through the Sectoral Cyber Security Officers (SCOs). There are 20 such SCOs in various ministries where the senior officer holds the rank of a Joint Secretary or Director. The NISCC deals with the following topics: CERT functions, research and development, encryption, laws, interception and early warning, cyber-crime, training, and international cooperation. It represents the government in international forums for cyber-security and cyber-terrorism-related issues.[259]

258 Presentation by Commander Mukesh Saini of the National Security Council, India, at the Indo-US Cyber-Security Forum in Washington, DC, on 9–10 November 2004.

259 Information provided by Indian expert involved.

Information Infrastructure Protection Centre (IIPC)

The planned Information Infrastructure Protection Centre (IIPC) will provide advanced warning to critical infrastructure operators. Moreover, the IIPC will handle emergency incidents, undertake horizon scanning, and function as a law enforcement agency for the Indian cyberspace.[260]

Ministry of Communications and Information Technology (MOC): Department of Information Technologies (DIT)

The Department of Information Technologies (DIT),[261] part of the Ministry of Communications and Information Technology (MOC),[262] was established with the purpose of making India a leading IT nation by 2008. Through the DIT organization, the Indian government has undertaken several initiatives and strategies:

- The promotion of the internet and provision of IT infrastructure;
- The development of legislation;
- The support of IT education and development;
- The promotion of standardization, testing, and quality in IT;
- The establishment of an Information Security Technology Development Council (ISTDC);
- The creation of a National Information Security Assurance Framework;
- The establishment of Inter Ministerial Working Groups.[263]

The Indian Computer Emergency Response Team (CERT-In) and the Controller of Certifying Authorities (CCA) are also DIT organizations. The Standardisation, Testing, and Quality Certification (STQC) Directorate and the National Informatics Centre (NIC) are also attached offices of the DIT.[264]

260 Information provided by Indian expert involved.
261 http://www.mit.gov.in.
262 http://www.moc.gov.in.
263 http://www.mit.gov.in/about.asp. Cf. presentation by Shri R. Chandrashekhar "On The National E-Governance Plan - Approach & Key Components". National e Governance Plan - Workshop with States and UTs, (New Delhi, 11–12 March 2005). http://www.mit.gov.in/plan/cmmp.asp.
264 http://www.mit.gov.in/org.asp.

The DIT has set up the following Inter Ministerial Working Groups on:

- Cyber-Security Education and Research;
- Cyber-Security Assurance and Awareness;
- Encryption Policy and PKI;
- Legislation and Forensics in Cyberspace;
- Critical Infrastructure Protection.[265]

Standardisation, Testing and Quality Certification (STQC) Directorate
The Standardisation, Testing, and Quality Certification (STQC) Directorate is an office attached to the DIT. The STQC provides quality and security assurance services that meet international standards to Indian companies and users. The STQC program has been in place for over three decades, and the STQC has positioned itself as a prime provider of assurance services to both the hardware and the software industry, as well as for users. The recent focus of the DIT on IT security, software testing, and certification, and the assignment of a national assurance framework, have further raised the responsibility of the STQC as well as the expectations it must meet.[266] The STQC worked together with the US National Institute of Standards and Technology (NIST) to create a US standard for controls of Information Security, SP-800-53.

Information Security Technology Development Council (ISTDC)

The Information Security Technology Development Council (ISTDC)'s main objective is to facilitate, coordinate and promote technological advancements, and to respond to information security incidents, threats and attacks at the national level. ISTDC was established for the following functions:

- To evaluate the cyber-security project proposals, and to provide recommendations for further processing by DIT;
- To review on-going projects through monitoring committees and recommend any modification in scope, funding, duration, additional inputs, termination, transfer of technology;

265 Presentation by Shri R. Chandrashekhar, op. cit.
266 http://www.stqc.nic.in.

- To recommend follow-up action on completed projects – transfer of technology, initiation of next phase;
- To form project review and steering groups of projects approved and funded by the DIT.[267]

Public-Private Partnerships

Indo-US Cyber Security Forum

In pursuance of the Indo-US Cyberterrorism Initiative announced by Indian Prime Minister Shri Atal Behari Vajpayee and US President George Bush in Washington in November 2001, the first plenary session of the Indo-US Cyber Security Forum was held at the National Security Council Secretariat (NSCS) in India in April 2002. The second plenary meeting was held in Washington, DC in November 2004. This meeting resulted in the creation of five working groups on legal issues and law enforcement, research and development, emergency response and watch and warning, defense cooperation, and standardization. In the past year, the NSCS has organized five seminars and a workshop with the help of the Confederation of Indian Industry (CII). There has also been some exchange of experts.

The Indo-US Cyber Security Forum is a part of the Indo-US High Technology Group a public-private partnership between India and the US established to discuss and implement ways and means of increasing cooperation between the two countries in high-technology areas.

267 http://www.nasscom.org//download/india.pdf.

Early Warning and Public Outreach

Indian Computer Emergency Response Team (CERT-In)

The Indian Computer Emergency Response Team (CERT-In)[268] was established in January 2004 by the Department of Information Technologies (DIT) as part of the international CERT community. It has a mandate to respond to computer security incidents reported by the national computer and networking community as well as to create security awareness among Indian IT users. The main CERT is located in New Delhi, with backup in Bangalore. It has reactive as well as proactive functions.[269] CERT-In aims to become India's most trusted agency for responding to computer security incidents. In addition, CERT-In will also assist Indian IT users in implementing proactive measures to reduce the risks of security incidents.

Another five sector-specific CERTs have been set up: three for the army, air force, and navy; one for banking, known as FinCERT; and one for railways, known as RailCERT. It is anticipated that more CERTs will be established for the telecom and the power sectors.

CERT-In has recently appointed a panel of IT security auditors, whose tasks will include vulnerability assessment and penetration testing of computer systems and networks of various organizations of the government, critical infrastructure organizations, and in other sectors of Indian economy.[270] The auditors will assist CERT-In in assessing the information security risks. They will determine the effectiveness of information security controls over information resources and assets that support operations in the auditor organizations at their request.[271]

268 http://www.cert-in.org.in.
269 http://www.cert-in.org.in/roles.htm.
270 http://www.cert-in.org.in/audit-background.htm.
271 Ibid.

Law and Legislation

In the year 2000, the government of India enacted the Information Technology Act ("IT Act") to provide a framework for the legal recognition of electronic commerce in India. The IT Act provides for the establishment of a public-key infrastructure in India and addresses issues of cyber-crime and the admissibility of digital evidence. It achieves this through various provisions and by way of amendments to other statutes, such as the Indian Penal Code 1860, the Indian Evidence Act of 1872, the Bankers' Books Evidence Act of 1891, and the Reserve Bank of India Act of 1934. The amendments relate to the inclusion of electronic records and other such computerized data alongside the traditional forms of documents.

Information Technology Act 2000 (IT Act)

The IT Act comprises 13 chapters, divided into 94 sections. The chapters relevant to the present discussion are: Chapter V (Secure Electronic Records and Secure Digital Signatures), Chapter VII (Digital Signature Certificates), Chapter IX (Penalties and Adjudication), Chapter XI (Offences), and Chapter XII (Network Service Providers Not To Be Liable In Certain Cases).

The IT Act provides a much-needed legal framework for electronic transactions in India. The National Association of Software and Service Companies (NASSCOM), the leading trade body and the chamber of commerce of the IT software and services industry in India, summarizes some of its key progressive features as follows:[272]

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. First of all, these provisions have approved e-mail as a valid and legal form of communication in India that can be duly produced and approved in a court of law.
- Companies are now able to carry out electronic commerce using the legal infrastructure provided by the act.
- The act bestows legal validity and sanction on digital signatures.

272 http://www.nasscom.org/artdisplay.asp?cat_id=852.

- The act allows companies to become certifying authorities that may issue digital signature certificates.
- The act allows the government to issue legal notifications on the internet, a first step towards e-governance.
- The act enables companies to file any form, application, or other document with any office, authority, body, or agency owned or controlled by the government in such electronic formats as may be prescribed by the government.
- The IT Act also addresses important issues of security that are critical for the success of electronic transactions. The act has given a legal definition to the concept of secure digital signatures that must undergo a security procedure as stipulated there under.
- The act offers companies a statutory remedy in the case that anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the act is in the form of monetary damages not exceeding 10 million rupees.

In order to resolve IT-related disputes in a focused and timely manner, the IT Act provides for the constitution of a Cyber Appellate Tribunal, which acts as a forum for original jurisdiction on issues arising under the IT Act. Appeals from the tribunal can be made to the relevant state high courts.

Section 79 of the IT Act declares that no person providing any service as a network service provider shall be liable for any third-party information or data made available by him if he proves that the offense or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such an offense. This provision is crucial, as it is the only one under which a network service provider can claim a defense under the provisions of the act.

In order to further strengthen the scope and ambit of the IT Act, a committee has been set up comprising several experts in cyber-law and data protection who will review the act and make necessary changes to ensure that the existing lacunae in the law can be filled. These amendments are likely to deal with provisions concerning third-party liability, issues of privacy and data protection security, and the replacement of digital signatures with electronic signatures, among others.

IT related offenses under the IT Act

Section 43 of the IT Act specifies acts committed without the permission of the owner or person in charge of a computer, computer system, or computer network that may cause damage by destruction, alteration, deletion, addition, modification, or rearranging of any computer resource. The offenses specifically relate to: (a) accessing or securing access to a computer, computer system, or computer network; (b) downloading, extracting, or copying of data or information from such computers, computer systems, or computer networks; (c) introducing or causing to be introduced any virus or computer contaminant; (d) disrupting or causing disruption to computers, computer systems, or computer networks; (e) damaging or causing to be damaged any computer, computer system, or computer network or any programs residing therein; (f) denying or causing denial of access by any person authorized to use the computer system or computer network; (g) assisting a person in contravention of the IT Act; (h) manipulating a computer for financial benefit.

Sections 65 through 74 of the IT Act contain provisions relating to various cyber-crimes.

Hacking and Tampering with Computer Source Code

The popular and notorious offense of hacking is dealt with under Section 66 of the IT Act. Hacking is defined as the act of destroying, altering, deleting, diminishing in value, or injuriously affecting the information residing in a computer resource, by any means. An essential element of this offense is the intention or knowledge on the part of the perpetrator of causing the wrongful loss. This provision is often viewed as a "catch-all" provision because of its broad wording, which could be potentially used to cover any IT crimes that are not covered by any other provision of the IT Act.

Tampering with computer source code has been made an offense under Section 65 of the act. This provision applies to offenders who alter, conceal, or destroy computer source codes.

The maximum punishment for both hacking and tampering with computer source code is three years' imprisonment and/or a fine of up to 200,000 rupees, or both.

Breach of confidentiality and privacy
Section 72 of the IT Act deals with the penalty for breach of privacy and confidentiality. It applies to situations where a person who has gained access to any electronic record, book, register, information, document, or other material by virtue of powers conferred to him under the IT Act or related legislation makes an unauthorized disclosure of the same.

Offenses relating to digital signatures, which include misrepresentation or suppression of material facts from the Digital Signature Certificate and publishing a digital signature for fraudulent purposes, are also covered under this section.

Indian Penal Code (IPC)

IT-Related Offenses under the Indian Penal Code

The Indian Penal Code of 1860 ("IPC") is the statute governing criminal jurisprudence in India. With the enactment of the IT Act, specific provisions of the IPC dealing with offenses relating to documents and paper-based transactions were amended to include crimes conducted using electronic devices.

The amendments made to the IPC refer to the sections dealing with forgery, extortion, criminal breach of trust, criminal intimidation, and cheating.

Forgery
The offense of forgery is covered by Section 463 of the IPC. It is defined as an act of creating false documents or electronic records for the purpose of causing damage or injury to the public or any person, or to commit fraud. A "forged document or electronic record" is defined under Section 470 as a document or electronic record that is false and has been forged either entirely or in part. The general offense of forgery is further classified into a range of individual offenses. These include forgery for the purpose of cheating or defaming another party; making, using, or possessing forged documents; and counterfeiting authentication marks and designs.

Extortion
Such an offense would involve a person dishonestly inducing another to deliver any property or valuable security by intentionally putting fear of injury in

that person's mind. This offense is dealt with by the IPC under Section 383. When such crimes are committed electronically, they would be included within the purview of this section as well. Web-jacking and threatening e-mails are examples of extortion committed by an electronic medium.

Criminal breach of trust

Section 405 of the IPC defines "criminal breach of trust" as any act whereby a person who has been entrusted with property, or with any power over any property, dishonestly misappropriates the property, makes wrongful use of the property, dishonestly disposes of that property, or induces any other person to do so.

Criminal intimidation

When a person threatens another or someone in whom such other person is interested with injury to their physical well-being, reputation, or property and causes them to commit or desist from actions against their free will in order to avoid the execution of such threats, this constitutes criminal intimidation. When such threats or intimidation occur through e-mails or other electronic means of communication, they are punishable under Section 503 of the Indian Penal Code. Threats of denial-of-service attacks, e-mail bombing, virus attacks, cyber-stalking. etc. can be used to intimidate a person and amount to criminal intimidation.

Cheating

Section 420 of the Indian Penal Code deals with cheating cases. Under the section, whoever cheats and consequently dishonestly induces a person to deliver any property (to any other person), or to alter or destroy the whole or any part of a valuable security, shall be punished. When cheating is committed with the use of a computer, as in the case of credit card fraud, money-laundering, or e-mail spoofing, it is punishable under the IPC.

Further Issues

Data Protection

The only provision of the IT Act that currently addresses the issues of data protection and confidentiality is Section 72. To address the issue of misuse of personal information and data, India is currently in the process of reviewing the various clauses of the IT Act. In the absence of a specific law on data protection, appropriate principles, safeguards, and liquidated damages for breach would need to be built into a contract between relevant parties to ensure adequate remedies for data protection.

The Indian Contract Act of 1872 ("Contract Act") codifies the way one enters into a contract, the execution of a contract, the implementation of its provisions, and the effects of breach of such contract. Contracts are one of the best ways for foreign firms to protect their data and intellectual property while subcontracting work to India. The Indian Contract Act provides adequate safeguards to foreign companies, provided that both firms (Indian and foreign) agree to the contract. The companies subcontracting their work to India need to enter an exhaustive Service Level Agreement (SLA) with their vendor that covers various aspects of data security and confidentiality. This will help companies to safeguard against any fraud or misconduct.

Copyright

The Indian Copyright Act of 1957 was amended in 1994–1995 to include penalties for any person who knowingly makes use of an illegal copy of a computer program. Such an act is punishable with a minimum imprisonment of seven days, although a sentence of up to three years can be imposed. The act further provides for fines of 50,000 to 2,000,000 rupees, a jail term up to three years, or both.

Italy

Critical Sectors

ICT plays an important role in a number of critical sectors in Italian society.[273] In the ongoing effort towards an official definition of critical sectors, the following sectors are taken into consideration:[274]

- Banking and Finance,
- Public Safety and Order,
- (Tele-) Communication,
- Emergency Services,

* The Country Survey of Italy 2006 was reviewed by Roberto Setola, Working Group for Critical Information Infrastructure Protection; Paolo Donzelli, Prime Minister's Office - Dept. for Innovation and Technologies, and Tommaso Palumbo, Postal and Communication Police.

273 Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate. Protezione delle Infrastrutture Critiche Informatizzate – La realtà Italiana (October 2003); and Ministero per l'innovazione e le tecnologie. Le politiche governative in tema sicurezza.

274 Information provided by the Italian experts involved.

- Energy Production, Transportation, and Distribution,
- Natural Gas and Oil Production, Transportation, and Distribution,
- Public Administration,
- Health Care Systems,
- Transportation and Logistics (Air, Rail, Marine, Surface),
- Water (Drinking Water, Waste Water Management).

Past and Present Initiatives and Policies

Action Plan for e-Government

The Italian government intends to reform the public administration to meet user needs, to provide modern services, and to create public value. The necessary steps are outlined in detail in the e-Government Action Plan of June 2000.[276] One crucial step is the establishment of a model for e-government. It must be based on a modern infrastructure that will ensure the efficient and secure provision of a number of basic functions. To achieve this goal, the Ministry for Innovation and Technologies has developed the following strategic reference points for e-government:

- Service Provision,
- Digital Identification,
- Access Channels,
- Service Provision Agencies,
- Interoperability and Cooperation,
- Communication and Infrastructure.

In April 2003, the document on "E-Government for Efficient Federalism" was released. It defined rules for secure use of e-government services and included the "Decree on the National Plan" for the adoption of ICT security standards.[277] Approved on 30 October 2003, this decree authorizes ISCOM to certify the security of ICT products supplied to government offices by Italian firms.[278]

276 http://www.innovazione.gov.it/eng/egovernment/index.shtml.
277 http://www.innovazione.gov.it.
278 http://www.innovazione.gov.it/eng/egovernment/infrastrutture/sicurezza_privacy.shtml.

The Government's Guidelines for the Development of the Information Society

On 28 May 2002, the Committee of Ministers for the Information Society welcomed the "Government Guidelines for the Development of the Information Society" published by the Ministry of Innovation and Technologies.[279] This document stated the Italian government's commitment to making Italy a leader in the digital age, stressed its dedication to modernizing the country through the widespread use of new ICT in both the public and private sectors, and vowed to boost the country's competitiveness by accelerating e-business and e-government.[280] The "Government Guidelines" also deal with network security and introduce a national plan for ICT security and privacy. The aim of this security model is to increase network security; in particular, it aims to create trust and to convince consumers and businesses to use the internet, especially in their dealings with government. The national plan is based on the following principal actions:

- The introduction of an ICT Security Directive (to define the basic minimum of security that all government departments must achieve);
- The establishment of a National Technical Committee for ICT Security (to co-ordinate all activities);
- The establishment of an organizational model for ICT security (to include guidelines, recommendations, standards, and certification procedures);
- The specification of the activities, areas of responsibility, and deadlines for the introduction of necessary standards and methods for security certification in government;
- The final certification of ICT security for the public administration within five years.[281]

279 Minister for Innovation and Technologies, Government Guidelines for the Development of the Information Society (June 2002). http://www.innovazione.gov.it.

280 Ibid., p. 19f.

281 Ibid., pp. 65–6.

Report on Critical Information Infrastructure Protection: The Case of Italy

The Working Group on Critical Information Infrastructure, established as part of the Prime Minister's Office in 2003 to address CIIP, released the report "Protezione delle Infrastrutture Critiche Informatizzate — La realtà Italiana" ("Critical Information Infrastructures Protection: The Case of Italy") in March 2004, offering a synthesis of its efforts. The document describes many elements of the Italian infrastructures, emphasizes their interdependencies, and suggests CIIP policy strategies. In particular, the Working Group suggests that full responsibility for the correct implementation of a survivability policy should remain with the individual owners and operators of critical infrastructure, while the government should be responsible for the definition of an overall policy to minimize interdependencies and cascading failures.

Organizational Overview

Public Agencies

There is no central unit in Italy devoted to defining CIP and CIIP policies and strategies: Various activities are assigned to ministries and public bodies in charge of the different critical sectors, as well as those responsible for public safety and security. In addition, a variety of coordination efforts have been undertaken:

- In order to create an inter-sector forum and to improve awareness on CIIP, a Working Group on Critical Information Infrastructure Protection was set up in March 2003 at the Department for Innovation and Technologies of the Presidency of the Council of Ministers. All ministries involved in the management of critical infrastructures are represented in the group, together with many Italian infrastructure operators and owners as well as various research institutes. The main goal of the Working Group is to help the Italian government to come to a better understanding of the problems associated with CIIP, and to provide a basis for the identification of organizational requirements

and initiatives that could increase the robustness of critical infrastructures.

- In July 2005, to better coordinate activities and improve the protection of CII with respect to cyber-attacks, the Postal and Communications Police was identified as the unit responsible for law enforcement initiatives, and a center for CIIP was created. This center has the specific goals to prevent, and investigate malicious activities in cyberspace against critical information infrastructures. To this end, in collaboration with the different stakeholders and operators of critical infrastructures, the center defines specific operational protocols to improve information-sharing and behavioral rules to adopt before, during, and after any cyber-attack to facilitate and support investigations.
- The Ministry of Communication, within the Istituto Superiore delle Comunicazioni e delle tecnologie dell'informazione (ISCOM), has established a specific working group to analyze the responsibilities and security requirements that CIIP imposes on communication infrastructure operators, and to analyze the dependencies of the latter on other critical infrastructures.

Besides the Working Group on Critical Information Infrastructures Protection, the main Italian government bodies dealing with CIIP are the Ministry of Innovation and Technologies, the Ministry of Communication, and the Ministry of the Interior (Postal and Communications Police).

Ministry for Innovation and Technologies (MIT)

The Ministry for Innovation and Technologies[282] has been delegated to act on behalf of the prime minister in the areas of technological innovation, the development of the information society, and related innovations for government, citizens, and businesses. This ministry has particular responsibility for network structures, technologies and services, the development and use of information and communication technologies, and the fostering of IT and digital awareness and literacy, including through links with international and EU bodies that are active in the sector. The MIT has also been delegated to chair the Committee of Ministers for the Information Society and the Committee of Ministers for Joint Satellite Navigation Initiatives.

282 http://www.innovazione.gov.it/eng/index.shtml.

The Department for Innovation and Technologies (DIT) is the department of the Presidency of the Council of Ministers that provides support to the minister of innovation and technologies. It serves to coordinate ministerial policies for the development of the information society and to promote innovation in public offices and among citizens and businesses.[283]

National Technical Committee for ICT Security in the Public Administration

On 16 October 2002, the Ministry for Innovation and Technologies and the Ministry of Communication created the National Technical Committee for ICT Security in the Public Administration. The establishment of this new committee followed from the Directive on ICT Security for the Public Administration, which enacts EU recommendations with the important initial aim of achieving compliance with a set of minimum-security standards. The Technical Committee can therefore be seen as the operative arm of the new national IT security policy.[284] It was constituted in July 2002 with support from the Ministry for Innovation and Technologies and the Ministry for Communications.[285]

The committee aims to attain a satisfactory security level in information systems and digital communications, in compliance with international standards, in order to guarantee the integrity and reliability of the information. It prepares strategy proposals concerning computer and telecommunications security for the public administration. In particular, it develops:

The "National Emergency Plan for the security of information and communication technologies in the public administration". The committee annually verifies its state of progress, and proposes corrective measures if required;

The ICT security national organizational model for the public administration. The committee monitors its level of activation and application.

Furthermore, the committee formulates proposals for regulating certification and security assessment, as well as certification criteria and guidelines

283 http://www.innovazione.gov.it/eng/intervento/pol_soc_eng.shtml.

284 http://www.innovazione.gov.it/eng/comunicati/2002_10_11.shtml.

285 Minister for Innovation and Technologies. Government Guidelines for the Development of the Information Society (13 February 2002). http://www.innovazione.gov.it/eng/intervento/allegati/docu_base130202.pdf.

for ICT security certification in the public administration, on the basis of national, sectoral, and international norms of reference.

Finally, the committee elaborates guidelines for agreements with the Ministry of Public Administration for training public employees in ICT security. Among other proposals, the group is to set up the Computer Emergency Response Team (CERT) for the Public Central Administration (CERT-PA, now GovCERT.it, which has also assumed the role of coordinating the CERTs of the other parts of the public administration). It will have a central Early-Warning System operating around the clock.

In March 2004, the National Technical Committee on ICT Security published a preliminary proposal for the National Security Plan and an organizational model. Guidelines were suggested for building an organizational infrastructure to coordinate and support public offices at the national level, and the most urgent areas of action to put the process on track were identified.[286]

National Center for Informatics in the Public Administration (CNIPA)

The Authority for IT in the Public Administration (AIPA), founded in 1993, was transformed into the National Center for Informatics in the Public Administration (CNIPA) in 2003.[287] CNIPA is supervised by the Ministry of Innovation and Technologies, and its head is nominated by the Council of Ministries. It addresses central and local administrations, especially the elements responsible for IT systems in the public administration. CNIPA's main task is to promote modern information technologies in the Italian public administration, to establish standards and methods, to deal with security issues, and to make recommendations and technical regulations in the field of IT for public administration.[288] CNIPA published a comprehensive guide on the protection of personal data in 2001.

286 http://www.innovazione.gov.it/eng/egovernment/infrastrutture/sicurezza_privacy.shtml.
287 http://www.cnipa.gov.it.
288 http://www.cnipa.gov.it.

Ministry of Communication

The Ministry of Communication supervises postal and telecommunications services, acting as a regulator as well as practicing a policy of coordination, supervision, and control.[289] It is involved in the definition of security policies for communication and the internet.

Institute for Information and Communication Technologies (ISCOM)

ISCOM's[290] main activity is specifically to address ICT companies, government agencies, and private users. It essentially focuses on legislation, experimental activities, fundamental and applied research, specialized training, and education in the TLC field.

ISCOM also manages the National Information Security Certification Body (OCSI),[291] which is devoted to security certification of systems and products in the ICT field. OCSI acts in the framework of the European ITSEC criteria and relevant ITSEM methodologies, and in accordance with the international ISO/IEC IS 15408 (Common Criteria) standard.
Moreover, ISCOM is actively involved in creating a public-private forum for addressing security problems related to (tele-) communication networks. In 2004, ISCOM established a working group in this framework to analyze the different aspects of security in communication networks and the security requirements required in communication networks to guarantee an adequate level of services for critical infrastructures. To this end, ISCOM in March 2005 released guidelines that address some topics related to the security and quality of services in communication networks. One of these was specifically devoted to the issue of security for CIIP.[292]

289 http://www.comunicazioni.it/en/index.php?Mn1=5.
290 Istituto Superiore delle Comunicazioni e delle Tecnologie Informatiche. http://www.iscom.gov.it.
291 Organismo di Certificazione della Sicurezza Informatica. http://www.ocsi.gov.it.
292 http://www.iscom.gov.it/news04.htm.

Permanent Working Group on Network Security and Communications Protection

The Ministries of Communication, the Interior, and Justice established the Permanent Working Group on Network Security and Communications Protection in 1998 with a focus on criminal, legal, and economical aspects of communication services, such as the duration for which a provider should store communication data. Within this group, the Subgroup Internet deals with investigative and judicial matters related to the internet. This subgroup is preparing a list of data that internet service providers will have to supply to the police if ordered by a judge. A similar list already exists for telephone companies. A coordination center was recently constituted to coordinate crime-fighting within governmental institutions.[293]

Postal and Communications Police

In 1992, the Ministry of the Interior issued a directive assigning to the state police specific responsibilities for IT and telecommunications security that are in fact carried out by the Postal and Communications Police. The Postal and Communications Police is a flexible organization with a staff of around 2,000 highly trained officers, and placed at the peak of a structure involving 19 regional departments and 76 territorial sections. The Postal and Communications Police reviews communications regulations, studies new technical investigative strategies to fight computer crime, and coordinates operations and investigations for other offices. This police force also collaborates with other institutions — in particular with the Ministry of Communication and the Privacy Authority — and with private operators who deal with communications. As the Italian contact point for G8 computer crime offices, it is available at all times. This particular organizational aspect guarantees a quick, qualified, and efficient response[294] in the event of a threat or computer attack originating nationally or internationally.

The Postal and Communication Police Service also hosts and manages an emergency center at both the national and regional levels, in order to better deal with computer crimes against critical infrastructure and to conduct pre-

293 Information provided by Italian expert involved.
294 http://www.poliziadistato.it/pds/english/specialist.htm.

ventive monitoring activities on a technical and operational level. The center will be a focal point for the evaluation of threats, thus providing adequate countermeasures to face such situations.

Early Warning and Public Outreach

A number of CERTs (Computer Emergency Response Teams) are currently active in Italy. They are all devoted to the development of IT security, and to supporting organizations in increasing their level of security with respect to cyber-threats.

CERT-IT: The Italian Computer Emergency Response Team[295] was founded in 1994 as a non-profit organization. It is mainly supported by the Department of Informatics and Communications (DICO) at the University of Milan. CERT-IT is a member of the Forum of Incident Response and Security Teams (FIRST). It promotes research and development activities in security systems, provides information about computer security, and has an expertise team for handling computer incidents.[296] CERT-IT has also developed an electronic forum in order to disseminate all information related to vulnerabilities in a broad and timely fashion.[297]

GovCERT.it:[298] This initiative was planned by the National Technical Committee on Computer and Telecommunications Security to help public administrations to improve their level of ICT security by providing an early-warning service on cyber-threats.

GARR-CERT:[299] The GARR Network Computer Emergency Response Team assists the users of the GARR Network (the Italian Academic and Research Network) in implementing proactive measures to reduce the risk of computer security incidents and in responding to such incidents when they occur.

295 http://security.dsi.unimi.it.
296 http://idea.sec.dsi.unimi.it/index.html.
297 Dependability Development Support Initiative (DDSI). European Dependability Policy Environments, Country Report Italy (2002).
298 http://www.cnipa.gov.it/site/it-IT/Attivit%C3%A0/Servizi_per_la_PA/Govcert.it.
299 http://www.cert.garr.it.

MoD-CERT:[300] The CERT of the Ministry of Defense assists its users in protecting ICT networks and disseminates information about ICT security.

The Ministry of the Interior, together with the Postal and Communication Police, is also active in early-warning activities. These agencies continuously monitor cyberspace to discover criminal or malicious behavior in order to provide adequate countermeasures. Moreover, specific protocols have been established to prevent incidents and to manage and share information as well as criminal evidence.

Law and Legislation

Italy has specific laws and ministerial decrees devoted to CIP and CIIP.[301] In the early 1990s, a new law related to computer crimes was introduced (**Law 547** of 23 December 1993) that gave more power to investigators in the evidence-collection phase and allowed computer and telecommunication intercepts. Italy was one of the first European countries to adopt such legislation, mainly due to the incidence of new crimes in the areas of computer fraud, forgery, data corruption, computer misuse, unauthorized interceptions of computer communications, and sabotage. The great attention given to such crimes is underscored by the fact that computer intrusions are treated as domestic property violations.

The innovative concept of "High-Tech Crime", which had already enjoyed currency in the Italian penal legislation for different types of offenses, was introduced with Law 547. According to Article 420 of the Italian Penal Code (attempt to damage public utilities systems), actual damage or destruction to the systems are not required for such activities to constitute an offense; the mere intention suffices. Such cases will be prosecuted even if the attempt was unsuccessful.

Other relevant laws include:

- Legislative Decree 518, enacted on 29 December 1992 and modified by **Law 248** (18 August 2000), a legislative decree against illicit ICT piracy;

300 http://www.difesa.it/CaSMD/SMD/Reparti/II-reparto/CERT.

301 Information supplied by Roberto Setola, secretary of the Working Group on Critical Infrastructure Protection coordinated by the Cabinet Office of the Italian government.

- **Law 547**, enacted on 23 December 1993, a comprehensive and integrated law against ICT crimes;
- **Law 675**, enacted on 31 December 1996, a law governing personal data protection, integrated by subsequent legislation (DPR 318/1999, Law 325/2000, Legislative Decree 467/2001, and Legislative Decree 196/2003);
- Legislative Decree 374/2001, changed into **Law 438/2001**, a law devoted to better law-enforcement instruments and the repression of terrorism.

Note that Law 374/2001, transformed into Law 438/2001 after 11 September 2001, has updated the Penal Code, so that now, crimes committed in Italy are liable to prosecution even if they are directed against a foreign state or against a multilateral institution.

Privacy Law

Part of Article 15 of **Law 675/96**[302] (the Privacy Law) deals with the organizational issues that the use of IT systems raises. By establishing a duty to store data in a way that minimizes the risk of loss and prevents unauthorized access (including access inconsistent with the reasons given for the original acquisition and processing of such data), Article 15 requires data holders to update their security to keep up with technical advances and changes in the methods of infiltration.

Consequently, not only should the minimum measures established by Presidential Decree 318/99 be strictly implemented and observed, but all appropriate additional measures should also be taken and regularly updated to match technical progress.

A New Privacy Code, which contains specific requirements for the protection of personal data online, has been in force since July 2003.[303]

302 http://www.innovazione.gov.it/ita/privacy/legge675_96.rtf.
303 http://www.innovazione.gov.it/eng/egovernment/infrastrutture/sicurezza_privacy.shtml.

Italian Penal Code

Penal Code Article 615 ter: Unauthorized Access to Computers or Telecommunication Systems:

Anyone who enters unauthorized into a computer or telecommunication system protected by security measures, or remains in it against the expressed or implied will of the authority that has the right to exclude him, shall be sentenced to imprisonment not exceeding three years.
The imprisonment is from one until five years:

> 1) if the crime is committed by a public official or by an officer of a public service, through abuse of power or through violation of the duties concerning the function or the service, or by a person who practices – even without a license — the profession of a private investigator, or by abusing the authority of a system operator;
> 2) if, to commit the crime, the culprit uses violence against things or people, or if he is manifestly armed;
> 3) if the deed causes the destruction or the damage of the system or the partial or total interruption of its working, or the destruction or damage of the data, information, or programs contained in it.

If the crimes listed in the first and second paragraphs concern computer or telecommunication systems of military interest, or public order or public security, or civil defense, or any public interest whatsoever, the penalty is one to five years and three to eight years of imprisonment, respectively. In the case provided for in the first paragraph, the crime is only liable to prosecution after an action by the plaintiff; the other cases are prosecuted ex officio.

Penal Code Article 615 quater: Illegal Possession and Diffusion of Access Codes to Computer or Telecommunication Systems:

Whoever, in order to obtain a profit for himself or for another or to cause damage to others, illegally gets hold of, reproduces, propagates, transmits, or delivers codes, key-words, or other means for accessing a computer or telecommunication system protected by safety measures, or whoever provides information or instructions for the above purpose, will be punished by imprisonment not exceeding one year and a fine.

Penal Code Article 615 quinquies: Diffusion of Programs Intended to Damage or to Disrupt a Computer System:

Whoever propagates, transmits, or delivers a computer program — written by themselves or by another party — with the aim and the effect of damaging a computer or telecommunication system, the data or the programs contained therein or pertinent to it, or achieving the partial or total interruption or an alteration in its working, will be punished by imprisonment not exceeding two years and a fine.[304]

304 http://www.cybercrimelaw.net/countries/italy.html.

Japan

Critical Sectors

Information systems in critical infrastructures such as power supply, transportation, and electronic control play a crucial role in maintaining public safety and stable supplies of indispensable services. The following sectors are considered to have the largest impact on Japan's everyday life and welfare:

- (Tele) Communication[305],
- Government and Administrative Services[306],
- Finance[307],

* The Country Survey of Japan 2006 was reviewed by Mika Shimizu, Osaka School of International Public Policy, and by Japanese experts from the Ministry of Internal Affairs and Communication (MIC), the Ministry of Foreign Affairs (MOFA), the National Police Agency (NPA), the Cabinet Secretariat, and the Ministry of Economy, Trade and Industry (METI).

305 Responsible: Ministry of Internal Affairs and Communications (MIC).

306 Ibid.

307 Responsible: Financial Services Agency (FSA).

- Transport by Aviation and Railway[308],
- Distribution, Logistics[309],
- Electrical Power[310],
- Gas[311],
- Medical Services[312],
- Water.[313]

Past and Present Initiatives and Policies

The government of Japan, based on the "Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society" of 1998,[314] has been steadily promoting policies contributing to the advancement of information technology and telecommunications in Japan.[315]

In 2003, the Ministry of Economy, Trade, and Industry (METI) released a "Comprehensive Strategy on Information Security". This document considered the new ICT-related risks and threats confronting the Japanese society from a national-security perspective: "The issue of information security should not be only pursued for the safety of 'economic activities' but is an issue that requires scrutiny on the national level for Japan's own national security."[316] The overall aim of this strategy is to develop a "highly reliable society", including greater economic competitiveness for Japan as well as improving its overall security by preventing cyber-terrorism and securing stable energy and food supply.[317]

308 Responsible: Ministry of Land, Infrastructure and Transport (MLIT).
309 Ibid.
310 Responsible: Ministry of Economy, Trade and Industry (METI).
311 Ibid.
312 Responsible: Ministry of Health, Labor and Welfare (MHLW).
313 Ibid.; Information Security Policy Council (ISPC). Action Plan on Critical Infrastructure (13 December 2005). Information provided by Japanese expert involved.
314 Decision of the Advanced Information and Telecommunications Society Promotion Headquarters (9 November 1998).
315 Outline of the First Follow-up of the Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society (19 May 2000) (provisional translation). http://www.kantei.go.jp/foreign/it/2000/0706outline.html.
316 Comprehensive Strategy on Information Security: Executive Summary. Chapter 1.2 New Dimensions of Risks Confronting Society as a Whole (no date). http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf.
317 Ibid.

Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure

In 2000, the Cabinet Secretariat released a "Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure",[318] which was replaced in December 2005 by the "Action Plan on Critical Infrastructure". The former plan has the aim of protecting critical infrastructures from attacks by cyber-terrorists. The government – in close cooperation with the private sector – aims to enhance the voluntary, independent participation of businesses as well as the regional public organizations involved with critical infrastructures. The plan includes the following preventive measures by government and the private sector:

- To prevent damage by raising security levels;
- To establish and enhance communication and coordination systems between government and the private sector, especially critical infrastructure groups;
- Detection and emergency response to cyber-attacks through cooperation between government and the private sector;
- To establish foundations of information security, including personal training, research and development, and appropriate laws and regulations;
- International cooperation.[319]

e-Japan Priority Policy Program and e-Japan Strategy II

The aim of the "e-Japan Priority Policy Program", initiated by the prime minister of Japan in 2001, is to create a "knowledge-emergent society" where everyone can utilize IT and its benefits, and to make Japan the world's most advanced IT nation within five years. Priority policy areas include the establishment

318 Special Action Plan on Countermeasures to Cyber-terrorism of critical infrastructure (15 December 2000) (provisional translation). http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN009986.pdf, and Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure (Summary) (provisional translation; no date). http://www.kantei.go.jp/foreign/it/security/2001/cyber_terror_sum.html.

319 http://www.kantei.go.jp/foreign/index-e.html; and http://www.bits.go.jp/active/general/kijun01.html.

of the ultra-high-speed network infrastructure and competition policies, the facilitation of e-commerce, the realization of e-government, and the promotion of education and human resources development relating to it.

A special section of the policy program deals with ensuring the security and reliability of advanced information and telecommunications networks. The aim is to eliminate threats to continued service provision that arise from inadequate IT security, including unauthorized access, computer viruses, and denial-of-service (DOS) attacks against ICT, in particular regarding those elements of e-government, e-commerce, critical infrastructures, etc. that may have a great influence upon the everyday life of the Japanese people and their socioeconomic activities.

Yet the approach is much broader: At the same time, due consideration is to be given to international collaboration, maintenance of public order, disaster prevention, and national security. Priority policies also include the preparation of regulatory frameworks, the establishment of IT security measures within the government, the protection of personal information, the raising of public awareness in the private sector, research and development on IT security, and the further education of staff in charge of IT security.[320]

The follow up e-Japan Strategy II was introduced on 2 July 2003, at the 19th meeting of the IT Strategic Headquarters, which was attended by all ministers and private-sector experts.[321] It focuses on the users of IT and the promotion of collaboration between government ministries and agencies. Among other topics, the e-Japan Strategy II deals with international IT strategies in Asia, security measures, IT regulatory reforms, and the promotion of e-government.[322]

Comprehensive Strategy on Information Security

The Information Security Committee established under the Industrial Structure Council (METI's advisory council) began discussions in June 2003 on realizing a "Highly Reliable Society". As a result, it released the "Comprehensive Strategy

320 e-Japan Priority Policy Program: http://www.kantei.go.jp/foreign/it/network/priority-all/7.html.
321 The 19th Meeting of the IT Strategic Headquarters, Wednesday, 2 July 2003. http://www.kantei.go.jp/foreign/koizumiphoto/2003/07/02it_e.html.
322 http://www.kantei.go.jp/foreign/policy/it/040318senryaku_e.pdf.

on Information Security"[323] on 10 October 2003. The aim of the strategy is to realize a highly reliable society in Japan. The strategy paper explains that this is necessary because hitherto, measures to assure information security have been issue-specific and only aimed at resolving the problem at hand, such as measures implemented by business enterprises and private individuals, as well as by the Japanese government. Since the measures adopted so far have been tailored to individual requirements, a more comprehensive approach is required. Moreover, the strategy paper explains that, based on the assumption that "information security is never guaranteed and accidents happen […] rather than developing measures for each specific issue, studies must be conducted to develop measures for the development of a 'self-recoverable' social system prepared for accident/incident occurrences".[324]

Action Plan on Critical Infrastructure Information Security Measures

On 13 December 2005, the Information Security Policy Council (ISPC) published an "Action Plan on Critical Infrastructure Information Security Measures"325 that replaced the "Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure". The new plan includes definitions of critical infrastructure elements and threats, safety standards for information security, information-sharing systems in public-private partnerships (PPP), interdependency analyses, and exercises. The plan emphasizes the importance of PPPs and aims to establish within each critical sector capabilities for protection, technical operation, analysis, and response by the end of 2006. Moreover, the plan contains uniform standards for government information security measures. The plan will be reviewed in three years.[326]

323 http://www.meti.go.jp/english/policy/index_information_policy.html.

324 Comprehensive Strategy on Information Security (Summary), p. 2 http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf.

325 Provisional translation.

Organizational Overview

Public Agencies

Within the Japanese government, the IT Strategic Headquarters as part of the Cabinet Secretariat plays an important role in the field of CIIP and is the main actor for central government policy issues. From July 2004 to May 2005, an Interim Committee for Essential Issues on Information Security[327] was set up to focus on information-security policies more comprehensively by collecting expert opinions and forwarding these to the IT Strategy Headquarters.[328] The committee proposed the establishment of the National Information Security Center (NISC) and the Information Security Policy Council (ISPC), both of which became operational in 2005. NISC is subordinate to the Cabinet Secretariat, and ISPC is part of the IT Strategic Headquarters. For the time being, these two organizations are the focus of CIIP policies in Japan. However, as these organizations were only established recently, many policies are still under development.[329]

In addition, the Ministry of Economy, Trade and Industry (METI), the National Police Agency (NPA), and the Ministry of Internal Affairs and Communications (MIC) assist the Cabinet Secretariat and play major roles in the field of CIIP.

326 Information provided by a Japanese expert involved. So far, the plan is only available in Japanese.

327 Joho-Sekyuriti-Kihon-Mondai Iinkai.

328 Shimizu, Mika. Governance for a New Security Issue: Cyber Security in Critical Infrastructure Protection. Prepared for the 2004 Annual Meeting of the American Political Science Association (2 – 5 September 2004); and Yoshida, Mabito. "Information Security Policies in Japan". Presentation held at the ITU WSIS Thematic Meeting on Cybersecurity (Geneva, 28 June – 1 July 2005). http://www.itu.int/osg/spu/cybersecurity/presentations/session7_yoshida.pdf.

329 An IT Security Office was established within the Cabinet Secretariat in February 2000, following increasing public attention on IT security incidents, such as unauthorized access and dissemination of computer viruses. The IT Security Office undertook efforts to secure both public and private information systems, such as making government electronic systems safe or protecting the critical infrastructure, in close cooperation with the responsible departments and the public and private specialists. The office coordinated important policies of ministries and agencies. The roles of the IT Security Office were taken over by the National Information Security Center (NISC) and the Information Security Policy Council (ISPC). http://www.bits.go.jp/en.

IT Strategic Headquarters

In July 2000 the IT Strategy Council, consisting of 20 opinion leaders, was established in order to study the issue of making Japan an internationally competitive IT nation, and by combining private-public partnerships.[330] In January 2001, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) was launched under the provisions of the Basic Law on the Formation of an Advanced Information and Telecommunications Network Society (IT Basic Law), with the prime minister as its director-general, and including all cabinet members and opinion leaders from the private sector as members, to serve as a new base for joint government and private-sector promotion of IT policies.[331]

The National Information Security Center (NISC)

The National Information Security Center (NISC) was launched in April 2005 with about 35 staff (to be increased to 60 in 2006) as Japan's central entity dealing with IT security issues. It is part of the Cabinet Secretariat and pursues the following tasks:

- Planning government-wide fundamental strategies for information security policy;
- Promoting comprehensive measures on information security concerning government organizations;
- Supporting these government organizations in an appropriate way when information security incidents occur;
- Strengthening the information security of critical infrastructures;[332]
- Reinforcing information-sharing systems;
- Implementing cross-sector cyberspace exercises;
- Creating an international strategy and promoting relationships with other countries.

330 E-Japan Priority Policy Program: http://www.kantei.go.jp/foreign/it/network/priority-all/1.html.
331 IT Strategic Headquarters. e-Japan 2002 Program: Basic Guidelines Concerning the IT Priority Policies in FY2002 (26 June 2001). http://www.kantei.go.jp/foreign/it/network/0626_e.html.
332 Yoshida, op. cit..

Information Security Policy Council (ISPC)

The Information Security Policy Council (ISPC), set up in May 2005, is chaired by the chief cabinet secretary and forms part of the IT Strategic Headquarters with members from various ministries as well as private-sector experts. It has the following tasks:

- To develop a basic strategy for information security policy;
- To undertake proactive and retrospective assessments of information security policy, based on the basic strategy;
- To develop safety guidelines for information security that are uniform throughout government;
- To recommend information security policies based on the government-wide safety guidelines;

To respond efficiently to emergencies.[333]

The Critical Infrastructure Committee, established within the ISPC, issued an initial "Action Plan on Critical Infrastructure Information Security Measures" on 13 December 2005.[334]

Ministry of Economy, Trade and Industry (METI)

The Ministry of Economy, Trade and Industry (METI) is responsible for planning and implementing various information policies in the Japanese government in order to realize a new social and economic system and lifestyle by utilizing advanced information technology. Besides the promotion of the "Comprehensive Strategy on Information Security", the information policies of METI include:

- Promotion of e-commerce;
- Personal information protection, e.g. raising the awareness of both companies and consumers regarding the Personal Data Protection Law, the Japanese industrial standard JIS on the protection of personal information, and METI guidelines;

333 Yoshida, op. cit.
334 See above.

- e-Government;
- Research and development, including programs to develop fundamental technology in the fields of IT such as network systems, wireless networks systems, semiconductors, software, and displays;
- Human resource development in high-level IT: METI is implementing several policies in this area, including the promotion of IT skill standards that clarify and systematize the actual ability of IT service personnel, testing information processing technicians, and supporting IT experts who can advise managers of private companies on the strategic use of IT;
- International cooperation;
- Information security: Implementing an incident-response system, and developing evaluation systems for information security. In cooperation with the Information Technology Promotion Agency (IPA) Security Center and the Japan Computer Emergency Response Coordination Center (JPCERT/CC), METI provides information for the private sector and individuals in order to prevent incidents such as unauthorized access and computer virus attacks that affect all of society.

Since it is difficult for each private company to ascertain whether its security levels are adequate when obtaining software, cryptography, or IT services on the open market, METI has developed several information security evaluation systems that are conducted through a third party since April 2003. These systems include an information-auditing system, an information-security management system, a certification for evaluating security products, and evaluation systems for encryption technology. These standards are not only used by the government in procuring its own software and IT services, but can also be used by the private sector in the future.[335]

335 The Japan Information Processing Development Corporation (JIPDEC) developed the Information Security Management System (ISMS), a new accreditation system for all services dealing with information, based on ISO/IEC 17799, in April of 2002, replacing the Information-Processing Accreditation Scheme (IAS). http://www.meti.go.jp/english/policy/index_information_policy.html.
The Ministry of Internal Affairs and Communications (MIC) and the Ministry of Economy, Trade and Industry (METI) established the CRYPTREC Advisory Committee (chaired by Prof. IMAI Hideki, University of Tokyo) in May 2001 to promote information security measures by objectively evaluating secure cryptographic techniques. Based on the results of the evaluations, a list of recommended cryptographic techniques for e-government was compiled. http://www.meti.go.jp/english/policy/index_information_policy.html.

In the field of CIIP, METI focuses on information security measures in the electricity sector. The Federation of Electric Power Companies (FEPC) and the Central Research Institute of the Electric Power Industry (CRIEPI) will conduct virtual exercises to prevent cyber-terrorism against the electricity sector.[336]

Committee of Information Security Governance at METI

This committee was established in September 2004 with the goal of promoting information security governance within corporate management. Measures under discussion include IT security benchmarks for effective security investment by CIOs/CEOs; guidelines for business continuity plans to prevent security incidents and unauthorized access; and an appropriate format for information security reports to stakeholders.[337]

National Police Agency (NPA)

The National Police Agency[338] has long been committed to maintaining computer and network security and investigating cyber-crimes. Traditionally, it has done this via its High-Tech Crime Prevention Department. In 1999, a new program was established to help fight high-tech crime. The High-Tech Crime Technology Division (HTCTD) was set up in the Information-Communications Bureau, and a National Police Agency Technology Center was created as the technical heart of the division. In April of 2004, the National Police Agency established the HTCTD in each Prefectural Information-Communications Department in order to enhance the capacity for technological support.

Cyber Forces

Additionally, the National Police Agency is committed to creating a monitoring and emergency response service to prevent and minimize the spread of cyber-terrorism, as well as to arrest cyber-terrorists. One branch of this service are the mobile technical teams, or Cyber Forces. These technical computer-

336 Hayami, Yutaka (METI). Realizing a World-Class "Highly Reliable Society". Presentation held on 25 November 2004 (no place). http://www.aavar.org/2004web/AVAR2004/Presentations/ps011.ppt.

337 Ibid.

338 http://www.cyberpolice.go.jp/english/action01_e.html.

security teams are stationed throughout Japan, and the Cyber Force Center acts as their command center. It monitors internet security around the clock and collects and analyzes relevant information. It is also equipped with facilities for a wide range of research and development, as well as for personnel education and training.

A major interest of the Cyber Force is to strengthen cooperation between the government and civilians as well as establishing partnerships with key infrastructure providers. The Cyber Force is currently working with prefectural police agencies to request the cooperation of collective or individual service providers.[339]

The NPA provides policies for information security, contact information for the prefectural police in case of cyber-crime, and crime statistics on its homepage.[340]

Ministry of Internal Affairs and Communications (MIC)

The MIC publishes an annual "White Paper on Information and Communications in Japan".[341] In each edition, a special chapter deals with privacy protection as well as information security. The aim is to strengthen public-private partnership cooperation to ensure information security. Moreover, the MIC conducts research related to secure operating systems and to the protection of personal information in the field of ICT, and carries out measures to upgrade emergency information functions in the telecommunications area.

The 2005 whitepaper deals with ways to achieve a ubiquitous network society ("u-Japan") by 2010 that allows connection to networks anytime, anywhere, by anyone, and enables an easy exchange of information. The MIC outlined the future of such a society and summarized the necessary policies as the "u-Japan Policy", which is based on the four principles "ubiquitous", "universal", "user-oriented", and "unique". Among these, "ubiquitous" (connects everyone and everything) plays the key role.[342]

339 http://www.cyberpolice.go.jp/english/action05_e.html.

340 NPA Japan Countermeasure against Cybercrime Homepage: http://www.npa.go.jp/cyber/english/index.html.

341 http://www.johotsusintokei.soumu.go.jp/english/index.html.

342 Ministry of Internal Affairs and Communications, Information and Communications in Japan. Stirring of u-Japan. White Paper 2005. http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2005/2005-index.html.

Public-Private Partnerships

In the Japanese "Comprehensive Strategy on Information Security", it is suggested that for measures that require cooperation between the national government and private enterprises, the distribution of roles and methods of coordination should be identified clearly.[343]

Central coordination for cooperation with the private sector lies with the Cabinet Office. In addition, the MIC deals with the information and communications sector; METI with the energy sector (gas and electricity); the Financial Service Agency (FSA) with the financial sector; and the National Police Agency is in charge of cross-sector crime prevention.

Early Warning and Public Outreach

National Incident Response Team (NIRT)

The National Incident Response Team (NIRT) has been part of the IT Security Office of the Cabinet Secretariat since April 2002, and is in charge of the first response to cyber-incidents as the Japanese government CERT. Based on the "Action Plan for Ensuring e-Government's IT Security" (adopted on 10 October 2001 by the IT Security Promotion Committee), NIRT comprises 15 computer security experts from both the government and the private sector and has the following tasks:

- To handle incidents relating to IT security that require risk management by the government, such as a failure in the IT infrastructure of e-government;
- To collect and analyze information and intelligence related to incidents, and to predict the future spread of damage;
- To develop technical countermeasures for the mitigation of damage; recovery and reoccurrence prevention; analysis of countermeasures for

343 Comprehensive Strategy on Information Security (executive summary), op. cit. http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf.

incidents; and compilation of concrete remedies to be implemented by ministries and agencies;
- To assist in implementing countermeasures by providing advice to ministries and agencies and to conduct support activities in implementing countermeasures upon request.[344]

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

JPCERT/CC[345] is an independent non-profit organization acting as a national point of contact for the other Computer Security Incident Response Teams (CSIRTs) in Japan. Since its establishment in 1992, the center has been gathering information on computer incidents and vulnerabilities, issuing security alerts and advisories, and providing incident responses as well as education and training to raise awareness of security issues. JPCERT/CC coordinates with network service providers, security vendors, government agencies, and industry associations, and is a member of the Forum of Incident Response and Security Teams (FIRST).

Asia Pacific Computer Incident (Emergency) Response Team (AP-CIRT/ AP-CERT)

The aim of the Asia Pacific Security Incident Response Coordination (AP-CIRT) is to foster close collaborations among the CIRTs (Computer Incident Response Teams) in the region. In February 2003, its name was changed to Asia Pacific Computer Emergency Response Team (APCERT), and it continues to carry out its original mission. JPCERT/CC currently serves as a secretariat for APCERT.[346]

Cyber Force

The Cyber Force, a section within the police, gathers data on the internet around the clock and looks for evidence of cyber-crime. When the Cyber Force

344 http://www.bits.go.jp/en.
345 http://www.jpcert.or.jp/english.
346 http://www.apcert.org.

detects an unusual phenomenon, it provides critical infrastructure operators with security information to prevent cyber-terrorism and conducts vulnerability tests. Additionally, the Cyber Force will give operators of critical infrastructures advice on how to limit the damage from such an incident and how to recover their services safely, and to find the cause of the incident.[347]

@police

The National Police Agency has a security portal site, @police, whose purpose is to prevent cyber-terrorism incidents or keep them from spreading by quickly providing information gathered by the police on information security. Moreover, @police makes efforts to increase security awareness among internet users. Therefore, it provides a wealth of diverse content in order to help as many people as possible improve their security. Special online security courses, examples of internet crimes and how to avoid them, quick security checks, and information on security holes are provided for the benefit of private PC users as well as server administrators.[348]

Ministry of Economy, Trade and Industry (METI)

METI has responded to security breaches in cooperation with JPCERT/CC and the IPA since 1990. Around that time, it also began releasing reports on computer viruses and unauthorized access and started to gather information about damage caused by computer viruses and disseminating it to the public immediately after the incident.[349]

347 Information provided by experts from NPA.
348 http://www.cyberpolice.go.jp/english.
349 Hayami, op. cit., http://www.aavar.org/2004web/AVAR2004/Presentations/ps011.ppt.

Law and Legislation

Unauthorized Computer Access Law 1999

The Unauthorized Computer Access Law No. 128 of 1999[350] prohibits acts of unauthorized computer access (Article 3) as well as acts that facilitate unauthorized computer access (Article 4).

Article 3 includes acts such as:

- Facilitating a specific use that is restricted by an access control function, by entering via a telecommunications line another person's identification code into a specific computer that controls access.[351]
- Facilitating a specific use that is restricted by an access control function, by entering via a telecommunications line any information (excluding an identification code) or command that can evade the restrictions of that access control function for that specific purpose.
- Facilitating a specific use that is restricted by an access control function, by operating a computer whose specific use is restricted by an access control function installed on another specific computer that is connected, via a telecommunication line, to that specific computer, by entering via a telecommunications line any information or command that can evade the restriction concerned.

Article 4 makes it illegal to provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function, or to the authorized user for that identification code, while indicating that it is the identification code for a specific computer's specific use, except where such acts are conducted by the access administrator, or with the approval of that access administrator or of the authorized user.

350 Husei access kinski hou.

351 To exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code.

Moreover, the **Japanese Penal Code, Article 258**, makes it illegal to damage documents or electronic-magnetic records in public or private use.[352]

Law on Electronic Signatures and Certification Services 2000

The Law on Electronic Signatures and Certification Services No. 102 of 2000 aims to promote the diffusion of information using electronic methods and information processing by assuring easy use of electronic signatures, by establishing provisions such as the presumption of the authenticity of electro-magnetic records, the provision for accreditation with regard to designated certification services, and the prescription of other necessary matters concerning electronic signatures.[353]

Basic Law on Formation of an Advanced Information and Telecommunication Network Society 2001 (IT Basic Law)

The purpose of the IT Basic Law, which entered into force on 6 January 2001, is to promote measures for forming an advanced information and telecommunications network society where citizens can enjoy the benefits of ICT. Its measures include (Articles 16–24) the formation and expansion of advanced ICT networks; the promotion of fair competition; increasing IT user skills and development of expert human resources; reform of regulations and facilitation of e-commerce through appropriate protection; promotion of e-government and digitalization of administration; assuring security and reliability for networks and the protection of personal data; promotion of creative research and development; and international cooperation.[354]

352 http://www.cybercrimelaw.net/countries/japan.html.
353 http://www.soumu.go.jp/joho_tsusin/eng/Resources/Legislation/eSignLaw/eSignLaw.pdf.
354 http://www.kantei.go.jp/foreign/it/it_basiclaw/it_basiclaw.html.

Republic of Korea

Critical Sectors

The following sectors are counted among the critical infrastructures that are heavily dependent on information and telecommunication technologies:

- e-Government and National Government Administration,
- Emergency Services,
- National Defense,
- Media Service, e.g. Broadcasting Facilities,
- Financial Service,
- Gas and Energy, e.g. Power Plants,
- Transportation, e.g. Subways and Airports,
- Telecommunication.[355]

* The Country Survey of the Republic of Korea 2006 was reviewed by Seok-Koo Yoon, Director National Cyber Security Center (NCSC).

355 Lim, Chaeho. Creating Trust in Critical Network Infrastructures: Korean Case Study, 20 May 2002 (slides). http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.14.pdf. Cf. also Lim, Chaeho. Creating Trust in Critical Network Infrastructures: Korean Case Study, p. 4. Paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures. (Seoul, 20–22 May 2002). http://www.itu.int/osg/spu/ni/security/docs/cni.05.doc.

Past and Present Initiatives and Policies

Report on the Status of the Critical Information Infrastructure

In 2001, the Korean Information Security Agency (KISA) published a "Report on the status of the Critical Information Infrastructure". The scope of the research was:

- To provide technical consulting for critical information infrastructure management agencies to perform a risk assessment and establish safeguards;
- To evaluate the security and confidentiality of internet data centers;
- To assign information-security consultants for information infrastructure.

These efforts resulted in a model and guidelines for vulnerability analysis and assessment of critical information infrastructures, including a protection guide and protection measures; a vulnerability analysis and assessment model; a guide to risk computation; asset classification; threat classification; and vulnerability analysis. In addition, technical consulting was provided for the Ministry of Information and Communication.[356]

e-Korea Vision 2006

In April 2002, the Ministry of Information and Communication published its third master plan for Informatization Promotion for the years 2002–2006, called "e-Korea Vision 2006", in consultation with the Korean Informatization Promotion Committee.[357] "e-Korea Vision 2006" is the third master plan for informatization promotion, following the first master plan of informatization promotion devised in 1996 and "Cyber Korea 21" drawn up in 1999.[358] e-Korea

356 Korean Information Security Agency (KISA). Report on the status of the Critical Information Infrastructure, 12 January 2001. http://www.kisa.or.kr.

357 Ministry of Information and Communication. e-Korea Vision 2006. The Third Master Plan for Informatization Promotion (2002–2006) (April 2002). http://www.nca.or.kr/homepage/ehome/ehome.nsf/0/4f84e7068921413ec9256ce80024c20a/$FILE/e-Korea%20Vision%202006.pdf.

358 http://www.ipc.go.kr/ipceng/policy/vision_ground.jsp?num=1.

Vision focuses on "Ensuring Safety and Reliability of Cyberspace" to strengthen the security of the critical information infrastructures. Government policies relevant to the vision include the following:

- Identifying critical information infrastructures important for national security and economy, systematic analysis of vulnerabilities and preparation for protective plans, and establishment of cooperation between the public and private sectors in order to prevent cyber-attacks and intensify response measures;
- Reinforcement of real-time warning system to fight against hacking and viruses and strengthening international cooperation, because cyber-terrorism is intrinsically transnational;
- Developing information security technologies and training new information security experts to meet the changing needs of the information security environment;
- Devising plans to establish information ethics that enable secure cyberspace, and encouraging voluntary regulation of the private sector in terms of online information circulation.

With the designation of major information and communication facilities as critical to the national defense and the economy, the government plans to conduct a systematic analysis of their weaknesses and implement strong security measures to protect these facilities. The government has established an Information Sharing and Analysis Centre (ISAC) for each area of the government and the financial and information sectors. In addition, standards have been developed for information security technologies, together with an evaluation methodology for information security systems.[359]

Mid- to Long-Term Roadmap for Realizing a Safe u-Korea

The downside of the information revolution is seen in the growing number of cyber-attacks on the internet, infringement of private information, and spam. In the u-Korea future, which is based on the four principles "ubiquitous" (connects everyone and everything), "universal", "user-oriented", and "unique", the resulting damage would not be limited to individuals, but would affect the

359 Information provided by Korean expert involved.

whole society and its economy, and even pose a threat to the life and property of its citizens. Therefore, a new framework of information protection is required that takes the new virtual environment into account.

In May 2005, the Ministry of Information and Communication issued a report on "Mid- to Long-Term Roadmap for Information Protection" dealing with the security of high-technology infrastructures and the establishment of reliable systems for new IT services. In particular, the report presents a phased roadmap from 2005 to 2008 for the prevention of attacks on the internet, advanced response measures, reinforced protection of privacy, improvement of the legal system regarding information protection, and the training of a specialized force.[360]

Organizational Overview

Public Agencies

All governmental organizations and their subsidiary organizations are in charge of CIIP. The National Cyber Security Center (NCSC) coordinates the efforts of these departments and agencies. In the field of cyber-crime investigation and prevention, the Internet Crime Investigation Center (ICIC) under the Supreme Public Prosecutors' Office plays a central role. The Ministry of Information and Communication and the Korea Internet Security Center (KISC; KrCERT/CC) within the Korean Information Security Agency (KISA) undertake efforts to foster a culture of safe internet and telecommunication networks. The National Security Research Institute (NSRI), which is an affiliated organization of the Electronics & Telecommunications Research Institute, has the lead in developing technology and providing support to protect critical information infrastructure.

National Cyber Security Center (NCSC)

The government established the National Cyber Security Center (NCSC)[361] in February 2004 as a platform that brings together the private, public, and

360 Information provided by Korean expert involved.
361 http://www.ncsc.go.kr.

military sectors to fight cyber-threats. This is based on the understanding that cooperation among all sectors is crucial for the effective prevention of cyber-attacks as well as for the minimization of damage. The NCSC is under the wing of the National Intelligence Service (NIS) and is the central point of government for identifying, preventing, and responding to cyber-attacks and threats in Korea. NCSC performs the following tasks:

- Overall management of national cyber-security by working out plans and guidelines to improve national cyber-security systems, as well as providing support for strategic committee meetings;
- Publishing national cyber-security manuals, security guidelines, and analysis reports, and collecting, analyzing, and distributing information on cyber-threats;
- Detecting and responding to cyber-threats, issuing warnings and information on cyber-incidents, and developing cyber-security technology;
- Preventing the spread of cyber-attacks, providing support for recovery procedures, and establishing and managing pan-governmental working groups for prompt response measures;
- Promotion of cooperation among international and domestic IT security organizations;
- Education and public relations regarding cyber-security issues.

In addition, NCSC operates a 24-hour monitoring center and issues cyber-security warnings of different grades (green, blue, yellow, orange, and red), and operates information-sharing systems among the private, public, and military sectors. NCSC also publishes monthly cyber-security news to provide experts with advanced technologies and the public with knowledge of cyber-security.[362]

Internet Crime Investigation Center (ICIC)

The Supreme Public Prosecutor's Office has established the Internet Crime Investigation Center (ICIC)[363] to deal more effectively with internet-related crimes. The ICIC monitors crime trends such as hacking, the spread of viruses,

362 Information provided Korean expert involved.
363 http://www.icic.sppo.go.kr.

fraud in electronic commerce, and infringement of privacy. In doing so, it develops more effective response measures and new investigative methods to crack down on cyber-crimes. Moreover, to maximize the investigation capacity, it maintains close cooperation with international and domestic organizations. The ICIC was set up at both the Supreme Public Prosecutor's Office and the Seoul District Public Prosecutor's Office. It is operated by a high-tech crime investigation team of the Central Investigation Department and performs the following tasks:

- Intensive and systematic monitoring of cyber-crime trends;
- Collecting reports on cyber-crimes;
- Developing effective investigation methods;
- Improving the legal system in the field of cyber-crime;
- 24-hour/7-day monitoring system to respond to high-tech crime.

Korea Information Security Agency (KISA)

The Korea Information Security Agency (KISA),[364] affiliated with the Ministry of Information and Communication, was established in 1996 to create a safe, reliable information environment in Korea by reacting effectively to various acts of electronic infringement and intrusion. KISA is devoted to enhancing the security and reliability of electronic transactions by developing and supplying cryptographic algorithms. In addition, KISA has supported the development of information security in Korea through evaluations of IT-security products, IT-security education, public awareness campaigns, information security policy, and research and standardization in support of the legislative framework. In January 1998, KISA acquired membership of the Forum of Incident Response and Security Teams (FIRST).

KISA opened the Korea Certification Authority Central in 1999, and the Personal Information & Privacy Protection Center in 2000. In addition, the Korea Information Security Industry Support Center (KISIS) was established under KISA in 2001. The Korea Internet Security Center (KISC, KrCERT/CC)[365] was founded in 2003, the Korea Spam Response Center (KSRC) also

364 http://www.kisa.or.kr/index.jsp.
365 http://www.certcc.or.kr/english/vision.htm.

in 2003, and finally the Korea IT Security Evaluation Center (KISEC)[366] in 2004.[367]

In accordance with the Information Infrastructure Protection Act and the Act on Promotion of Utilization of Information and Communication Network and Data Protection, which became effective as of July 2001, KISA acquired additional duties such as the analysis and evaluation of the vulnerabilities of the critical information infrastructure, and the certification of information security management systems.

KISA includes an Information Infrastructure Protection Division with a CIIP Planning Team, a Critical Infrastructure Security Management Team, and the Korea Certification Authority Central Team, providing:

- Vulnerability analysis and assessment, including technical consulting and vulnerability analysis for facilities designated as CII;
- Security technology service for CII, including technical consulting for CII management agencies to establish safeguards and help in computer system recovery;
- Certification for information security management systems, including certifying integrated information security management systems, as well as technical and physical safeguards.[368]

National Security Research Institute (NSRI)

The National Security Research Institute (NSRI),[369] an affiliated research institute of the Electronics & Telecommunications Research Institute (ETRI),[370] is managed by the Ministry of Science and Technology.[371] NSRI contributes to the public welfare by developing technology for protecting critical information infrastructures and enables the government to exercise information sovereignty by providing national security technology and policies required to protect the country and public organizations from cyber-attack. NSRI deals with:

366 http://www.kisa.or.kr/kisae/kisec/jsp/kisec_6010.jsp.
367 Information provided by the Korean experts involved.
368 http://www.kisa.or.kr.
369 http://www.nsri.re.kr/kor/index.html.
370 http://www.etri.re.kr/www_05/e_etri.
371 http://www.most.go.kr.

- Developing technology to deal with cyber-terror and cyber-attacks, and for evaluating information protection systems, as well as to ensure the reliability and viability of governmental and military critical information infrastructures;
- Raising awareness of CIIP and giving seminars;
- Analyzing weaknesses in the government, public, and military sectors;
- Supporting Korea's e-government strategy for information protection;
- Demonstration projects in the area of information protection for governmental organizations.[372]

Telecommunication Infrastructure Protection Committee

The Telecommunication Infrastructure Protection Committee, which is chaired by the prime minister and whose members are appointed by the chiefs and chairpersons of central administrative organizations, reviews items related to critical information infrastructures. The chairperson of the Telecommunication Infrastructure Protection Committee can set up the Joint Working Group for Security Incident Response in order to provide emergency measures, technological support, and recovery procedures in the case of a large-scale security incident.[373]

Public-Private Partnerships

National Information Security Alliance (NISA)

The National Information Security Alliance (NISA)[374] was established in September 2002 to improve information security by facilitating information exchange, presenting policies, and concentrating pan-governmental efforts. The alliance consists of 22 major governmental organizations, such as the Ministry of National Defense and the Ministry of Information and Communication, as well as information security officials from 17 public enterprises, communication network providers, the Korea Information Security Industry Association,

372 Information provided by Korean expert involved.
373 Information provided by Korean expert involved; and Chaeho, op. cit., p. 4.
374 http://www.nisa.or.kr/link_2.php.

research institutes, and experts from industry and academia. One main aspect of NISA's work is the executive meeting of chairpersons of the National Information Security Alliance, the Public Enterprise Information Security Alliance, and the Industrial-Educational-Research Information Security Alliance as a way of improving cooperation, while guaranteeing the autonomy of each of these actors within the alliance.

Financial Information Security Alliance

The Financial Information Security Alliance was established in October 2002 to protect financial information security systems from cyber-terror and hacking, and to implement changes in international information protection policies such as the Banking Industry Technology Secretariat (BITS). The alliance has 87 members (20 banks, 27 security corporations, 30 insurance companies, and 10 non-bank financial institutions). The Financial Information Security Alliance develops information protection standards and policies for the financial sector, as well as assessments and certifications. It also performs research in information security, and provides education.[375]

Information Security Practice Alliance

The Information Security Practice Alliance was set up in July 2002 as a way of voluntarily increasing information protection activities in the private sector, in cooperation with various security companies and associations and with the help of the Korean Information Security Alliance (KISA). KISA has introduced a variety of projects in order to promote information protection campaigns with voluntary efforts from the public.[376]

Korea Information Security Industry Association (KISIA)

The Korea Information Security Industry Association (KISIA)[377] was established in July 1998 as a platform for nurturing the information security industry (KISA has about 110–120 members so far). Moreover, KISIA became a cor-

375 Information provided by Korean expert involved.
376 Ibid.
377 http://www.kisia.or.kr/new.

poration in 2004 in accordance with Section 2 of Article 59 of the Act on Telecommunication Network Usage Promotion and Information Protection. It proposes measures to improve the legal system relevant to information security, trains specialized forces in the field, does joint research on innovative technology, analyzes market trends to understand the status of information security industry and to make plans, solves IT problems of the industry, reflects the opinions of members on governmental policies, promptly shares information with related authorities through an integrated system, provides support for participating in information security seminars or expositions, and promotes joint research with governmental or other related organizations.

Early Warning and Public Outreach

National Cyber Security Center (NCSC)

The National Cyber Security Center (NCSC) takes preventive measures against cyber-threats. It also analyzes collected information on IT security, traffic, and capacity, using the service networks of 150 organizations, including government high-speed networks. Moreover, NCSC issues color-coded cyber-threat warnings (green, blue, yellow, orange, and red) should more damage be expected. It also distributes various security guidelines and information on worms and viruses, security news, cyber-incidents, and security technology to the private, public, and military sectors. Furthermore, if a cyber-incident takes place, NCSC staff are dispatched to the site to investigate its cause and swiftly restore the system. The NCSC staff also examines the security of the system to prevent similar incidents in advance. Besides, the security center has organized a response team alliance dealing with national cyber-attacks, and is installing an emergency contact system for affected organizations.[378]

Korea Internet Security Center (KISC, KrCERT/CC)

The Korean Internet Security Center (KISC, also called the Korea Computer Emergency Response Team Coordination Center, or KrCERT/CC), established

378 Information provided by Korean expert involved.

in 2003, aims at raising the technical capability for the protection of critical network infrastructure in order to create a safe internet and communication network. KISC develops effective countermeasures against hacking and viruses, such as cyber-attack countermeasure methodology and attack tools. KISC is organized in five major teams:

- Incident Analysis Team,
- Response Coordination Team,
- Hacking Response Team,
- Spam Response Team,
- Network Monitoring Team.

KISC responds to threats against the IT networks and has built cooperation systems with relevant organizations in order to immediately handle incidents. As a member of FIRST, KISC does its utmost to fulfill its duties in cooperation with international organizations. The tasks of KISC (KrCERT/CC) are as follows:

- Technological support to prevent cyber-incidents;
- Analysis of cyber-incidents, analysis of malicious codes and their destructive power, and development of response and recovery measures;
- Analysis of network traffic and the status of the internet, monitoring of vulnerabilities at the national and the international levels;
- Analysis of the latest hacking tools and development of response measures;
- Receiving reports on spam, making improvements in the legal system, and analyzing domestic as well as international trends;
- Reinforcing cooperation with international CERTs;
- Dealing with phishing, activating CERTs, and raising awareness in the private sector.[379]

379 http://www.certcc.or.kr/english/vision.htm.

Information Sharing and Analysis Centrer (ISAC)

The Information Sharing and Analysis Center (ISAC) prevents and detects cyber-attacks on critical information infrastructures by collecting information on cyber-incidents taking place within similar businesses or areas and by promptly reporting the data to the authorities concerned. This organization began to operate after regulations were enacted according to Article 16 of the National Information Infrastructure Protection Act. The aim is to protect critical information infrastructure in the financial and telecommunication sectors; to provide information on vulnerabilities, causes of cyber-incidents, and response measures; to issue warnings; and to analyze cyber-incidents in real time. The ISAC operates in the various sectors:

In the financial sector, the main role of the ISAC is establishing a database on cyber-incidents, vulnerabilities, and patches in order to offer analysis of the system vulnerability as far as hacking, worms, and viruses as well as response measures are concerned. Furthermore, it maintains CERTs and monitoring systems for real-time analysis and response in case of cyber-attacks. The ISAC also analyzes and assesses the vulnerability of critical information infrastructures and elaborates response measures.

In the security sector, the ISAC offers a database on cyber-incidents, vulnerabilities, and patches, shares information with relevant organizations outside the ISAC, and provides information online. In addition, it operates a monitoring system as well as a CERT, while planning to develop systems that gather and analyze data on cyber-terror, viruses, and hacking in the financial sector. It assesses and monitors the vulnerability of critical information infrastructures.

In the telecommunication sector, the ISAC provides information on vulnerabilities, causes of incidents, and response measures. It operates a warning and analysis system when cyber-attacks occur. Moreover, it supports members with preventive measures and collects their opinion for government policy on cyber-security.[380]

380 Information provided by Korean expert involved.

Law and Legislation

Information Security Promotion Systems

Information-security promotion systems in Korea can be divided into national cyber-security systems, e-government security systems, critical information infrastructure systems, and private information security systems. With respect to the national cyber-security system, the "National Cyber Security Management Regulation" was issued by a presidential directive on 31 January 2005, which regulates cyber-security organizations such as the National Cyber Security Strategy Council or the National Cyber Security Center. Meanwhile, for e-government security systems, the "Act on Promotion of Electronic Administration for e-Government", enacted on 28 February 2001, regulates matters of information protection as well as e-government.

National Information Infrastructure Protection Act 2001

The ministerial meeting on the prevention of cyber-terrorism in February 2000 decided to pass a law covering comprehensive and systematic information infrastructure protection and countermeasures against cyber-terrorism. The "Information Infrastructure Protection Act" was passed in January 2001. It outlines the government framework for information infrastructure protection. It directs the affairs of the Critical Information Infrastructure Security Committee, the Working Group for Security Incident Response, and other central administrative organizations. Moreover, protection measures, prevention and response, technical support, development of technologies, international cooperation, and penalties for cyber-crimes are addressed.[381]

The Act on Private Information Protection of Public Organizations, the Act on Promotion of Electronic Administration for e-Government, and the Resident Registration Act in the public sector, as well as the Act on Promotion of Utilization of Information and Communication Network Utilization and Information in the private sector deal with private information security systems.[382]

381 Cha, Yang-Shin. Korea's Approach to Network Security (21 Mai 2002). http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.21.pdf.

382 Information provided by Korean expert involved.

e-Signature and Certification

As electronic transactions and commerce across long distances become more common due to the development of ICT networks, a legal framework has been established regarding e-signatures and their certification, in order to secure safety and reliability for electronic documents that are drawn up by data processing systems and then transferred, received, or saved. The e-Signature Act and the e-Commerce Framework Act regulate certification of e-signatures, and the Act on Promotion of Electronic Administration for e-Government governs the use of e-signatures in the public administration.[383]

Protection of Telecommunication Networks and Information Systems

As attacks on telecommunication networks and information systems increase in the public and private sectors, the need for a systematic national-level protection system has become urgent. The Framework Act on Information Promotion, the Critical Information Infrastructure Protection Act, the Act on the Promotion of Utilization of Information and Communication Network Utilization and Information, the e-Commerce Framework Act, the e-Government Act, the Act on Trade Automation Promotion, the Act on Industrial Infrastructure, and the Freight Distribution Promotion Act have been passed to protect telecommunication networks and information systems.[384]

Cyber-Attacks

The following laws and regulations are applied in order to prevent national and social loss arising from hacking, viruses, service rejection in relation to telecommunication networks as well as information systems, and theft or forgery of information:

- Article 28 of the National Information Infrastructure Protection Act imposes a penalty for attacks on critical information infrastructures.

383 Information provided by Korean expert involved.
384 Information provided by Korean expert involved.

- Article 62 of the Act on the Promotion of Utilization of Information and Communication Network Utilization and Information Protection punishes attacks on telecommunication networks and violations of a duty to protect secret information.
- Article 25 of the Act on Trade Automation Promotion, as well as Sections 2 and 4 of Article 54 of the Freight Distribution Promotion Act can be applied as well.

In addition, there are provisions in the national criminal legislation dealing with computer crime.[385]

385 Information provided by Korean expert involved.

Malaysia

Critical Sectors

In Malaysia, the following sectors are regarded as making up the national critical infrastructure:

Financial Sector,

- Water and Sewerage,
- Communications and Media,
- Energy,
- Health and Emergency Services,
- Industry,
- Central Government,
- Government Services,
- Transportation,
- Military.[386]

386 Rahman, Bistamam Siru Abdul (MCMC). Malaysia's Approach to Network Security. Presentation held at ITU Workshop on "Creating Trust in Critical Network Infrastructures" (Seoul, May 2002), slide 7. http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.19.pdf.

Past and Present Initiatives and Policies

Malaysia launched the "National IT Agenda" (NITA) in 1996 as part of a major strategy to prepare the nation for the challenges of the information age. The agenda contains an outline for a national framework aimed at providing a balanced IT development of Malaysia, its infrastructure, and the applications found within. According to the Agenda, for this effort to succeed, Malaysia requires greater trust and faith in the use of information and communication technology (ICT), which can be gained through enhanced ICT security.[387]

In March 1997, the Malaysian Computer Emergency Response Team (MyCERT) was launched.[388] Over the years, MyCERT has provided assistance to many Malaysians in handling ICT security incidents. During this period, there was an increase in national awareness of ICT – in particular, of the fact that ICT security issues encompass a much broader scope than previously envisaged. Purely technical measures, such as firewalls, are not sufficient for tackling security threats. The government of Malaysia realized that the growing number and variety of ICT applications and devices produced by suppliers lacking fundamental security precautions had created a strong need for a trusted ICT security center to support not only reactive measures, but also proactive measures in ICT security.

Realising this vital need, the 6th National Information Technology Council (NITC) Meeting on 15 January 1998 agreed to establish a national network security and accreditation agency, which in turn gave birth to the National ICT Security and Emergency Response Centre (NISER).[389] In the same year, the Communications and Multimedia Act (CMA) identified information security and the reliability and integrity of networks as national policy objectives.

National IT Agenda (NITA) and NITC Strategic Agenda

In December 1996, the "National IT Agenda" (NITA) was launched by the NITC, providing the foundation and framework for the utilization of information and communication technology to transform Malaysia into an information and knowledge society.

387 http://www.niser.org.my/about.html.
388 http://www.mycert.org.my/about.html.
389 http://www.niser.org.my/about.html.

Besides NITA, the NITC formulated the "NITC Strategic Agenda", a strategy involving a more participatory governance structure with active partnership between the public, private, and community-interest sectors. The Strategic Agenda includes concepts such as e-community, e-public services, and e-economy. It is based on the assumption that knowledge and information will be the most valuable assets in the new economy.[390]

e-Secure Malaysia 2005 International Conference

An important information security event, "e-Secure Malaysia 2005", took place in September 2005 in Kuala Lumpur. It consisted of two conferences and an exhibition targeted at security professionals, solution providers, policy-makers, corporate decision-makers, and government officials. The event was jointly organized by various government agencies such as the Ministry of Science, Technology and Innovation (MOSTI), the Ministry of Energy, Water and Communications (MEWC), the Malaysian Communications and Multimedia Commission (MCMC), the National ICT Security and Emergency Response Centre (NISER), and the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU). The conference focused on the following topics: Computer Emergency Response Teams (CERTs) and incident response; critical infrastructure protection; network and application security; security management and strategy; and knowledge-sharing.[391]

National Information Security Policy 2006

A major "National Information Security Policy" was completed on 22 December 2005 and is currently being considered by the Malaysian government. The publication and implementation of this policy will take place during 2006. Its aim is to ensure coordination and timely response to protect critical information infrastructure.[392]

390 http://www.msctc.com.my/idb/B-1.htm.
391 http://www.esecuremalaysia.org.my.
392 Information provided by a Malaysian expert from the Malaysian Communications and Multimedia Commission (MCMC).

Organizational Overview

Public Agencies

The Malaysian Communications and Multimedia Commission (MCMC) has a coordinating role. The Malaysian Administrative Modernization and Management Planning Unit (MAMPU) administers security issues in the public sector.

Malaysian Communications and Multimedia Commission (MCMC)

The MCMC[393] is a statutory body established in 1998 in accordance with the national policy objectives set out in the Communications and Multimedia Commission Act[394] and in the Communications and Multimedia Act (CMA).[395] The MCMC oversees the new regulatory framework for the converging industries of telecommunications, broadcast, and online activities. This includes the development and enforcement of access codes and standards. The MCMC ensures information security and the integrity and reliability of the network of Malaysia, identified as one of the ten national policy objectives in the CMA. Together with the police, the MCMC has enforcement powers for offences relating to network security in the CMA. In June 2002, MCMC hosted a workshop on "Information and Network Security and the Protection of Critical Infrastructure".[396]

Malaysian Administrative Modernization and Management Planning Unit (MAMPU)

Security issues in the public sector are administered by the Malaysian Administrative Modernization and Management Planning Unit (MAMPU).[397]

393 http://www.cmc.gov.my.
394 This act created a new regulatory body, the MCMC.
395 This act set out a new regulatory licensing framework for a convergent communications and multimedia industry. For example, it covers fraudulent use of network facilities/services and interception of communications.
396 Rahman, Malaysia's Approach to Network Security, op. cit., slide 17.
397 http://www.mampu.gov.my.

Within MAMPU, the ICT Security Division also operates as a Computer Emergency Response Team (CERT) for the government. Recently, the ICT Security Division launched the "Malaysian Public Sector Management of Information and Communications Technology Security Handbook" (MyMIS).[398] This handbook is a set of guidelines for best practices and measures for information and network security. It covers a variety of topics such as legal matters; examples of common threats, abuses, methods, and detection; ICT security risk analysis and management strategies; employee awareness; disaster recovery; and contingency planning. The public sector is obliged to abide by the handbook, and private companies are encouraged to do the same. The ICT Security Division has no enforcement powers, however. MAMPU also hosts the Government Computer Emergency Response Team (GCERT).[399]

In the field of e-government, MAMPU developed the "ICT Strategic Plan" in 2003 to provide citizens and businesses enhanced access to government information and services.[400]

The current information security measures provided by MAMPU fall under three categories:

- Proactive measures: providing ICT security documents such as an ICT security policy framework for the public sector; MyMIS; ICT incident reporting mechanisms; and best practices.
- Recovery measures: ensuring continuous function of critical business in the event of disruption; advice on how to upgrade patches; and warning of virus attacks.
- Continuous measures: monitoring, enforcement, policy review and improving ICT security management.[401]

Police Cyber Crime Unit

The Royal Malaysia Police has established a Technology Crime Investigation Unit under the Commercial Crime Investigation Division of the Criminal

398 Malaysian Administrative Modernisation and Management Planning Unit (MAMPU), Prime Minister's Department. Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMis) (January 2002). http://www.mampu.gov.my/mampu/bm/program/ict/mymis/mymis.htm.

399 http://gcert.mampu.gov.my.

400 http://www.mampu.gov.my/mampu/bi/program/ict/ISPlan/ISPlan.htm.

401 http://www.niser.org.my/news/2004_02_05_01.html.

Investigation Department. The investigation officers in this unit investigate and take proactive action against commercial crime involving computers and internet-related crimes. The police has also established a Forensic Computer Laboratory to assist officers investigating computer crime.[402]

Ministry of Science, Technology and Innovation (MOSTI)

Under a recent restructuring, the Ministry of Science, Technology and Innovation (MOSTI) took over responsibility from the former Ministry of Energy, Communication and Multimedia (MECM) for:

- Formulation and implementation of national policy on ICT;
- Formulation and implementation of national information security policy;
- Encourage research and development and commercialization of ICT;
- Development and promotion of ICT industries.[403]

In September 2005, MOSTI organized the "National Information Security Week". This event reflects the Malaysian government's commitment to positioning Malaysia as a regional hub for information security.[404]

Following the restructuring, the National Information Technology Council (NITC) Secretariat was transferred to MOSTI. The ICT Policy Division within MOSTI was established on 1 March 2005 with five units, namely the Policy and Strategic Unit, the ICT Technology Studies Unit, the Assessment and Monitoring Unit, the ICT Acculturation Unit, and the NITC Secretariat.[405]

Ministry of Energy, Water and Communications (MEWC)

The Ministry of Energy, Water and Communications (MEWC) was established in March 2004, and manages the nation's energy, communications (infrastructure), postal services, and water supply. MEWC develops and formulates

402 http://www.niser.org.my/news/2004_10_19_02.html.
403 http://www.mosti.gov.my/opencms/opencms/MostePortal/NITC/NITCIntro.html.
404 http://www.esecuremalaysia.org.my/left.htm.
405 http://www.mosti.gov.my/opencms/opencms/MostePortal/NITC/NITCIntro.html.

strategic and innovative policies, a self-regulatory framework, and an effective management system. One of its objectives is to ensure a secure and reliable supply and provision of energy, water, and communications services.[406]

Public-Private Partnership

Information Sharing Forum (ISF)

The Information Sharing Forum (ISF) was formed in June 2004 by the Malaysian Communications and Multimedia Commission (MCMC). It brings together various Internet Service Providers (ISP) and other agencies to address Malaysian information and network security issues . Apart from encouraging cooperation between different network owners, operators, and other agencies, this forum enables the sharing of experience and expertise for the benefit of the Malaysian network infrastructure.[407] Another important aim is to elaborate guidelines and best practices.[408]

Early Warning and Public Outreach

National ICT Security and Emergency Response Center (NISER)

The National ICT Security and Emergency Response Center (NISER)[409] was formed by the National Information and Communication Technology Council (NITC) to address e-security issues and to act as Malaysia's CERT. NISER evolved from what was originally the Malaysian Computer Emergency Response Team (MyCERT) in March 1997. NISER offers services to private and public entities such as research in vulnerability detection, intrusion detection, and

406 http://www.ktkm.gov.my/print_details.asp?Content_ID=397.

407 http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&thold=-1&mode=flat&order=0&sid=16395.

408 "Anti-Spam Activities in Malaysia – Current Situation, Regulatory Environment and Future Developments". Presentation held at the ITU Global Symposium for Regulators (Geneva 8–10 December 2004). http://www.itu.int/ITU-D/treg/Events/Seminars/2004/GSR04/documents/NurAbdullah.pdf.

409 http://www.niser.org.my.

computer forensic technology. It is also a member of FIRST and APCERT (Asia Pacific Computer Emergency Response Team). Through collaboration with other agencies, NISER provides specialized ICT security services and continuously identifies possible gaps that could be detrimental to national security. NISER fosters mutual co-operation, information-sharing and expert assistance among the different government agencies involved.[410]

Malaysian Computer Emergency Response Team (MyCERT)

The Malaysian Computer Emergency Response Team (MyCERT)[411] was formed in 1997 and provides a point of reference for the internet community to deal with computer security incidents and methods of prevention. MyCERT aims at reducing the probability of successful attack and lowering the risk of consequential damage. MyCert works closely with the CERT Coordinating Centre, AusCERT, and the Malaysian police. MyCERT has the following functions:

- Providing an expert point of reference on network and security matters;
- Reporting security incidents and facilitating communication to resolve security incidents;
- Disseminating security information, including system vulnerabilities and defense strategies;
- Acting as a repository of security-related information, acquiring patches, tools, and techniques;
- Educating the public with regard to computer security in Malaysia.[412]

410 http://www.niser.org.my/about.html.
411 http://www.mycert.org.my.
412 http://www.mycert.org.my.

Law and Legislation

The Malaysian government has passed a number of cyber-laws since 1997 to provide a comprehensive legal framework, which encompasses the security of information and network integrity and reliability, for the benefit of society at large as well as the business sector in particular.

Computer Crimes Act 1997

Part II, Offences

3 (1) A person shall be guilty of an offence if

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at –

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall on conviction be liable to a fine or to imprisonment not exceeding five years or to both.[413]

Communications and Multimedia Act (CMA) 1998

An Act to provide for and to regulate the converging communications and multimedia industries, and for incidental matters.

413 Communications and Multimedia Act 1998. http://www.cybercrimelaw.net/countries/malaysia.html.

Part 1 — Preliminary Section 3.

Objects (1)

The objects of this Act are — (a) to promote national policy objectives for the communications and multimedia industry; (b) to establish a licensing and regulatory framework in support of national policy objectives for the communications and multimedia industry; (c) to establish the powers and functions for the Malaysian Communications and Multimedia Commission; and (d) to establish powers and procedures for the administration of this Act.

(2) The national policy objectives for the communications and multimedia industry are - (a) to establish Malaysia as a major global centre and hub for communications and multimedia information and content services; (b) to promote a civil society where information-based services will provide the basis of continuing enhancements to quality of work and life; (c) to grow and nurture local information resources and cultural representation that facilitate the national identity and global diversity; (d) to regulate for the long-term benefit of the end user; (e) to promote a high level of consumer confidence in service delivery from the industry; (f) to ensure an equitable provision of affordable services over ubiquitous national infrastructure; (g) to create a robust applications environment for end users; (h) to facilitate the efficient allocation of resources such as skilled labour, capital, knowledge and national assets; (i) to promote the development of capabilities and skills within Malaysia's convergence industries; and (j) to ensure information security and network reliability and integrity.

(3) Nothing in this Act shall be construed as permitting the censorship of the Internet.[414]

414 http://www.mcmc.gov.my/mcmc/the_law/ViewAct.asp?cc=4446055&lg=e&arid=900722.

The Netherlands

Critical Sectors

Using the so-called "Quick Scan" method and in consultation with the industry and government, it was determined in 2002 that the Netherlands' critical infrastructure comprises 11 sectors and 31 critical products and services. The ensuing risk analysis phase has caused adjustments. Since April 2004, there are 12 sectors and 33 critical products and services. Infrastructures are deemed critical if they constitute an essential, indispensable facility for society, and if their disruption would rapidly bring about a state of emergency or could have adverse societal effects in the longer term. In the Netherlands, critical sectors (and products and services) include the following:[415]

- Drinking Water (Drinking Water Supply),
- Energy (Electricity, Natural Gas, and Oil),
- Financial (Financial Services and the Financial Infrastructure, both Public and Private),
- Food (Food Supply and Food Safety),

* The Country Survey 2006 of the Netherlands was reviewed and updated by Eric Luiijf, TNO Defense, Security and Safety.

415 Ministry of the Interior and Kingdom Relations. The Netherlands, September 2005: Critical Infrastructure Protection in The Netherlands (in Dutch), p. 58.

- Health (Urgent Health Care/Hospitals, Sera and Vaccines, Nuclear Medicine),
- Legal Order (Administration of Justice and Detention, Law Enforcement),
- Public Order and Safety (Maintaining Public Order, Maintaining Public Safety),
- Retaining and Managing Surface Water (Management of Water Quality, Retaining and Managing Water Quantity),
- Telecommunications (Fixed Telecommunication Network Services, Mobile Telecommunication Services, Radio Communication and Navigation, Satellite Communication, Broadcast Services, Internet Access, Postal and Courier Services),
- Public Administration (Diplomatic Communication, Information Provision by the Government, Armed Forces and Defense, Decision-making by Public Administration),
- Transport (Mainport Schiphol, Mainport Rotterdam, Main Road and Waterway Infrastructure, Rail Transport).
- Chemical and Nuclear Industry (Transport, Storage, and Production/Processing),

The Critical Information Infrastructure (CII) of the Netherlands consists mainly of the internal supporting infrastructure of critical sectors like the energy, transport, and financial sectors, and is supported by a set of services delivered by the telecommunications and energy sectors (fixed telecommunication, mobile telecommunication, internet access, electricity).

Past and Present Initiatives and Policies

In the Netherlands, CIP/CIIP is perceived increasingly as a crucial issue of national security. Since the end of the 1990s, several efforts have been made to better manage CIP/CIIP.

The Digital Delta

The publication "The Digital Delta" of June 1999 offers a framework for a range of specific measures regarding government policy on information and communications technology (ICT) for the next three to five years.[416] This memorandum notes the increasing importance of ensuring the security of information systems and communications infrastructure, and of mastering the growing complexities of advanced IT applications.[417]

Defense Whitepaper 2000

Likewise, the increasing importance of ICT is also explicitly mentioned in the Dutch "Defense Whitepaper 2000": "Given the armed forces' high level of dependence on information and communication technology, it cannot be ruled out that in the future attempts will be made to target the armed forces in precisely this area."[418]

Infodrome Initiative and BITBREUK

In March 2000, the key essay BITBREUK (English version "In Bits and Pieces") was published by the government-sponsored think-tank Infodrome[419] to stimulate the discussion on the need to protect CII. The essay offered an initial vulnerability analysis and postulated a number of hypotheses for further discussion and examination by the Dutch authorities in co-operation with the

416 http://www.gbde.org.

417 Luiijf, Eric, and Marieke Klaver. In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society (Amsterdam, March 2000); translation of the Dutch Infodrome essay 'BITBREUK', de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij, p. 5.

418 Ministerie van Defensie, Defensienota 2000, (1999), p. 59.

419 Infodrome was a think-tank founded in 1999 and sponsored by the Dutch government that served a threefold objective: (1) to develop an understanding of the social implications of the information revolution (this requires the gathering of empirical, quantitative knowledge and data on IT-related developments, and a systematic analysis thereof), (2) to stimulate social awareness of the importance of having a government policy that meets the requirements of the information society, and (3) to examine the priorities given by parties and interest groups to activities (public or private) undertaken in relation to the information society. This requires an understanding of the political and social value of knowledge, experience, and insights. The Infodrome project ended in 2002.

appropriate national public and commercial organizations.[420] In mid-2001, this document was used as a starting point for a so-called 24-hour cabinet session. This was a 24-hour workshop with a selected group of experts that created a manifesto on CI/CII issues with a set of recommendations for all political parties. This "KWINT-manifest" document is available only in Dutch.[421]

KWINT Report and Memorandum

The report entitled "Kwetsbaarheid op Internet — Samen werken aan meer veiligheid en betrouwbaarheid (KWINT)", written by Stratix Consulting/TNO[422] for the Ministry of Transport, Public Works, and Water Management (V&W), was completed in 2001. The report concluded that the Dutch internet infrastructure was extremely vulnerable. Final recommendations were made on policy measures with regard to awareness and education, coordination of incidents, protection, and security. The report concluded that the measures should be realized within a public-private partnership framework, while the government should play a facilitating and coordinating role.[423]

The findings and recommendations of this report triggered the formation of an interdepartmental working group of members of the Ministries of Economic Affairs, Defense, Finance, the Interior, Justice, and Transport (Telecom and Post Directorate).[424] As a result, the KWINT government memorandum "Vulnerability of the Internet" was endorsed by the cabinet on 6 July 2001. It includes a set of recommendations for action. A government-wide computer emergency response team, GOVCERT.NL, was established, and a malware-alerting service for SMEs and the public was set up.[425] Other KWINT tasks were given to the "Platform Electronic Commerce in the Netherlands (ECP.NL)", the public-private platform for e-commerce in the Netherlands.

420 Luiijf/Klaver, In Bits and Pieces, op. cit.
421 http://www.infodrome.nl and http://www.kwint.org.
422 TNO is the Netherlands' Organization for Applied Scientific Research.
423 De Bruin, Ronald. "From Research to Practice: A Public-Private Partnership Approach in the Netherlands on Information Infrastructure Dependability". Dependability Development Support Initiative (DDSI) Workshop (28 February 2002).
424 The Telecom and Post Directorate (DGTP) became part of the Ministry of Economic Affairs as of 1 January 2003.
425 http://www.waarschuwingsdienst.nl.

The Dutch CIIP policy as laid out by KWINT is based on three premises: measures should not decrease innovation; the dynamic character of threats should be taken into account; and there is no 100 per cent reliability.[426] The government policy is aimed at fostering wider application of ICT and an understanding of the consequences. In its report, entitled "Government losing ground", the WRR,[427] a government advisory body, analyzed some of the political aspects of the further advance of ICT across society.[428]

The "KWINT Program 2002–2005" was especially targeted at the protection and safe use of the internet. The 2005 report to the Dutch parliament recognizes the need to address the security of ICT that is used across critical sectors. The dependency and vulnerability of SCADA, for instance, is a cross-sector ICT area that will be analyzed in detail.

The successor KWINT program is called "Veilige Elektronische Communicatie" (VEC) and will run from 2006 until the end of 2008.[429]

Quick Scan on Critical Products and Services

In early 2002, the Dutch government initiated the critical infrastructure protection project "Protection of the Dutch Critical Infrastructure",[430] with the objective of developing an integrated set of measures to protect the infrastructure of government and industry, including ICT.[431]

To identify sectors, products, and services comprising the national critical infrastructure, a "Quick-Scan Questionnaire" was developed. Dutch government departments used this questionnaire in early 2002 to make an inventory of all products and services that they regarded as vital, including the underlying processes and dependencies. In June 2002, an analysis of the collected information was presented in a working conference with key representatives of both the public and the private sectors. The initial results were then augmented and refined in 17 workshops with the vital public and private sectors. In parallel,

426 De Bruin, From Research to Practice, op. cit.
427 Wetenschappelijke Raad voor het Regeringsbeleid.
428 http://www.infodrome.nl.
429 Information provided by Dutch expert involved.
430 Bescherming Vitale Infrastuctuur.
431 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Critical Infrastructure Protection in the Netherlands: Quick Scan on Critical Product and Services (April 2003).

damage experts evaluated the potential damage impact of loss or disruption of vital products and services.[432]

In April 2003, the findings of the Quick Scan, performed in close collaboration with the Netherlands Organization for Applied Scientific Research (TNO) were published by the Ministry of the Interior and Kingdom Relations.[433] The following main conclusions were drawn from the Quick Scan results:

- The Dutch government and industry now have a clear understanding of the critical products and services that comprise the Netherlands' critical infrastructure, and of their (inter-) dependencies.
- The direct and indirect vitality of critical products and services has been elaborated.
- It became clear that actors responsible for critical products and services only have a limited understanding of other critical products and services that depend on them, and of the extent of this dependence.[434]

The next steps concerning the strengthening of the Netherlands' CIP/CIIP included the pinpointing of the vital nodes for each of the critical services, risk and vulnerability analyses for each critical sector, scenarios to test the effectiveness of CIP/CIIP measures, and international exchange of CIP/CIIP information and coordination.[435]

As a result of the studies, a set of actions was announced in September 2005 by the minister of the interior in a letter to the Dutch parliament[436]:

432 To determine the elements of the national critical infrastructure, the Dutch approach aims to distinguish between products and services vital to the nation and those that are "merely" very important. Under this method, a product or a service is defined as vital if it "provides an essential contribution to society in maintaining a defined minimum quality level of (1) national and international law and order, (2) public safety, (3) economy, (4) public health, (5) ecological environment, or (6) if loss or disruption impacts citizens or the government administration at a national scale." By measuring criticality according to a predefined minimum level of acceptable quality in vital services to society, the approach shifts the problem of defining "vital" or just "very important" elements to the political level. It is the government that must determine the level of damage impact that is acceptable to society. Luiijf, Eric A.M., Helen H. Burger, and Marieke H.A. Klaver, "Critical Infrastructure Protection in The Netherlands: A Quick-scan". In: Gattiker, Urs E., Pia Pedersen, and Karsten Petersen (eds.): EICAR Conference Best Paper Proceedings 2003.

433 Ibid., p. 7.

434 Ibid., p. 23.

435 Ibid., p. 25.

436 House of Parliament (Tweede Kamer) 2005–2006, 26643 No. 75, 16 September 2005, and annex "Rapport ter Bescherming Vitale Infrastructuur" dated 1 September 2005.

- Intensifying critical infrastructure security policy. A framework for assessing the desired and required degree of security, the corresponding measures, and the associated costs will be developed in the follow-up phase. A task force security will work with all involved parties, public and private, to draw up a plan of approach in the short run in order to gain clarity on how a security impulse can be achieved before the end of 2006. This includes information sharing by intelligence and law enforcement on threats and best practices;
- Initiating a regional-based approach, especially for areas where vital nodes of multiple CIs are collocated;
- CI protection measures that correspond to the various levels of the Dutch Terrorism Warning System;
- Scenario exercises involving distribution plans for CI products/services in the event of scarcity of supply, both at the national and regional levels;
- Improving the national emergency communication networks;
- Setting up a "Critical Infrastructure Strategic Consultation Group (SOVI)" that includes both public and private CI stakeholders;
- Intensifying cross-critical sector communication: Critical sectors must be able to get in touch with each other — not only to determine the extent of the crisis, but also to assess its likely duration. The last answer will determine whether the affected critical sectors will have to take additional measures in order to guarantee continuity. Communication on risk and security aspects will be intensified;
- Development of a cross-critical sector regime of visitation to assess the quality of measures designed to protect critical infrastructure, in order to improve cross-sector understanding of protection measures taken and of the need for protection by the dependent sectors.[437]

Anti-Terrorism Plan

The Ministry of the Interior and Kingdom Relations was tasked by the cabinet as part of the nation's anti-terrorism plan with elaborating a coherent package of measures to protect (critical) infrastructure in both the public and private

437 Information provided by Dutch expert involved.

sectors, and to anchor this package as part of normal business operations.[438] From 2002–2004, the National Coordination Center (NCC), which is part of the Ministry of the Interior and Kingdom Relations, was entrusted with protecting the Dutch critical infrastructure by leading and coordinating the multi-step project.[439] Since September 2004, the national CIP efforts have been coordinated by the Directorate of Crisis Management within the Ministry of the Interior and Kingdom Relations. The CIP project comprised the following steps:[440]

1 A quick-scan analysis of the Dutch critical infrastructure to identify products and services vital to the nation, the (inter-) dependencies of these products and services, and underlying essential processes;
2 Stimulation of a public-private partnership;
3 Threat and vulnerability analysis;
4 A gap analysis of protection measures.

Organizational Overview

Public Agencies

As stated above, responsibility for the Dutch CII lies with various actors and involves public and private sectors as well as multiple ministries. In particular, the Ministry of Economic Affairs/Directorate-General Telecom and Post[441] is responsible for the protection policy for telecommunications and the internet. Other parts of the same ministry are responsible for CIP/CIIP policies regarding the private industry, including SMEs. The Ministry of the Interior and Kingdom Relations is responsible (in terms of policy) for the protection of government information infrastructures (government CIIP). It coordinates

438 House of Parliament (Tweede Kamer). Dossier 27925 - action line 10.
439 Bescherming Vitale Infrastuctuur.
440 Critical Infrastructure Protection in the Netherlands, op. cit., p. 9.
441 From 1 January 2006 it will be known as the Ministry of Economic Affairs/Directorate-General Energy and Telecommunications.

CIP policy across all sectors and responsible ministries, and is responsible for international CI/CIIP co-ordination and policy activities.

Ministry of the Interior and Kingdom Relations (BZK)

The duties of the Ministry of the Interior and Kingdom Relations include the promotion of public order and safety as well as the administration of the national police forces. It includes the Directorate of Crisis Management, the National Co-ordination Center (NCC), which is in charge of coordination activities at the policy level in case of emergencies and disasters with a nation-wide impact. The BZK is also responsible for the government computer emergency response team GOVCERT.NL.

Ministry of Economic Affairs (EZ)

The Directorate-General for Telecommunications and Post (DGTP) is subordinated to the Ministry of Economic Affairs. On 1 January 2006, the DGTP merged with the Directorate-General for Energy and became the Directorate-General for Energy and Telecommunications. The two most important goals are the strengthening of the Netherlands' competitive position in the field of telecommunications, telematics, and postal services, and to ensure the continuation of supply of critical energy and telecommunication services to citizens and companies.[442] This ministry is responsible for CIP/CIIP policy for the private energy and telecommunication sectors as well as the private industry, including SMEs.

Ministry of Transport, Public Works, and Water Management (V&W)

The Ministry of Transport, Public Works, and Water Management (V&W)[443] is responsible for coordinating the protection of the transport and water management critical infrastructures.

442 http://www.minez.nl/index.jsp.
443 http://www.verkeerenwaterstaat.nl/?lc=uk.

Ministry of Housing, Spatial Planning, and the Environment (VROM)

The Ministry of Housing, Spatial Planning, and the Environment (VROM)[444] is responsible for coordinating the CI protection of the chemical and nuclear industries, as well as the potable water infrastructure.

Ministry of Health, Welfare and Sport (VWS)

The Ministry of Health, Welfare, and Sport (VWS)[445] is responsible for coordinating the protection of the critical health sector services. This includes the biochemical quality of the surface water.

General Intelligence and Security Service (AIVD)

The General Intelligence and Security Service (AIVD)[446] is a division of the Ministry of the Interior and Kingdom Relations and is tasked with protecting the information security and vital sectors of the Dutch society.[447] The AIVD's focus shifts in accordance with social and political changes. One of its tasks is to uncover forms of improper competition, such as economic espionage, that could harm Dutch economic interests.[448] Another task is foreign intelligence. In the interests of national security, it will carry out investigations abroad, though only in the non-military sphere.[449] The AIVD is responsible for analyzing potential and likely threats to the Dutch CI sectors.

National High-Tech Crime Center (NHTCC)

The National High-Tech Crime Center (NHTCC)[450] is a joint initiative of the Netherlands Police Agency KLPD and the Ministries of the Interior and Kingdom Relations, Economic Affairs, and Justice to tackle crimes carried out

444 http://international.vrom.nl/pagina.html?id=5450.
445 http://www.minvws.nl/en.
446 Algemene Inlichtingen- en Veiligheidsdienst, AIVD, formerly called BVD. In December 2000, a total of 594 personnel were employed by the BVD. This figure has since increased by over 100 people per year.
447 http://www.fas.org/irp/world/netherlands/bvd.htm.
448 http://www.minbzk.nl/uk.
449 Ibid.
450 http://www.nhtcc.nl/index_en.html.

using or against ICT. The NHTCC has operated informally since 2003/2004 as a project organization. The NHTCC is expected to become fully operational in 2006. It has a proactive approach and focuses on the negative consequences that a possible attack could have for Dutch society in general, and for the critical information infrastructures in particular. The NHTCC supports cross-agency and public-private collaboration and information-sharing at both the national and international level. Agreements have been made with certain private CIP stakeholders like banks and Schiphol Mainport. The aim is to establish the NHTCC as a center of expertise and as a possible reporting center, designed to give early warning of and the swiftest possible response to high-tech crime.[451]

Public-Private Partnerships

The above-mentioned KWINT study of 2001 led to a flurry of policy recommendations that are elaborated in further detail in the public-private partnership platform ECP.NL. These recommendations refer to awareness-raising, research and development, alarm and incident response, and the integrity of information.

Public-private co-operation within the project "Protection of the Dutch Critical Infrastructure"[452] also involves the Confederation of Netherlands Industry and Employers (VNO-NCW) in a coordinating private-sector role.

Platform Electronic Commerce in the Netherlands (ECP.NL)

The Platform Electronic Commerce in the Netherlands (ECP.NL),[453] the platform for eNetherlands, has been tasked by the Ministry of Economic Affairs with setting up a public-private partnership program to implement the action guidelines of the KWINT Memorandum.

The objective of the KWINT program[454] (2002–2005) was to define concrete protective measures against the risk for businesses, consumers, the government, and citizens when using the internet. A second objective was to provide a platform for public-private partnership, thus offering a sounding-board for government policy-making. The steering board and the various

451 Ibid.
452 Bescherming Vitale Infrastuctuur, op. cit.
453 http://www.ecp.nl.
454 http://www.kwint.org.

working groups consist of representatives of the government and the private sector.

Acting on the recommendations of a risk analysis, the program focused on the following aspects: continuity of the internet infrastructure in the Netherlands, viruses, denial-of-service attacks, hacking, transparency of internet services, integrity and confidentiality of information, and misuse by personnel.

Within the program, a best practice has been developed for defining solutions, creating commitment, and communicating solutions to the end users who will be implementing them. The program has delivered many different results, from complex risk analyses to practical tools; e.g. security guidance documents for SMEs; the required steps to report cyber-crime; continuity of the Dutch internet; courseware on the "Safe Internet" for parents ("A safer Internet for all"); and transparency through "transparameters" (quality of internet service provision). These measures have created a sense of commitment not only among participants, but also among many stakeholders. To this end, public stakeholder debates are organized involving politicians, researchers, business executives, and users. KWINT Marketplaces have been organized to present solutions to intermediary organizations that play a key role in disseminating them to their members. These intermediaries also provided feedback to the KWINT program on the actual implementation of the solutions by their members. Finally, the program has also co-operated closely with the government on international developments, for example within the OECD and the EU.

National Continuity Plan for Telecommunications (NACOTEL) and National Continuity Consultation Platform Telecommunications (NCO-T)

Furthermore, the "National Continuity Plan for Telecommunications" (NACOTEL) structures the contingency policy and crisis management in the telecommunications sector. The NACOTEL platform prepares for managing serious disruptions of the critical telecommunications sector. The public-private partnership includes BT, Enertel, KPN Telecom, Telfort, Orange, T-Mobile, and Vodafone - as well as the Ministry of Economic Affairs. It is expected that the NACOTEL agreement will be extended in 2006 to include more telecommunication providers.

NACOTEL will soon be superceded by the "National Continuity Consultation Platform Telecommunication (NCO-T)". NCO-T will have as tasks:

- State preventive measures to prevent disruptions and crises which may affect vital interests;
- Take preparation measures to resolve such disruptions and crises as fast as possible and with as few damage as possible to the vital interests.

This NCO-T will be based upon a forthcoming change (early 2006) in the Dutch telecommunication regulations. Some telecommunication providers will be obliged by the government to participate in and contribute to the NCO-T. The representatives of the telecommunication providers in the NCO-T will be the policy-makers and decision-takers on service continuity. Chairperson is one of the Directors of the Dutch Ministry of Economic Affairs Directorate-General Energy and Telecommunications.

Early Warning and Public Outreach

CERT-NL (part of SURFnet)

CERT-NL is the Computer Emergency Response Team of SURFnet, the internet provider for institutes of higher education and for many research organizations in the Netherlands. CERT-NL handles all computer security incidents involving SURFnet customers, either as victims or as suspects. CERT-NL also disseminates security-related information to SURFnet customers on a structural basis (e.g., distributing security advisories) as well as on an incidental basis (distributing information during disasters).[455] CERT-NL disseminates information coming from CERT-CC/FIRST.

455 http://cert-nl.surfnet.nl/home-eng.html.

GOVCERT.NL

A computer emergency response team for government departments (CERT-RO) was established in June 2002. In February 2003, it was renamed GOVCERT.NL.[456] It is operated under the responsibility of the Ministry of the Interior and Kingdom Relations[457] under its ICT agency ICTU. The GOVCERT.NL team is co-located and co-operates with "Waarschuwingsdienst.nl",[458] a website and initiative by the Ministry of Economic Affairs that is responsible for issuing alerts and advice memoranda to the public and SMEs about viruses, Trojan Horse codes, and other malicious software, or "malware". Warnings are disseminated to the public via e-mail, web services, and SMS. The Waarschuwingsdienst was founded in early 2003 and is funded by the Ministry of Economic Affairs/Directorate-General for Energy and Telecom.

At the tactical level, the KWINT program focuses on improving general awareness of ICT security through best-practice procedures. This includes, for example, the free provision of the Dutch version of ISO/IEC 17799:2000 (or BS 7799). Apart from the National High Tech Crime Center (NHTCC), no early-warning or incident-analysis capability is planned at the strategic national level. This is because CII is mainly considered a subsidiary of the individual CI sectors.

Hacking Emergency Response Team (HERT) and the National High Tech Crime Center

In June 2002, the cyber-crime unit of the Dutch police (KLPD) founded a special response group to be activated in the case of an attack on the ICT part of a CI. The priorities of the Hacking Emergency Response Team (HERT) will be to restore CI services and assist in recovery and logistics while collecting evidence. In the course of its development and as a result of the multi-agency private partnership approach, its focus has shifted. In the end, the HERT initiative became part of the legal and operational framework of the Dutch National High-Tech Crime Center.[459]

456 http://www.govcert.nl/render.html?it=41.
457 http://www.minbzk.nl/uk.
458 http://www.waarschuwingsdienst.nl/render.html?cid=106.
459 http://www.nhtcc.nl/index_en.html.

Law and Legislation

Computer Crime Laws 1999

A new version of the computer crime law has been under development since 1999. The European Cybercrime Convention has been included in this new national law. The Computer Crime Law II is expected to be introduced in 2006.[460]

Telecommunications Law

This law states the requirements that must be met by public telecommunication operators regarding the capacity, quality, and other properties of the services offered (e.g., free access to the 112 emergency number), as well as regulations with respect to safety and privacy precautions regarding their network and services.[461]

Criminal Code

Article 138a:
Any person who intentionally and unlawfully accesses an automated system for the storage or processing of data, or part of such a system, is guilty of a breach of computer peace and shall be liable to a term of imprisonment not exceeding six months or a fine if they:

a) Break into a security system, or
b) Obtain access by a technical intervention, with the help of false signals or a false key, or by acting in a false capacity.

460 Information provided by Dutch expert.
461 http://www.verkeerenwaterstaat.nl/?lc=uk.

New Zealand

Critical Sectors

Critical information infrastructure protection (CIIP) in New Zealand is about the protection of infrastructure necessary to provide critical services. "Critical services are those whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement."[462] New Zealand's critical sectors comprise the assets and systems required for the maintenance of:[463]

- Emergency Services,
- Energy (including Electricity Generation and Distribution, and the Distribution of Oil and Gas),

* The Country Survey of New Zealand 2006 was reviewed by Richard Byfield and Mike Harmon, Centre for Critical Infrastructure Protection (CCIP).

462 http://www.ccip.govt.nz/about-ccip/niip-report-final.htm#_Toc501363182.

463 e-Government Unit, State Services Commission. Protecting New Zealand's Infrastructure from Cyber-Threats (8 December 2000). http://www.ccip.govt.nz/about-ccip/niip-report-final.htm.

- Finance and Banking,
- Governance (including Law and Order and National and Economic Security),
- Telecommunications and the Internet,
- Transport (including Air, Land, and Sea).

Various critical sectors depend on each other. Most systems assume the continuity of power and telecommunications infrastructures and make extensive use of networked information technology in their management and control systems.

Past and Present Initiatives and Policies

The New Zealand government's "Defence Policy Framework" is a crucial document that illustrates that CIIP is a key objective of the country's overall security policy. The Centre for Critical Infrastructure Protection (CCIP) addresses the cyber-threat aspects of that objective.

CIIP within the Defence Policy Framework

New Zealand's government promotes a comprehensive approach to security and aims to protect and maintain the country's physical, economic, social, and cultural security. In the government's Defence Policy Framework of June 2000, critical infrastructure protection is identified as one of the key objectives: "[…] to defend New Zealand and to protect its people, land, territorial waters, Exclusive Economic Zone, natural resources and critical infrastructure."[464]

Report on Protecting New Zealand's Infrastructure from Cyber-Threats

New Zealand's State Services Commission's e-Government Unit released the report "Protecting New Zealand's Infrastructure from Cyber-Threats"[465] on 8

464 Minister of Defence. The Government's Defence Policy Framework (June 2000), p. 4. http://www.executive.govt.nz/minister/burton/defence/index.html; http://www.defence.govt.nz/public_docs/defencepolicyframework-June2000.pdf.

465 Protecting New Zealand's Infrastructure from Cyber-Threats, op. cit.

December 2000. The report deals with the protection of New Zealand's critical infrastructure from cyber-crime and other IT-based threats. The report assessed levels of risk due to IT-based threats in finance and banking, transport, electric power, telecommunications and the internet, oil and gas, water, and critical state services that support national safety, security, and income.[466] The report made several recommendations such as:

- The establishment of a New-Zealand-based security-monitoring and incident-handling organization;
- Harmonization of computer-crime legislation with that of other nations (e.g., Australia, the US, Britain, and Canada);
- Adoption of specific IT security standards;
- Establishment of an ongoing cooperation program between owners of critical infrastructure and the government.[467]

Towards a Centre for Critical Infrastructure Protection (CCIP)

On 11 June 2001, the report "Towards a Centre for Critical Infrastructure Protection (CCIP)" was issued by the e-Government Unit.[468] It recommended that the government establish a Centre for Critical Infrastructure Protection. The argument was that the dependence of citizens and businesses on various infrastructure services, the vulnerability of IT systems, and the risks and possible damage caused in case of failure were increasing. Therefore, measures must be taken to ensure that infrastructure operators and government agencies are kept up to date on vulnerability and threat information: "The CCIP is proposed as an insurance measure in that it mitigates, for a low cost, a risk of a large loss."[469]

In the early stages of CCIP planning, the location of the new center was constrained by the need to give private-sector companies the confidence that their sensitive commercial and security information would be adequately safe-

466 Minister of State Services. Media Release on Cyber-Crime: "Government addressing cyber-crime and IT-Based Threats" (11 February 2001). http://www.ccip.govt.nz/about-ccip/media-release-cyber-crime.htm.

467 Protecting New Zealand's Infrastructure from Cyber-Threats, op. cit.

468 e-Government Unit, State Services Commission. Towards a Centre for Critical Infrastructure Protection (11 June 2001). http://www.ccip.govt.nz/about-ccip/ccip-final-report.htm.

469 Ibid., p. 5.

guarded, as well as by the need to provide a secure environment to adequately protect intelligence information that the CCIP had to be able to access. It was stated that "Overseas experience shows that the Centre should not be part of a law-enforcement agency, since this might reasonably focus on the pursuit of offenders, to the detriment of rectifying damage and of confidentiality."[470] The Government Communications Security Bureau was finally appointed based on cost- effectiveness as well as its significant IT security skills and its culture of security.[471]

Furthermore, the e-Government Unit acknowledged that CCIP would require timely access to classified intelligence, among other sources, in order to provide the best chance of a successful threat warning.[472]

Manual on Security in the Government Sector

The Interdepartmental Committee on Security issued a comprehensive and detailed manual in 2002 called "Security in the Government Sector", which took into account the Australian/New Zealand Standard AS/NZS ISO/IEC 17799:2001 "Information Technology – Code of Practice for Information Security Management" that deals with possible sources of threats to information and how to counter them. The manual's security guidelines are mandatory for government departments, ministerial offices, the New Zealand Police, the New Zealand Defence Force, the New Zealand Security Intelligence Service, and the Government Communications Security Bureau (GCSB). In the manual, the government requires that information important to its functions, its official resources, and its classified equipment be adequately safeguarded to protect the public and national interests and to preserve personal privacy.[473]

Furthermore, the manual proposes that overall responsibility for security should rest with a manager, the designated Departmental Security Officer (DSO). That person's duties should include formulating and implementing the general security policy and common minimum standards within the organization, issuing instructions on security, and serving as liaison with the

470 Cabinet Paper. Centre for Critical Infrastructure Protection (13 August 2001), pp. 5, 9–11: http://www.ccip.govt.nz/about-ccip/cabinet-paper.htm.
471 Ibid. See also: Towards a Centre for Critical Infrastructure Protection, op. cit, p. 2.
472 Towards a Centre for Critical Infrastructure Protection, op. cit., p. 9.
473 Department of the Prime Minister and Cabinet. Security in the Government Sector (2002). http://www.security.govt.nz/sigs/index.html.

Secretary of the Interdepartmental Committee on Security (ICS), the New Zealand Security Intelligence Service (NZSIS), and the GCSB for any special advice.[474]

Security Policy and Guidance Website

The security policy and guidance website (www.security.govt.nz) provides information on the government's activities in the area of information security. This website acts as a focal point for the publication of government information about security standards, procedures, and resources.[475]

Standards New Zealand (SNZ)

Standards New Zealand (SNZ)[476] promotes several standards specific to New Zealand, as well as a host of joint Australian/New Zealand and international standards. AS/NZS ISO/IEC 17799 Information Security Management provides an overview of factors to be considered and included in the protection of information and information systems.

Organizational Overview

Public Agencies

The Domestic and External Security Secretariat (DESS)

The main actor in charge of formulating New Zealand's security policy, including CIIP, is the Domestic and External Secretariat (DESS), which co-ordinates central government activities aimed at protecting New Zealand's internal and external security, including intelligence, counter-terrorism preparedness, emergency and crisis management, and defense operations. The DESS director provides timely advice to the prime minister on issues affecting the security of

474 Ibid., chapter 2.
475 http://www.gcsb.govt.nz/infosec/index.html.
476 http://www.standards.co.nz/default.htm.

New Zealand, including policy, legislative, operational, and budgetary aspects. DESS is the support secretariat for the Officials Committee for Domestic and External Security Co-ordination (ODESC).[477]

Officials Committee for Domestic and External Security Co-ordination (ODESC)

The Officials Committee for Domestic and External Security Co-ordination (ODESC) is chaired by the prime minister and makes high-level policy decisions on security and intelligence matters, including policy oversight in the areas of intelligence and security, terrorism, maritime security, and emergency preparedness. ODESC comprises chief executives from the Ministry of Foreign Affairs and Trade, the Ministry of Defence and the Defence Force, the New Zealand Security Intelligence Service, the Government Communications Security Bureau, the Police, the Ministry of Civil Defence and Emergency Management, the Treasury, and others when necessary.[478]

Interdepartmental Committee on Security (ICS)

The Interdepartmental Committee on Security (ICS)[479] is a sub-committee of the Officials Committee for Domestic and External Security Co-ordination (ODESC). It formulates and coordinates the application of all aspects of security policy and sets common minimum standards of security and protection that all government organizations must follow. In addition, the ICS provides detailed advice on information security matters to government and other organizations or bodies that receive or hold classified information.[480]

Centre for Critical Infrastructure Protection (CCIP)

The Centre for Critical Infrastructure Protection (CCIP) was established in 2001 to provide advice and support to public and private owners of CI, in order to protect New Zealand's critical infrastructure from cyber-threats. The CCIP is located within the Government Communications Security Bureau and has three main tasks:

477 http://www.dpmc.govt.nz/dess/index.htm.
478 Ibid.
479 http://www.security.govt.nz.
480 Security in the Government Sector, op. cit.

- To provide a round-the-clock vigilance and advice service to owners of critical infrastructure and to government departments;
- To analyze and investigate cyber-attacks; and
- To collaborate with national and international critical infrastructure organizations to improve awareness and communications regarding information technology security.[481]

Whereas the CCIP provides coordination, support, and advice on the ways in which information security can be maintained and improved, owners of critical infrastructures in the public and private sectors remain responsible for the security of their own systems.[482]

Government Communications Security Bureau (GCSB)

In 1977, the Combined Signals Organization was replaced by the current signals intelligence agency — the GCSB, which is a civilian organization. Its chief executive reports directly to the prime minister. The GCSB gives advice and assistance to New Zealand government departments and agencies concerning the security of information-processing systems.[483]

One of the GCSB's tasks is to ensure the integrity, availability, and confidentiality of official information through the provision of Information Systems Security (INFOSEC) services to departments and agencies of the New Zealand government, and to contribute to the protection of the critical infrastructure from IT threats.[484] The New Zealand Security of Information Technology (NZSIT) publications are therefore produced as guidelines for New Zealand government organizations in support of securing and protecting IT systems and associated information and services.[485] The CCIP is part of the Government Communications Security Bureau (GCSB).

481 http://www.ccip.govt.nz/about-ccip/about-ccip.htm.
482 Cabinet Paper: Centre for Critical Infrastructure Protection (13 August 2001). http://www.ccip.govt.nz/about-ccip/cabinet-paper.htm.
483 Domestic and External Security Secretariat. Securing our Nation's Safety: How New Zealand manages its security and intelligence agencies (December 2000). http://www.dpmc.govt.nz/dpmc/publications/securingoursafety/index.html.
484 http://www.gcsb.govt.nz/functions/index.html.
485 http://www.gcsb.govt.nz/publications/nzsit/index.html.

e-Government Unit

The e-Government Unit was established in July 2000 within the State Services Commission (a department of the New Zealand Public Service)[486]. The following projects are under the umbrella of this unit:

A Secure Electronic Environment (S.E.E.) for the protection of sensitive information within and among government agencies. A sub-project of the S.E.E. project is the development of a framework for authentication in accessing sensitive systems that are part of public key infrastructures. The intention is to develop minimum requirements and a framework for the accreditation of certification authorities;

The study "Protecting New Zealand's Infrastructure From Cyber-Threats" on the national critical infrastructure and its level of vulnerability to cyber-threats.

Public-Private Partnerships

New Zealand Security Association (NZSA)

The New Zealand Security Association (NZSA) was formed in 1972. It represents licensed and certificated persons providing services to government departments, state-owned enterprises, businesses, and private users. The NZSA has two member groups: Corporate members, who are individuals or companies engaged in the security industry, and associate members, who are individuals or companies involved or interested in security without offering the services to the public. Members of the latter category include government departments, insurance companies, airlines, banks, food distributors, area health boards, oil companies, etc.[487] Among the NZSA's main objectives are:

- To set minimum operating standards for members, and to develop and approve codes of practice;
- To co-operate with the police, government departments, and other organizations and agencies concerned with the safekeeping of people, property, and information in New Zealand;

486 http://www.ssc.govt.nz/display/home.asp.
487 http://www.security.org.nz/pages/members/main.htm.

- To provide information and advisory services, education, and training.[488]

Computer Society Special Interest Group on Security (NZCS SigSec)

The New Zealand Computer Society's Special Interest Group on Security (NZCS SigSec) is a forum for networking with others with an interest in IT security from within and outside government. It meets quarterly for a presentation and networking.[489]

Early Warning and Public Outreach

AusCERT

AusCERT[490] is the national Computer Emergency Response Team for Australia. It also provides significant support to New Zealand organizations. It is one of the leading CERTs in the Asia/Pacific region; it provides prevention, response, and mitigation strategies for members.[491]

AusCERT was founded as a commercial CERT for Australia before the New Zealand Centre for Critical Infrastructure Protection (CCIP) was formed. The CCIP has a working relationship with AusCERT, but also provides an early-warning service and a moderated mailing list through its website.

Several commercial organizations – including the New Zealand company Co-logic — also provide vulnerability alerts filtered and tailored for their customers.[492]

488 http://www.security.org.nz/Pages/education.htm.
489 http://www.security.org.nz/pages/home.htm.
490 See also the Country Survey on Australia in this book.
491 http://www.auscert.org.au.
492 http://www.cologic.co.nz.

Law and Legislation

Crimes Amendment Act 2003: Crime involving computers

The Crimes Amendment Act came into force in October 2003. It includes four new offenses relating to the misuse of computers and computer systems. These offenses are:

- Accessing a computer system for a dishonest purpose (Section 249);
- Damaging or interfering with a computer system (Section 250);
- Making, selling, or distributing or possessing software for committing a crime (Section 251);
- Accessing a computer system without authorization (Section 252).

The terms "access" and "computer system" are defined in Section 248.

The first two offenses carry a range of penalties depending on the seriousness of the offense, with a maximum of seven and ten years' imprisonment respectively, while the remaining offenses carry a maximum penalty of two years' imprisonment.

The Section 249 offense involves accessing a computer system directly or indirectly, either to obtain a benefit for oneself or to cause loss to another person, or with intent to do so. The essential element of the crime in either case is dishonesty or deception (which is separately defined in Section 240(2)).

The Section 250 offense involves intentional or reckless destruction, damage, or alteration of a computer system. In the most serious case, if this is done by a person who knows or ought to know that danger to life is likely to result, the section provides a maximum penalty of ten years' imprisonment. In cases where a person damages, deletes, modifies, or otherwise interferes with or impairs any data or software without authorization, or causes a computer system to either fail or deny service to any authorized users, the maximum penalty is seven years' imprisonment.

The key element of the Section 251 "sale, supply, or distribution" offense is that the person must either know that a crime is to be committed, or must promote the software in question as being useful for the commission of a crime, knowing that or being reckless as to whether it will be used for such a

purpose. In the case of the "possession" offense, the key element is intention to commit a crime.

In practice, the more significant of these two offenses is likely to be Section 252, which in effect makes computer "hacking" a criminal offense. The offense is simple unauthorized access, whether direct or indirect, to a computer system, knowing that or being reckless as to whether one is unauthorized to access that computer system.

Sections 253 and 254 contain qualified exemptions in respect of the Section 252 offense for the New Zealand Security Intelligence Service and the Government Communications Security Bureau respectively, where those organizations are acting under the authority of (in the case of the NZSIS) an interception warrant or (in the case of the GCSB) a computer access authorization issued under Section 19 of the GCSB Act 2003.[493]

493 http://www.cybercrimelaw.net/countries/new_zealand.html.

Norway

Critical Sectors

A central premise underlying the Norwegian CIIP policy concept is that the production of most goods and services depends in some way or other on information and communication technology (ICT) systems. This dependency may occur as part of the production process itself, or as part of the logistics of making goods or services available to consumers. ICT forms an important part of the production of goods and services in a number of critical sectors of society. In Norway, the critical sectors are the following:[494]

- Banking and Finance,
- Central Government Administration,
- (Tele-) Communications,
- Defense,

* The Country Survey of Norway 2006 was reviewed by Stein Henriksen, Directorate for Civil Protection and Emergency Planning (DSB), and Laila Berge and Dagfinn Buset, Ministry of Justice and the Police.

494 Ministry of Trade and Industry. Society's Vulnerability due to its ICT Dependence – Abridged Version of the Main Report (Oslo, October 2000), pp. 9–10.

- Energy and Utilities,
- Oil and Gas Supply,
- Police,
- Public Health,
- Rescue Services,
- Social Security,
- Transport,
- Water Supply and Drainage.

Rapid technological development, deregulation, globalization, interdependencies, the lack of expertise, and outsourcing of manpower and systems have been identified as the main challenges to society concerning information infrastructure.[495]

Norway's CIIP policy is based on the following goals: CII must reach a level of robustness that ensures the functioning of important services to society during a "normal" peacetime situation. In times of crisis or war, the infrastructure must be sufficiently robust to maintain functionalities that are critical for society. Due to the wide range of threats against society and the challenges to many CII sectors, the government has initiated several relevant measures such as the security part of eNorway, the ITSEC (IT Security) National Strategy, the Government Initiative (Warning System for Digital Infrastructure, VDI), and the Center for Information Security (SIS).[496]

Past and Present Initiatives and Policies

Over the past few years, and as a result of technological developments, there has been an increased focus on CIIP. CIIP has been regarded as a security issue in Norway since the end of the 1990s. In fact, CIIP was placed on the political agenda by the government commission on "A Vulnerable Society". The Ministry of Trade and Industry, on the other hand, perceives CIIP as an economic issue.[497] Moreover, US policy has been an important trigger in

495 Ministry of Trade and Industry. Information and Infrastructure Protection – a Norwegian View (no date). http://www.ntia.doc.gov.

496 Report No. 17 to the parliament (2000–2001).

497 Information provided by a Norwegian expert of the Directorate for Civil Protection and Emergency Planning (DSB), March 2002.

putting CIIP on the political agenda in Norway as a political, security, and economic issue.[498]

Policy Statements

In 1998, the State Secretary Committee for ICT[499] formed a subcommittee with a mandate to report on the status of ICT vulnerability in Norway. Furthermore, the importance of CIIP is also stressed by the "Defense Review 2000" and the "Defense Policy Commission 2000".[500] In the aftermath of 11 September 2001, the government considered it necessary to increase national safety and security, particularly within civil defense, in the Police Security Service, and in emergency planning within the health sector.[501]

Commission on a Vulnerable Society

The governmental commission on "A Vulnerable Society" was established by royal decree on 3 September 1999. It was active from 1999 until 2000. The findings gave important input to the national planning process.[502] The commission's task was to study vulnerabilities in society with a broad perspective. The mandate was to assess the strengths and weaknesses of current emergency planning, to assess priorities and tasks, and to facilitate increased awareness, knowledge, and debate about vulnerabilities.

The government commission identified several focus areas. One of these was CI.[503] In its green paper, "NOU (2000:24) – A Vulnerable Society",[504] the commission placed great emphasis on the significance of ICT for the vulnerability of society in general. The commission, in what was probably its most controversial proposal, recommended that responsibility for safety, security,

498 Information provided by a Norwegian expert of the Directorate for Civil Protection and Emergency Planning (DSB), March 2002.
499 "Statssekretærutvalget for IT – SSIT".
500 Information provided by Norwegian expert.
501 Report no. 17 to the Storting (2000–2001).
502 Information provided by Norwegian expert.
503 Hovden, Jan. Public policy and administration in a vulnerable society. (Norwegian University of Science and Technology and the Norwegian Academy of Science and Letters, Center for Advanced Study, June 2001). http://www.delft2001.tudelft.nl/paper%20files/paper1074.doc.
504 http://odin.dep.no/jd/norsk/dok/andre_dok/nou/012001-020005/dok-bn.html.

and emergency planning should be concentrated in one single ministry.[505] Furthermore, a strategy based on the following pillars was proposed:[506]

- Partnership between the public and private sectors;
- Promotion of information exchange;
- Establishment of an early-warning capacity;
- Harmonization and adjustments of laws and regulations;
- Public responsibility for CIP.

ICT Vulnerability Project

The "ICT Vulnerability Project"[507] was an interdepartmental group commissioned by the Ministry of Trade and Industry in 1999. The project collaborated with the government commission on "A Vulnerable Society", and the two groups coordinated their findings on ICT vulnerabilities.[508] In the "ICT Vulnerability Project", each sector authority evaluated the risks linked to specific functions in that sector.[509] This project resulted in the publication of the National Strategy for Information Security in 2003.

eNorway (eNorge) 2005 Action Plan

In May 2002, the government presented the "eNorway (eNorge) 2005 Action Plan", which describes the needs, responsibilities, and action required for the development of an information society.[510] With "eNorge", the government ensures that the country has equally ambitious objectives as those formulated by the EU in the "eEurope Plan".[511] "eNorge" deals predominantly with the furtherance of e-government and e-business.

505 Ibid.
506 Ibid.
507 Society's vulnerability, op. cit., p. 10.
508 Dependability Development Support Initiative (DDSI). European Dependability Policy Environments, Country Report Norway (April 2002 version).
509 A common feature of these evaluations is that each individual sector operation is dependent on its own ICT user systems as well as on the public telecommunications services. Therefore, robust access to telecommunications seems to be very important to most sectors. The telecommunications services are dependent on ICT.
510 DDSI, Country Report Norway, op. cit.
511 National Strategy for Information Security, op.cit. http://www.odin.dep.no/archive/nhdv-edlegg/01/06/Nasjo006.pdf.

Safety and Security of Society

On 5 April 2002, the Ministry of Justice and the Police presented its 17th report on the "Safety and Security of Society" to the Norwegian Storting (parliament). The report is a comprehensive statement of the government's proposals regarding the reduction of vulnerabilities in modern society and measures to increase safety and security in the future. It states that when assessing the vulnerability of society, it is important to "consider the consequences of lapses in CI, such as a lapse in the distribution of power or a lapse in telecommunication".[512] The recommendations laid the basis for new government measures, including most importantly the formation of the new Directorate for Civil Protection and Emergency Planning (DSB), established on 1 September 2003.[513]

National Strategy for Information Security

The Ministry of Trade and Industry published a national strategy for securing ICT systems in Norway in June 2003[514] that proposed several initiatives for improving security based on the "OECD Guidelines for the Security of Information Systems and Networks". The strategy involves all aspects of ICT security, ranging from security for individuals, businesses, and the daily activities of the government to the security of IT-dependent critical infrastructure.

The Norwegian national authorities started implementing the suggested measures in the autumn of 2003. One recommendation, the establishment of a Center for Information Security (SIS), has already been carried out. Other initiatives include the establishment of a coordination committee for ICT security and campaigns to raise awareness of challenges and problems related to the use of ICT systems.[515]

512 Report No. 17 to the Storting (2000–2001). Statement on Safety and Security of Society (Summary) (April 2002).

513 http://www.dsb.no/forside.asp.

514 Justice and Police Department. National Strategy for Information Security (June 2003; in Norwegian). http://www.odin.dep.no/archive/nhdvedlegg/01/06/Nasjo006.pdf.

515 http://www.norsis.no.

Organizational Overview

Public Agencies

In Norway, the ministry or authority that has the responsibility for an area during peace or non-crisis times also has the responsibility during times of crisis and war. This system also applies to CIIP. The coordinating authority on the civilian side is the Ministry of Justice and Police. The overall authority for ICT security is the Ministry of Modernization, which took over this task from the Ministry of Trade and Industry, while the Ministry of Defense is responsible on the military side. The Ministry of Transport and Communications has responsibility for the communication sector in Norway, including all related security issues. The directorates and authorities that are responsible for handling the various aspects of CIIP on behalf of the ministries are answerable to the respective ministries.[516]

A Unit on Telecom Infrastructure Security has been established at the Post and Telecommunications Authority. In the future, the Ministry of Justice will have a greater coordinating role regarding security in civilian society, which will require several steps towards a reorganization of the civilian agencies.[517]

Directorate for Civil Protection and Emergency Planning (DSB)

The Directorate for Civil Protection and Emergency Planning (DSB)[518] was established on 1 September 2003, replacing the former Directorate for Civil Defense and Emergency Planning and the Directorate for Fire and Electrical Safety.

The new DSB is subordinate to the Ministry of Justice and Police, and its main task is to serve as a center of resources and expertise for emergency contingency planning. The DSB is a point of contact between the central authorities and regional commissioners during disasters occurring in peacetime.

516 Information provided by a Norwegian expert from the Directorate for Civil Protection and Emergency Planning (DSB), 2003.

517 Information provided by a Norwegian expert from the Norwegian Ministry of Trade and Industry, June 2002.

518 http://www.dsb.no/forside.asp.

To ensure adequate preparedness measures in the community, the DSB devotes considerable efforts to ensure that all Norwegian municipalities carry out risk and vulnerability analyses. The DSB works to ensure that activities involving preparedness responsibilities lead to the implementation of internal control systems to ensure the quality of emergency planning at local government level. The DSB also supervises the planning efforts in the ministries and offices of the regional commissioners.

In the context of CIIP, the DSB coordinates and carries out research on vulnerabilities and the protection of critical assets in cooperation with other actors.

Norwegian National Security Authority (NSM)

The Norwegian National Security Authority (NSM)[519] was established on 1 January 2003 and coordinates preventive IT-security measures. It controls the level of security, e.g. of central and local public administration, and monitors private suppliers of goods and services to the public when the products or services concerned are security-sensitive. The NSM also develops technical and administrative security measures and issues threat evaluations and vulnerability reports. The Ministry of Defense funds and administers the NSM. Moreover,

- The NSM hosts SERTIT, a public Certification Authority for IT Security in Norway.
- The Warning System for Digital Infrastructures (VDI), a network between major private and public infrastructure operators and intelligence services, is part of the NSM.
- Within the NSM, a "NorCERT" is planned as an effort to explore a concept for establishing a National CERT.

The National Information Security Co-ordination Council (KIS)

The National Information Security Co-ordination Council (KIS) was established in May 2004. It is chaired by the Ministry of Modernization and consists of representatives from seven ministries, the Prime Minister's Office,

519 http://www.nsm.stat.no.

and nine different directorates. KIS discusses national security and CIIP from an IT-security perspective. Its task is to supervise the strategic orientation and overall consistency of governmental IT policies. Topics addressed in the KIS include IT security, national security (interests), critical infrastructure, common standards, working methods for IT security, risks and vulnerabilities, and IT-security legislation as well as monitoring activities. The KIS keeps track of the strategic orientations presented in the National Strategy for Information Security.[520]

Commission for the Protection of Critical Infrastructures in Norway

The Norwegian CIP commission defines and identifies critical infrastructures in Norway, and assesses different means for protecting critical infrastructures. Among other reasons, this has been considered necessary due to challenges caused by privatization and exposure to the market. The private sector's responsibility for critical infrastructure is significant, and so is the public's dependency on the goods and services that the market provides. It is important to ensure that the private sector upholds its social responsibility to protect and secure the critical infrastructure to a degree that ensures the national security and other interests that are of vital importance to the nation.

In order to establish a comprehensive evaluation of CIP in Norway, the government established a commission for the protection of critical infrastructure in October 2004. The commission consists of members from a wide range of sectors and with different fields of expertise. The commission has the following tasks:

- Identify activities that ensure the interests of national security and other interests that are considered vital to the nation; in other words, identify critical infrastructure;
- Identify and assess measures to protect critical infrastructure;
- Assess all actors for critical infrastructure;
- Assess which infrastructures the government should own completely or in part;

520 Buset, Dagfinn. "Civil Protection in Norway", presentation held at the Workshop on Critical Infrastructure Protection and Civil Emergency Planning: Dependable Structures, Cybersecurity, and Common Standards, 9–11 September 2004 in Zurich. http://www.eda.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/cybsec/buset.html.

- Consider the administrative and financial consequences of the proposals;
- Report to the Ministry of Justice and the Police no later than January 2006.

Public-Private Partnerships

The most important public-private initiatives in Norway are the Center for Information Security (SIS) and the Warning System for Digital Infrastructure (VDI) project.

Center for Information Security (SIS)

The Norwegian government decided some years ago to establish a Center for Information Security (SIS). In 2001, a pilot study was commissioned to investigate options for the establishment of this center.[521]

SIS is now responsible for coordinating activities related to information and communication technology security in Norway. This includes the exchange of information, competence, and knowledge about threats and countermeasures, and generation of a holistic threat picture.[522] The clients of the SIS are government agencies, security services, politicians, and private enterprises, offering a broad basis for assessing the status of national security. SIS has recently been moved away from the UNINETT system (see section on early warning) in Trøndheim to the IT-specific research college of Gjøvik.

Warning System for Digital Infrastructure (VDI)[523]

At the beginning of the new millennium, several agencies and business actors began cooperating with the Norwegian intelligence and security services to prevent computer crimes. The Warning System for Digital Infrastructure (VDI) is an initiative by the government intended to enable security professionals to chart the extent of the threat to vulnerable information infrastruc-

521 Dependability Development Support Initiative (DDSI). Public-Private Co-operation: Business Governmental Actions Towards Achieving a Dependable Information Infrastructure in Europe. Issues and background paper for the DDSI workshop on Public-Private Co-operation (Stockholm, 6–7 June 2002), p. 10.

522 Henriksen, Stein. "National Approaches to CIP: Norway". ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead (Zurich, 8–10 November 2001).

523 Ibid.

ture through the use of intrusion detection systems (sniffers). The project was a cabinet reaction to the commission on "A Vulnerable Society" and the Ministry of Trade and Industry report in the summer and autumn of 2000. The VDI will alert clients to breaches and attempted breaches of computer networks. Each client is free to report the incident to the police. Due to the success of the project, the government wants to prolong it. The success of the VDI is, to a great extent, attributed to its control structures, which alleviate possible concerns about business privacy and other issues. VDI co-ordination has moved to the National Security Agency.

Early Warning and Public Outreach

UNINETT CERT

UNINETT CERT is the Norwegian computer emergency response team and an academic network for research and development. It was formed in 1995. The constituency are the Norwegian state universities, colleges, and research and development institutions.[524] The team was created to contribute to better internet security for UNINETT member institutions, and to serve as a focal point for security issues regarding UNINETT member institutions.[525] The basic duty of UNINETT CERT is to provide assistance on handling and investigating incidents involving one or more members of the constituency. Examples of incidents are spamming, suspicious port-scanning, and denials of service.[526]

524 DDSI, Country Report Norway, op. cit.
525 http://cert.uninett.no/policy.html.
526 http://cert.uninett.no/policy.html.

Law and Legislation

Norwegian Penal Code

Penal Code, Paragraph 145

Any person who unlawfully opens a letter or other closed document or in a similar manner gains access to its contents, or who breaks into another person's locked depository, shall be liable to fines or to imprisonment for a term not exceeding six months.

The same penalty shall apply to any person who, by breaking a protective device or in a similar manner, unlawfully obtains access to data or programs that are stored or transferred by electronic or other technical means.

If damage is caused by the acquisition or use of such unauthorized knowledge, or if the felony is committed for the purpose of obtaining for any person an unlawful gain, imprisonment for a term not exceeding two years may be imposed.

Accomplices shall be liable to the same penalty.

Public prosecution will only be pursued if required in the public interest.

Penal Code, Paragraph 151b

Paragraph 151b of the Penal Code states that whosoever causes comprehensive disturbances to the public administration or other parts of society by disrupting the collection of information, or by destroying or damaging power supply plants, broadcasting facilities, telecommunications services, or other kinds of communication, will be punished by a maximum of ten years' imprisonment. Unlawful negligence will be punished by incarceration for a maximum of one year. Accessories will be punished in the same manner. This law came into effect on 12 June 1987.[527]

Penal Code, Paragraph 291

Any person who unlawfully destroys, damages, renders useless, or wastes an object that wholly or partly belongs to another shall be guilty of vandalism.

The penalty for vandalism shall be fines or imprisonment for a term not exceeding one year. An accomplice shall be liable to same penalty.

527 Information provided by Norwegian expert.

Public prosecution will only be pursued if requested by the aggrieved party, unless it is required in the public interest.

On 4 November 2003, the cyber-crime committee presented to the Ministry of Justice a proposal for a new provision in the Penal Code, which was enacted on 8 April 2005 by Act 16:

Penal Code, Paragraph 145b

Any person who unlawfully makes available a computer password or similar data, by which the whole or any part of a computer system is capable of being accessed, shall be sentenced for spreading of access data, to a fine or imprisonment not exceeding six months or both.

Serious spreading of access data shall be punishable by imprisonment not exceeding two years. In deciding whether the spreading is serious, special consideration shall be given to whether the data may allow access to sensitive information, whether the spreading is extensive, and whether the conduct causes a danger of creating considerable damage in other respects.

An accomplice shall be liable to the same penalty.

Public prosecution will only be pursued at the request of an aggrieved party, or if deemed necessary in the public interest.[528]

On 4 March 2005, the Chamber in the Parliament (Stortinget) recommended an act amending the Penal Code and the ratification of the Council of Europe Convention on Cybercrime.[529]

528 http://www.cybercrimelaw.net/countries/norway.html;http://www.stortinget.no/cgi-wift/wiftldles?doc=/usr/www/stortinget/beso/beso-200405-048.html&titt=datakriminalitet&ting=beson+besog+belsn+beslg&sesjon=*&.

529 http://www.cybercrimelaw.net/countries/norway.html;http://www.stortinget.no/cgi-wift/wiftldles?doc=/usr/www/stortinget/beso/beso-200405-048.html&titt=datakriminalitet&ting=beson+besog+belsn+beslg&sesjon=*&.

Russia

Critical Sectors

During the last few years, Russia has made significant progress in improving its information infrastructure. The national security and economic welfare of the Russian Federation depends to a substantial degree on ensuring information security, a dependence that will increase in future with technological progress.

The criticality of the following sectors can be inferred from the "Information Security Doctrine of the Russian Federation",[530] which identifies the types of threats to the Russian information infrastructure.

- Domestic Industry, especially National Information Industry,
- Information Backing of State Policy in the Russian Federation,
- Information and Telecommunications Systems[531],

* The Country Survey of Russia 2006 was reviewed by Anatoly Streltsov, Professor at the Institute of Information Security, Lomonosov Moscow State University. We are also grateful to Martin Wählisch, Humboldt University Berlin, for his extensive research assistance and translation of Russian documents.

530 See next chapter for details.

531 Also including: information and accounting computerized systems (in the federal government agencies, as well as accounting at enterprises, institutions, and organizations); systems of collecting, processing, storing and transmission of financial exchange, tax and customs information, and information on foreign economic activities; systems of controlling sophisticated research complexes (nuclear reactors, particle accelerators, plasma generators, and others).

- Mass Media,
- Credit and Financial System,
- Transportation Infrastructure (especially Rail and Shipping),[532]
- Energy (Gas, Oil, Electricity),
- Military Infrastructure (especially Missile Defense and Space).

In Russia, CIIP is defined more broadly than in most other countries listed in this Handbook. Information assurance includes not only (technical) information security, but also restrictions on the free flow of information and information exchange (especially information that may harm the state), and the safeguarding of state secrets. Besides the physical or virtual information systems and flows, the state wants to protect the content of the information.

Past and Present Initiatives and Policies

Information Security Doctrine of the Russian Federation

The "Information Security Doctrine"[535] of the Russian Federation, adopted on 9 September 2000, is an extension of the "National Security Concept"[536] (approved by President Vladimir V. Putin on 10 January 2000) intended to strengthen the state policy regarding information security. Its aim is to help formulate legal, methodological, technical, and organizational provisions for information security in Russia and to assist the development of specific programs for this purpose. The doctrine defines the context of the nation's interests in the information sphere and assesses information threats to citizens, society, and the state. The doctrine is very comprehensive in scope and ranges over many policy areas, from data protection, personal privacy, copyright and computer misuse (hacking) to state secrets, access to information, and control of the

532 Ignatyev, Mikhail B. Analysis of the Threat of Cyberattacks to Major Transportation Control Systems in Russia. "Terrorism: Reducing Vulnerabilities and Improving Responses - U.S.-Russian Workshop Proceedings" (2004). http://www.nap.edu/openbook/0309089719/html/85.html#pagetop.

535 Doctrine of the Information Security of the Russian Federation. Approved by the President of the Russian Federation, Vladimir Putin (9 September 2000), No. Pr-1895. http://www.medialaw.ru/e_pages/laws/project/d2-4.htm.

536 http://www.kremlin.ru/eng/articles/institut04.shtml.

media. Inevitably, considering this broad spectrum, the policy is occasionally rather vague. It lacks concrete examples of specific reforms to address the various dangers and shortcomings that it identifies.[537]

The Information Security Doctrine of the Russian Federation reflects the G8 "Okinawa Charter of the Global Information Society", which was also prepared in the year 2000. However, in the Russian Information Security Doctrine, the specific social and economic circumstances and long-term reforms of the Russian Federation as well as its experience with terrorist attacks were taken into consideration.

Russian information security is defined in the doctrine as "the state of protection of its national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the state." Russia views both the minds of citizens and the national information systems as integral parts of its concept of information security.[538] Moreover, the uncontrolled spread of foreign media in Russia is considered as one of the threats to Russian information security and, as a result, the government intends to strengthen the state-owned media.[539]

The doctrine is legally based on Russian federal laws on security, state secrets, the protection of information, and participation in international information exchange. The document is divided into four major chapters, covering eleven sections. The for main chapters are:

1 Information security: This chapter defines the Russian Federation's national interests in the information sphere, referring to constitutional rights, to information backing for state policy, to the development of the information industry, and to the security of information against unauthorized access. Moreover, internal and external sources of threats to Russia's information security are identified. The doctrine acknowledges frankly that just like private monopolies and organized crime, government policy and legislation can also pose a threat. Aggressive foreign corporations and international terrorists are mentioned

537 Leigh, Ian. Information Security Doctrine of the Russian Federation (no date). http://www.isn.ethz.ch/news/dossier/ssg/pubs/books/FluriSulakshin/05A_LEIGH.pdf.

538 Thomas, Timothy L. Information Security Thinking: A Comparison of U.S., Russian and Chinese Concepts (July 2001). http://fmso.leavenworth.army.mil/documents/infosecu.htm.

539 This aspect of Putin's doctrine has been criticized by journalists who fear restrictions on freedom of opinion and speech. Albats, Yevgenia. "Information Security Doctrine Redux". In: The Moscow Times, 14 September 2000. http://dev.themoscowtimes.com/stories/2000/09/14/007.html.

as major foreign threats. In the domestic arena, the critical state of the national industry as well as the under-development of the legal framework can constitute a barrier to full exploitation of information technology, particularly where e-commerce is concerned. Finally, the chapter discusses the state of information security in the Russian Federation and objectives for amending it. The deteriorating safety of data constituting state secrets is identified as a major problem.

2 Methods of ensuring information security: This chapter covers legal, organizational-technical, and economic methods of CIIP. Moreover, it describes a number of features of information security in various spheres, such as the economy, domestic policy, foreign policy, science and technology, information and telecommunication systems, defense, law enforcement, and emergency situations. Finally, it mentions international cooperation in the field of information security such as banning information weapons, supporting information exchanges, coordinating law enforcement activities, and preventing unsanctioned access to confidential information.

3 The main provisions of the state policy for ensuring information security, and priority measures for implementing it: This chapter lays out – at a high level of abstraction — the policy of the government, ranging from observing the constitution to supporting the development of new technologies. The chapter suggests provisions for information security, such as developing guidelines for federal institutions. In addition, priority measures for implementing the rule of law, an increase in the efficiency of state leadership, programs providing access to information archives, a system of training, and for harmonizing standards in the field of computerization and information security are mentioned.

4 Organizational basis of ensuring information security: This chapter describes the functions of the system of information security, as well as the organizational elements and actors of Russia's information security system, including the president, the Federation Council of the Federal Assembly, the State Duma of the Federal Assembly, the government of the Russian Federation, the Security Council, and other federal executive authorities, presidential commissions, judiciary institutions, public associations, and citizens.

An area of obvious emphasis is the creation of a legal base for information security. The laws on the "Constitution of the Russian Federation", "State Secrecy", "Information, Computerization, and Information Protection", "Participation in International Information Exchange", and "Essentials of Legislation of the Russian Federation on the Archive Collection of the Russian Federation and Archives" are specifically mentioned. Legal instruments constitute one of three approaches to information security mentioned in the doctrine — the other two being organizational-technical and economic measures.[540]

Electronic Russia

The idea of "Electronic Russia"[541] appeared in early 2001, when the Ministry of Economic Development and Trade was elaborating a strategic development plan for Russia up to the year 2010. The program is based on the notion that in order to reduce the economic lag, it is necessary to develop the hi-tech sector, where it would be possible to reach a higher productivity level than in the raw-materials sector. None of this would be possible without computers and powerful ICT.[542]

Involving various ministries[543] and coordinated by the Ministry of Telecommunications and Informatization, Electronic Russia 2002–2010 is

540 Timothy, op. cit. http://fmso.leavenworth.army.mil/documents/infosecu.htm.

541 Federal Target Program "Electronic Russia (years 2002–2010)". Approved by the government of the Russian Federation (decree no. 65 of 28 January 2002). http://www.developmentgateway.org/download/182707/erussia_final_en_jr28-02.doc.

542 All cities in Russia with populations over 30,000 should soon be connected to the country's "fiber-optic backbone", although the connections to individual homes and offices can still be relatively primitive. Many thousands of villages in Russia still do not have a single telephone line, so it will be many years before some of the more sparsely populated areas can hope to have a fully operational telecommunications infrastructure. Many options are under consideration to provide this infrastructure, including satellite delivery. The Electronic Russia plan seeks to deliver an increasing number of government services online, and to alleviate some of the heavy bureaucratic burden on Russia's citizens and businesses. It will then be possible to perform tasks such as tax filing and business registration online.The country's vast geographic area and the financial difficulties of the education system have encouraged Russian planners to seek creative solutions to the provision of education throughout the country. The delivery of a wide range of distance-learning packages via the internet is seen as a potentially effective solution to this problem, which the Electronic Russia plan seeks to explore. http://www.tiaonline.org/policy/regional/nis/eRussia.cfm, and http://www.e-rus.ru.

543 Ministry of Economic Development and Trade, Ministry of Education, Ministry of Industry, Science and Technologies, Aviation and Space Agency, Federal Agency of Government Communications and Information with the President, Agency on Systems Management.

the core IT program that will lay the groundwork for a more efficient economy and public administration through mass implementation of information and telecommunications technology.[544] It is also designed to facilitate by technological means the advancement of civil institutions by securing the right of citizens to unrestricted information access, and by expanding IT training opportunities for specialists and qualified users.[545]

Electronic Russia has a nine-year planning horizon and addresses four key areas:

- Regulatory environment and institutional framework,
- Internet infrastructure,
- e-Government,
- e-Education.

The main objective of Electronic Russia is to increase the efficiency of the economy, to improve management in the public sector, and to enhance self-government by applying information and communication technologies. In order to reach this goal, the following tasks are addressed:

- To create effective legislation governing ICT;
- To ensure open communication and interaction between the state bodies, agencies, and companies by applying state-of-the-art ICT technologies;
- To create conditions for more extensive and more effective use of ICT in the economic and social spheres;
- To provide up-to-date computer training for professionals;
- To create incentives for the development of an independent press and media by employing ICT in their professional activities;
- To develop the infrastructure of telecommunication networks, as well as access to electronic libraries, archives, databases of scientific and technical information for citizens, state-owned organizations, and educational institutions;
- To support the establishment of e-commerce for state procurement and other commercial activities of the state.[546]

544 http://www.uni-koblenz.de/~kgt/PM/SemB/Russland.ppt.
545 http://www.bisnis.doc.gov/bisnis/bisdoc/011001E-Russia.htm.
546 Electronic Russia, op. cit., p. 3–4; and http://www.tiaonline.org/policy/regional/nis/eRussia.cfm.

Electronic Moscow

One of the regional branches of the Electronic Russia Program is the city program "Electronic Moscow".[547] This program, announced on 24 December 2002, aims to strengthen Moscow's role as the information industry center of Russia. The program is based on the city's powerful telecommunication infrastructure – the "Moscow Fiber Optic Network". The issues addressed by e-Moscow include the creation of a normative and legal basis for the information society; a more efficient city management, based on e-government; developing the urban economy and overcoming information inequality within the city; building a interoperability framework; and integrating all existing ICT projects of the municipal authorities.[548]

International Cooperation

International cooperation is an important component of the Russian Federation's efforts in the field of ensuring information security. Russia's international cooperation in ensuring information security has two distinctive features: International competition for the possession of technological and information resources and for dominance in the markets has increased, and the main world powers have achieved a growing technological lead that allows them to build up their potential for creating an "information weapon". Russia views this development with concern, as it could lead to a new arms race in the information sphere and raises the threat of foreign intelligence services penetrating Russia through agents and using operational-technical means, such as a global information infrastructure. Therefore, the main areas of the Russian Federation's international cooperation in the field of information security are:

- Banning the development, proliferation, and application of "information weapons";

547 http://mgd.iis.ru.

548 Filippov, Sergey. Policy for ICT Adoption in Moscow ("Electronic Moscow" Programme) (no date). http://www.telecities.nl/call_for_papers/paper_sergey_filippov_-_electronic_moscow.pdf.

- Ensuring the security of international information exchange, including the security of information being transmitted via national telecommunications channels;
- Coordinating the activities of law-enforcement bodies worldwide for preventing computer crime;
- Preventing unauthorized access to confidential information in international banks, telecommunications networks, and information support systems that are indispensable for maintaining global trade; and sharing information with international law-enforcement organizations;
- Active participation of Russia in all international organizations active in the field of information security, including standardization and certification.[549]

In compliance with UN General Assembly Resolution No. 58/32 of 8 December 2003, a Federal Expert Group on international information security was organized, chaired by a Russian representative.[550] The Federal Expert Group includes representatives of 15 countries.[551] Furthermore, the Russian government has special partnerships with the US,[552] China,[553] and Germany in the sphere of information security.

Organizational Overview

Public Agencies

The main organizations responsible for information security in Russia are the Security Council of the Russian Federation, the Federal Security Service of the

549 http://www.medialaw.ru/e-index.html.

550 Kremer, Arkadiy. "Cyber Security in Russia". Presentation held at ITU-T Cybersecurity Symposium (Florianopolis, Brazil, 4 October 2004). http://www.itu.int/ITU-T/worksem/cybersecurity/presentations/CsecS2-p2-kremer.ppt.

551 United Kingdom, China, Russia, France, Belarus, Brazil, Germany, India, Jordan, Malaysia, Mali, Mexico, South Korea, and South Africa.

552 http://www.russlandonline.ru/rupol0010/morenews.php?iditem=4185; http://books.nap.edu/books/0309089719/html/index.html; http://books.nap.edu/books/0309089719/html/146.html#pagetop.

553 http://www.greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=005YM3.

Russian Federation (FSB), the Federal Guard Service of the Russian Federation, the Federal Technical and Export Control Service as well as the Ministry of Information Technologies and Communications.

Security Council of the Russian Federation

The Security Council of the Russian Federation[554] is appointed by the president in accordance with the constitution and the Federal Law on Security. It is responsible for ascertaining Russia's national information related interests and defines information resources that must be defended. The Security Council defines conceptual approaches to national security.[555] It drafts policy proposals on defending the vital interests of individuals, society, and the state against internal or external threats. The Security Council also coordinates the elaboration of a strategy for the Russian Federation's information security, and helps the president to carry out his constitutional duties in defending human and civil rights, as well as Russia's sovereignty, independence, and territorial integrity.[556]

Federal Security Service of the Russian Federation (FSB)

According to its statute, the Federal Security Service of the Russian Federation (FSB; formerly known as the KGB)[557] is a federal agency of the executive branch of government with a mandate to safeguard the security of the Russian Federation. This includes defending and protecting the state borders of the Russian Federation, internal waterways, the territorial waters, the exclusive economic zone, and the continental shelf and their natural resources, and safeguarding the information security and the main areas of activity of agencies of the Federal Security Service, as defined in the laws of the Russian Federation.[558]

As far as technical support is concerned, the FSB has its own research institute specializing in information technologies. It carries out technical in-

554 http://www.scrf.gov.ru.
555 http://www.kremlin.ru/eng/articles/institut04.shtml.
556 http://www.fas.org/irp/world/russia/docs/edict_1024.htm.
557 http://www.fsb.ru.
558 Text of the Statute on the Federal Security Service of the Russian Federation and Structure of the Federal Security Service Agencies. Approved by presidential edict no. 960 of 11 August 2003, signed by V. Putin, President of Russian Federation. http://www.fas.org/irp/world/russia/fsb/statute.html.

formation assessments, particularly regarding criminal cases.[559] It is also responsible for cases of cyber-terrorism.[560] The FSB Computer and Information Security Directorate (Directorate-R) was established in October 1998. The Directorate's main tasks are counterintelligence and the fight against cybercrime. Since undergoing a minor reform in September 2004, the FSB has a new structure. The Computer and Information Security Directorate is part of its counterintelligence service.[561]

Among the fundamental objectives of the FSB in the field of information security are the planning and implementation of state and scientific-technical policy in the sphere of information security; the organization of support for the cryptographic and technical engineering security of information and telecommunications systems; and protecting state secrets as well as systems of encrypted, classified, and other special types of communications in the Russian Federation and in its institutions abroad. Another function is to certify equipment for the protection of information, telecommunications systems, and networks, as well as technical devices for the detection of electronic surveillance in buildings and technical equipment, in accordance with federal law.[562]

Federal Guard Service of the Russian Federation

According to its statute, the Federal Guard Service of the Russian Federation is a federal body of the executive branch of government with a public mandate to shape state politics and legal regulations, as well as to conduct monitoring and surveillance to ensure the safety of the president of the Russian Federation, the chairman of the government of the Russian Federation, and other important public figures. A new structure — the Special Communication and Information Service — was added in August 2004 as a result of the administration reform of the Federal Guard Service of the Russian Federation.[563]

559 Ibid.

560 http://www.russia-gateway.ru/content/NEWS/NewsItem_2376921.jsp.

561 http://www.agentura.ru/english/dosie/fsb/structure; http://www.agentura.ru/english/press/about/jointprojects/mn/fsbreform.

562 Statute on the Federal Security Service of the Russian Federation, op. cit.

563 Decree of the President of the Russian Federation No. 1013 of 7 August 2004: "Issues of the Federal Guard Service of the Russian Federation" (with Amendments and Additions of 28 December 2004, 22 March and 1./6. October 2005). http://egarant.park.ru/rubric.jsp?urn=1192285580.

Until 2004, the Federal Agency for Government Communications and Information (FAPSI), another former KGB branch,[564] was the main responsible body for information security. FAPSI was abolished in 2004 and its functions distributed between the Federal Security Service (FSB), the Foreign Intelligence Service, and Federal Guard Service of the Russian Federation. FAPSI was responsible for ensuring the security of communications;[565] the cryptographic and technical security of encrypted communications; intelligence-gathering activities, and providing information to higher bodies of authority.[566]

Federal Technical and Export Control Service

The Federal Technical and Export Control Service was formed in August 2004[567] and is assigned to the Ministry of Economic Development and Trade. The Federal Technical and Export Control Service's activities are guided by the president of the Russian Federation and come under the jurisdiction of the Ministry of Defense. The Federal Technical and Export Control Service is an executive body dealing with the following issues:

- Ensuring information security in ICT systems important for state security;
- Countering foreign technical espionage on the territory of the Russian Federation;
- Ensuring the protection of the state's classified information and other data by restricting access and preventing technical leaks and unauthorized access;
- Export control.

564 http://www.agentura.ru/english/dosie/brit/fapsi.
565 http://www.shaneland.co.uk/ewar/docs/dissertationsources/russiansource1.pdf.
566 http://www.fas.org/irp/world/russia/fapsi/index.html.
567 Edict no. 314 of the president of the Russian Federation of 9 March 2004 on the System and Structure of Federal Executive Bodies.

Ministry of Information Technologies and Communications

The Ministry of Information Technologies and Communications is a branch of the federal government that implements state policy and oversight in the telecommunications sector. Among many other tasks, the ministry, together with other parts of the federal government, takes measures aimed at the restoration of the information and communication networks of the Russian Federation in emergency situations. It develops and implements a scientific-technical strategy for information security. The ministry also coordinates efforts to develop the national IT infrastructure.[568]

Public-Private Partnerships

For many years, information security problems in Russia were only studied and addressed in a timely fashion for the protection of state secrets in military, governmental, or other state-related automated systems. Thus, over time, a situation developed in which very specific commercial-sector problems went unresolved because of the absence of such a sector.[569] At present, the development of commercial IT-security products in the Russian market is prospering, yet sometimes limited by financial restrictions and the shortage of IT specialists.

Genuine public-private co-operation in the field of information security remains rather limited when compared to efforts in other countries. This is a result of the fact that for many (especially small and medium-sized) businesses in Russia, information assurance is not the most pressing problem. But both sides – private and public — are currently changing their stance, making more cooperation a much likelier prospect.[570]

Russian Association of Networks and Services (RANS)

The Russian Association of Networks and Services (RANS)[571] is a public and governmental organization. RANS is developing norms and legal documents for the implementation and use of secure IT. It is a public and governmental

568 http://english.minsvyaz.ru/site.shtml?id=17&page=1.
569 Terrorism: Reducing Vulnerabilities and Improving Responses, op. cit.
570 Information provided by Russian expert.
571 http://www.rans.ru/eng/directions.

organization, and has 122 members. The establishment of RANS was initiated by the Ministry for Information Technologies and Communications of the Russian Federation in 1994. At present, RANS has members from all over Russia including universities, scientific institutions, ministries, legal and insurance companies, operators, ISPs, vendors, and users. RANS has several committees and workgroups on main topics, covering the internet, security and privacy, wireless communications, education and training, and IP telephony. One of its working groups monitors standards.

The main activities of RANS are:

- Assisting the development of the internet in Russia;
- Establishing a predictable, informative, non-contradictory, and clearly legal environment for internet activities;
- Creating and realizing projects and programs aimed at the development of networks, systems of data transmission, telematic services, and information safety;
- Integration and coordination of the interests of users, producers, and operators of information and telecommunication systems;
- Integration of Russian information and telecommunication systems into the European and global infrastructure;
- Organization of conferences and exhibitions; publishing activities and professional development.[572]

In the sphere of information security, the program of RANS covers:[573]

- The creation and development of the PKI and information security concept in Russia;
- The preparation of a draft law on electronic digital signatures;
- The preparation of proposals in co-operation with the Ministry for Internal Affairs for the prevention of illegal activities in the telecommunication networks;
- Creating a hierarchical PKI Infrastructure, managed by the Federal Cryptographic Body.

572 http://www.rans.ru/eng/directions.

573 http://www.rans.ru/eng/programs. Other major projects are in the fields of telecommunications, e-business, and education and training.

PRIOR

PRIOR[574] is a national public initiative that unites public, private, and non-profit organizations. Through its activities, this initiative aims to supplement the existing state and non-governmental programs and projects directed at developing an information society and a knowledge economy in Russia. PRIOR recognizes the importance of participating in the major development programs, including those of the state. These include the Federal Program Electronic Russia for the Years 2002–2010, the municipal program Electronic Moscow, the program Electronic Saint Petersburg, and others.

PRIOR's major project is creating the Russia Development Gateway[575], which is envisioned as an environment for partner interaction and collaboration to reach common goals as well as a means of integrating expert knowledge in the development field. It is an unprecedented coalition of equal partners instead of the traditional Russian hierarchical system.

PRIOR is a volunteer association of organizations and individuals who have pooled their efforts and resources in order to provide mutual informational, technological, consulting, financial, organizational, and other types of support to reach common goals. These goals include e-governance, e-business, the networked society, distance learning, digital libraries, and strengthening international, national, and local projects and initiatives through effective dissemination of best practice knowledge and experience.

Among others, PRIOR's aims are:

- To assist in developing the legal base of the information society, the infrastructure of information processing, and communications channels;
- To serve as an effective national system for applying innovations;
- To educate and train qualified knowledge workers;
- To provide relevant local information content and services;
- To establish a unified methodological and terminological base regarding the information society and knowledge economy;
- To give Russian users access to best-practice solutions and know-how and to assist in the implementation of partnership-based programs and projects aimed at development through ICT.[576]

574 http://russia-gateway.ru/en.
575 Ibid.
576 Ibid.

Early Warning and Public Outreach

The "Russian Information Security Doctrine" mentions the development of some early-warning mechanisms: "In these specific conditions, information security is ensured, among other things, by developing an effective system of monitoring critical objects whose malfunction may give rise to emergency situations and prediction of emergency situations".[577]

Russian Computer Emergency Response Team (RU-CERT)

The Russian Computer Emergency Response Team (RU-CERT)[578] was founded in 1998 and is maintained by the Russian Institute of Public Networks (RIPN).[579] RU-CERT is part of the RBNet (Russian Backbone Network) Operation Center.[580] RBNet was established to provide internet services for science and high school communities in Russia. RBNet is a project funded by the Russian government under the responsibility of the RIPN.

RU-CERT provides computer-incident prevention and response services for RBNET users. The initial goal of the RU-CERT project was the coordination of efforts in the Greater Moscow area in their fight against hackers, primarily "script kiddies" who used stolen dial-up passwords and caused considerable material damage. However, it quickly became clear that service providers prefer to solve all problems independently and hide the results of their anti-hacker efforts from the public. It was subsequently decided to change its scope of activity and to create an organization like the US CERT for Russia.

Law and Legislation

The legal framework for information security in Russia encompasses the "Law of the Russian Federation On State Secrets",[581] the "Basic Principles of the Legislation of the Russian Federation on the Archive Fund of the Russian Federation and Archives",[582] and the "Federal Laws On Information,

577 Doctrine of the Information Security of the Russian Federation, op. cit.
578 http://www.cert.ru/index_eng.html.
579 http://www.ripn.net.
580 http://www.ripn.net:8082/rbnet/en/description.html.
581 In Russian: http://www.medialaw.ru/laws/russian_laws/txt/8.htm.
582 In Russian: http://www.rusarchives.ru/lows/zakon.shtml.

Informatisation and Information Protection",[583] which focus mainly on the use of information resources, information access rights, and information protection in the sense of preventing unauthorized access to documented information that may lead to damage for government bodies or any other holder of information resources. The "Federal Law on Communications"[584] also covers communication network management in emergencies.[585] A number of other laws[586] have been adopted, and work has begun to implement them and to prepare draft laws regulating social relations in the information sphere.[587] Moreover, the "Law of the Russian Federation on Legal Protection of Computer Programs and Databases" protects the content of computer programs and databases.[588]

The government hopes that the new federal "Electronic Digital Signature (EDS) Law"[589] will serve as a tool for regulating the field of information security. The law provides for recognizing the EDS as being legally equivalent to a physical personal signature. Specifically, the EDS Law protects the rights of persons who use EDS in their electronic data exchange. As part of enforcing this law, the government has been working to put into place a network of EDS authentication centers that will help enforce the law and derive regulations.

The new "Russian Law on Technical Regulation"[590] also offers a new definition of the concept of security.[591] It states that "security is a condition in which intolerable risk of harm is absent". Furthermore, its Article 7 states that "technical regulations taking into account the degree of risk of harm establish minimum necessary requirements for ensuring, among others, electrical security."[592]

583 http://www.datenschutz-berlin.de/gesetze/internat/fen.htm.
584 http://www.medialaw.ru/e_pages/laws/russian/comm_eng/comm_1.html.
585 Chapter 10, Article 65–67.
586 Further information: http://www.fas.org/irp/world/russia/docs/arf_p2.htm.
587 http://www.medialaw.ru.
588 http://freeweb.supereva.com/pdenicto/protectsw.htm?p.
589 http://www.bakernet.com/ecommerce/Russia-E-Signature-Alert.doc; Code in Russian: http://www.akdi.ru/gd/proekt/086086GD.SHTM.
590 Code in Russian: http://www.aprok.ru/tecreg/chronicle.php.
591 http://books.nap.edu/books/0309089719/html/108.html#pagetop.
592 Interestingly, before 2003, documents issued by Russian state organizations on information security did not include the word "risk".

Russian Criminal Code 1996/2004

The number of cyber-attacks against enterprises, organizations, and citizens is growing at a stable pace. According to information from the Main Administration for Special Technical Measures of the Russian Ministry of Internal Affairs, the number of computer-related crimes committed in Russia increased by almost 150 per cent over the previous year in 2001.[593]

The Russian Criminal Code of 1996 (revised in 2004) provides for the punishment of the following crimes related to breaches of computer security:[594] unlawful access to lawfully protected computer information; development of computer programs or introduction of changes into existing computer programs that are known to lead to unsanctioned destruction, blocking, modification, or copying of information, disruption of the operation of the computer, the computer system or its networks, and likewise the use or dissemination of such programs or discs containing such programs; and violation of the rules of use of a computer, computer system, or network by a person having access to this computer, computer system, or network.[595]

Chapter 28: Crimes in the Computer Information Sphere

The Criminal Code of the Russian Federation now includes articles establishing penalties for types of crimes that had not been defined previously. Chapter 28 of the code, "Crimes in the Computer Information Sphere", consists of three articles outlining the penalties for unlawful access to computer information (Article 272); for the creation, use, and dissemination of malicious computer programs (Article 273); and for violations of rules for the operation of computers, computer systems, and networks (Article 274).[596]

593 http://www.mvdinform.ru/; Source: http://books.nap.edu/books/0309089719/html/105.html#pagetop.

594 Further information: http://www.crime-research.org/analytics/Liability_for_computer_crime_in_Russia.

595 Source: http://www.4law.co.il.

596 http://books.nap.edu/books/0309089719/html/102.html#pagetop.

Draft Information Security Act

The "Russian Draft Information Security Act"[597] aims at covering almost all fields, including:

- Administrative and physical protection;
- Protection against unauthorized access to information in individual systems;
- Protection of information and its availability in networks;
- Protection of electronic document interchange, including regulation of digital signatures;
- Protection of classified data by detection of signals and electromagnetic radiation;
- Protection from malicious software (viruses etc);
- Protection against threats to intellectual property, illegal copying, etc.

The legislation would legally protect a variety of secrets, including the operations of the state and the military, commerce, and banks, as well as personal data, microcircuits, and digital signatures. Appropriate criminal, civil, and labor laws are currently being developed. However, it is unclear when this act will be adopted.[598]

597 http://www.globalsecurity.org/intell/world/russia/gtk.htm.
598 Estimate by Russian expert.

Singapore

Critical Sectors

New security threats that have emerged in the post-11 September 2001 ("9/11") era emphasized the need for closer cooperation between the military and Homefront[599] agencies in Singapore. Immediately after 9/11, the Homefront agencies undertook a review of the vulnerabilities and strengths of the range of Singapore's national critical infrastructure from the following sectors:

- Banking and Finance,
- Information- and Telecommunications,
- Energy,
- Water,
- Transportation,
- Health.[600]

* The Country Survey of Singapore 2006 was reviewed by the relevant officers from the Ministry of Home Affairs (Chapters on NEST, NCIA, and The Fight Against Terror).

599 The 'Homefront' encompasses all aspects of daily life in Singapore, bodies/apparatus involved in the economic and social life, provision of the various services to the population, civil defence and the maintenance of civil security.

600 Speech by Senior Minister Of State For Law and Home Affairs Ho Peng Kee at the Monoc Seminar, Ministry Of Home Affairs, 22 March 2002. http://www2.mha.gov.sg/mha/detailed.jsp?artid=178&type=4&root=0&parent=0&cat=0&mode=arc.

These are the six sectors whose critical infrastructures have already been reviewed, assessed and remedial plans implemented. Three other sectors have since been added: the Food Supply, Environment and Economy sectors.

Moreover, in "The Fight Against Terror — Singapore's National Security Strategy",[601] the following sectors are explicitly mentioned in the section on "Protection of Critical Infrastructure and Key Installations":

- Prominent Public Places,
- High-Profile Events,
- Transport by Land, Air, and Sea.[602]

Initiatives and Policies

Singapore adopted the internet comparatively early. According to the Network Readiness Index by the World Economic Forum, Singapore was the most network-ready country in 2004–2005.[603] In spring 2005, the Singaporean government presented a comprehensive "Infocomm Security Masterplan" for the years 2005–2007 that is part of the country's national security strategy to address cyber-security and cyber-terrorism.[604]

National Emergency System (NEST)

Since the mid-1980s, Singapore has planned and developed its Homefront preparedness efforts along the lines of a total defense concept. The Ministry of Home Affairs (MHA) has brought various ministries and emergency authorities together to integrate homeland preparedness plans. NEST is a comprehensive system encompassing civil security, civil defense, the provision of essential services, and the smooth operation of the economy during an emergency. It

601 National Security Coordination Centre, The Fight Against Terror – Singapore's National Security Strategy (Singapore, 2004). http://www.pmo.gov.sg/NSCS/FightAgainstTerror.pdf.

602 Ibid., pp. 47–51.

603 Costa, Valerie D., "Singapore's Internet Policy", Workshop on Internet Governance at the National Level (Geneva, 19 July 2005). http://www.wgig.org/docs/Singapore%20Internet%20Policy%2019%20Jul%2005.ppt.

604 Keynote address by Minister for Information, Communications, and the Arts Lee Boon Yang at the 17th Annual FIRST Conference (Singapore, 29 June 2005). http://www.mica.gov.sg/pressroom/press_050629.html.

also ensures the provision of essential services and commodities such as water, power, health services, telecommunications, food, and fuel to the public.[605]

National Critical Infrastructure Assurance (NCIA) Program

As announced in 2002,[606] the Singapore government has set up a National Critical Infrastructure Assurance (NCIA) project to carry out an in-depth assessment of the vulnerabilities of their critical national infrastructures and of necessary measures to reduce these vulnerabilities. The project involves consultation and partnership between the government agencies and the private sector. The National Infocomm Security Committee (NISC) supports the NCIA program.[607]

The Fight Against Terror – Singapore's National Security Strategy

In August 2004, the government's National Security Coordination Centre released a document entitled "The Fight Against Terror — Singapore's National Security Strategy"[608], according to which security standards in crucial areas such as aviation security, maritime security, land transport security, border control, and critical infrastructure protection have been raised in Singapore.[609] As a result of 9/11 and based on the recommendations of the National Critical Infrastructure Assurance Committee, Singapore has initiated several measures to protect its physical critical infrastructure and key installations, including prominent public places, power stations, and transportation and water supply networks.[610]

605 Speech by Ho Peng Kee, op. cit.; and keynote address by Minister for Home Affairs Wong Kan Seng at the Monoc Seminar 2003 (Singapore, 29 March 2003). http://www2.mha.gov.sg/mha/detailed.jsp?artid=724&type=4&root=0&parent=0&cat=0.

606 Asia-Pacific Conference on Cybercrime and Information Security (Seoul, 11–13 November 2002). Country Report on Singapore, p. 15. http://www.unescap.org/icstd/cybercrime%20meeting/Presentations/Session%203%20-%20country%20and%20org.%20reports/Singapore/Singapore%20written%20report.doc.

607 Addendum to the President's Address by Minister for Home Affairs Wong Kan Seng (Singapore, 17 January 2005). http://www2.mha.gov.sg/mha/detailed.jsp?artid=1383&type=4&root=0&parent=0&cat=0&mode=arc.

608 The Fight Against Terror, op. cit.

609 Ibid., p. 12.

610 Acharya, Arabinda, Defending Singapore's Vital Infrastructure Against Terrorism, IDSS Commentaries (37/2004). Institute of Defence and Strategic Studies (Singapore, 2 September 2004). http://www.pvtr.org/pdf/IDSS372004.pdf.

Infocomm Security Masterplan

In response to cyber-threats such as hacking, virus attacks, and cyber-terrorism, the deputy prime minister announced the three-year "Infocomm Security Masterplan" (2005–2007) in February 2005. He said that as Singapore's economy would continue to rely heavily on ICT, securing the "infocomm" environment would be critical. The government would thus set aside S$38 million (about US$23 million) over the next three years to build capabilities in managing cyber-threats and enhancing the security of cyberspace.

The master plan was developed through a multi-agency effort led by the Infocomm Development Authority of Singapore (IDA) under the guidance of the NISC. Feedback and input were given by companies and government agencies through surveys and focus group discussions. It was discovered that businesses have difficulty formulating and complying with IT security policies and best practices as they lack the necessary professionals and experience. The Infocomm Security Masterplan has two main aims:

- To maintain a secure IT environment for the government, businesses, and individuals. This involves raising awareness amongst internet users and businesses about risks and cyber-threats as well as appropriate security measures. Two planned key projects to secure these three sectors are the "National Authentication Infrastructure", which will develop reliable and robust authentication means to curb identity theft and promote more secure e-services, and the "Business Continuity Readiness Assessment Framework". They will measure the effectiveness of government agencies' business continuity plans.
- To defend Singapore's critical infrastructure from cyber-attacks. The master plan also outlines strategies to develop national capabilities, to enhance security technology research and development, and to improve the resilience of critical information infrastructure. To defend against cyber-attacks, a National Cyber-Threat Monitoring Centre will be set up to maintain round-the-clock vigilance and analyze threat information. A "Vulnerability Study of National Critical Infrastructures" will assess the IT-security readiness of key economic sectors and the measures required to provide greater security.

Finally, a Common Criteria Certification Scheme and a set of international standards on security are planned.[611]

Organizational Overview

Public Agencies

The Infocomm Development Authority of Singapore (IDA) is the chief technology office of the Singapore government covering planning, policy formulation, regulation, and cooperation with the private sector in the field of ICT. The National Infocomm Security Committee (NISC) and the Technology Crime Division (TCD) within the Singapore Police Forces also play important roles in the field of CIIP.

Infocomm Development Authority of Singapore (IDA)

IDA is a statutory board of the Singapore government that was formed in 1999 as the result of a merger between the National Computer Board (NCB) and the Telecommunications Authority of Singapore (TAS). The aim was to have a single agency for integrated planning, policy formulation, regulation, and industry development of the ICT sector.[612] IDA operates under the Ministry of Information, Communications, and the Arts (MICA).

Among IDA's main responsibilities are fostering a competitive IT industry in Singapore, preparing residents for living and working in the "New Economy", supporting the delivery of citizen-centric e-government services, and building and operating the government's IT infrastructure.[613] IDA sets

611 IDA press release, "Singapore Gears Up for Cyber Security. Three-year Infocomm Security Masterplan Unveiled" (Singapore, 22 February 2005). http://www.ida.gov.sg/idaweb/marketing/infopage.jsp?infopagecategory=&infopageid=I3280&versionid=3.

612 Among other entities, IDA supports the Information Technology Standards Committee (ITSC), the National Trusts Council (NTC) – an industry-led council to build confidence in e-commerce –, and the Public Key Infrastructure (PKI) Forum Singapore.

613 http://www.ida.gov.sg/idaweb/aboutida/infopage.jsp?infopagecategory=&infopageid=I229&versionid=16

ICT standards and regulations and supports the private sector in implementing security measures.

IDA's Infocomm Security Division (iSec) plays a central role in establishing and implementing a solid IT security infrastructure for Singapore's national ICT infrastructures. iSec monitors the implementation of ICT security measures and practices for the whole public sector. Moreover, iSec conducts awareness programs for the public and the private sector as well as individuals. For instance, in 2001, IDA initiated a yearlong public-awareness campaign that aimed to instill safe computing practices among the public- and private-sector users as well as the general public.[614]

National Infocomm Security Committee (NISC)

The National Infocomm Security Committee (NISC) was set up to formulate policies and strategic direction for cyber-security at the national level. With members from various government agencies, it is a platform for the government to institutionalize considered policies and mandate strategic initiatives in IT security. It comprises representatives from the Ministry of Home Affairs, the Ministry of Defence, the Ministry of Information, Communication and the Arts, the Ministry of Finance, the DSO National Labs, and the Defence Science and Technology Agency (DSTA). IDA serves as the secretariat for this committee.[615]

Technology Crime Division (TCD) within the Singapore Police Force

Within the Singapore Police Force, the Criminal Investigation Department (CID)[616] is the primary investigation agency in Singapore for all criminal matters.[617] The Technology Crime Division (TCD) is part of the CID. TCD provides specialized investigative and forensic services as well as training the entire police force in investigating high-tech crime. Its scope of operation goes beyond computer crime and includes traditional crimes committed with the

614 Asia-Pacific Conference on Cybercrime and Information Security, op. cit.
615 Cf. "Singapore Gears Up for Cyber Security".
616 http://www.spf.gov.sg/publication/pla/03spfa_cid.htm.
617 http://www.spf.gov.sg.

use of technology, such as encrypted mobile devices, the internet, and even wireless platforms. In order to ready the nation for crimes of the future, the approach adopted by TCD is also to build capabilities through research, alliance-building, and education.[618]

Public Private Partnership

The government of Singapore is supporting local companies offering ICT security consultancy, services, and products (many are spin-offs from the research institutes).

National Infocomm Competency Centre (NICC)

The National Infocomm Competency Centre (NICC)[619] is an industry-led and government-supported organization that aims to assist individuals and organizations in reaching and maintaining a high level of ICT competence. Moreover, NICC is the main accreditation body for ICT certifications. NICC works closely with the Ministry of Manpower (MOM) and the IDA to promote knowledge and skills.

Among NICC's activities are:

- Development and maintenance of ICT skills, standards, and knowledge,
- Facilitating the development and implementation of certification programs,
- Promoting activities to increase the certification of IT professionals and users,
- Collaborating with international certifying bodies for the accreditation of certifications, and
- Promoting competence and learning management practices.[620]

618 Leong, Clement, "Security Initiatives in the Computerisation of the Singapore Government". http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/13-Homeland-Security-Singapore_R2GVIV_0Z5RDZ-i34K-pR.htm.
619 http://www.nicc.org.sg/index.aspx.
620 http://www.nicc.org.sg/aboutus/vision.aspx

Information Technology Standards Committee (ITSC)

Volunteer members from the industry, supported by the Productivity and Standards Board (PSB) and IDA, established the industry-led Information Technology Standards Committee (ITSC)[621] in 1990. It is a neutral platform for interested industry and government parties to convene to agree on technical standards. To this end, ITSC organizes workshops and seminars on various topics. Currently, some 350 technical experts and representatives from 180 organizations are engaged in ITSC's standardization activities. ITSC's Security and Privacy Standards Technical Committee has published the IT Security Standards Framework (SS493).[622]

Governmentware IT Security Seminar Series

The annual Governmentware IT Security seminar series began in 1991. The seminars are organized by the IT Command of the Internal Security Department (ISD) of the Ministry of Home Affairs (MHA) – whose organizing partner since 2002 has been the Institute of Public Administration and Management (IPAM) of the Civil Service College. The lectures are also open to an audience from outside the public sector. The first seminar, organized by ISD for civil service participants, was held urgently in the wake of concerns about virus attacks against government user PCs. The Governmentware seminars alert participants to the latest security threats posed by emerging technology and advanced hacking techniques. Private-sector IT security industry experts are invited to participate and share their knowledge.[623]

621 http://www.itsc.org.sg.
622 Asia-Pacific Conference on Cybercrime and Information Security, op. cit.

Early Warning Approaches

Singapore Computer Emergency Response Team (SingCERT)

The Singapore Computer Emergency Response Team (SingCERT)[624] is responsible for the detection, resolution, and prevention of security-related incidents on the internet. SingCERT also issues advisories and alerts about incidents. It maintains a website and a hotline for reporting and dissemination of advisories. SingCERT was initially established in October 1997 as a program of IDA, in collaboration with the Centre for Internet Research at the National University of Singapore (NUS).
SingCERT provides the following services:

- Broadcast alerts, advisories and security patches,
- Promote security awareness through security courses, seminars and workshops,
- Collaborate with vendors or other CERTs to find solutions to security incidents.

SingCERT is also a founding member of the Asia Pacific Security Incident Response Coordination Working Group (APSIRC-WG). The APSIRC-WG is staffed by volunteers from the national Incident Response Teams (IRTs) of Japan, Korea, and Singapore and aims to promote collaboration with other international IRTs and security groupings, such as the Forum of Incident Response and Security Teams (FIRST). Furthermore, APSIRC-WG provides assistance to countries in the region that would like to establish their own IRTs.[625]

National Cyberthreat Monitoring Centre (NCMC)

Under the Infocomm Security Masterplan, "the National Cyberthreat Monitoring Centre, or NCMC in short, has been set up as a national resource

623 Governmentware 2004 Seminar. Brief Facts. http://www2.mha.gov.sg/mha/upload/mid16/type4/cat0/1220_312_Brief%20Facts%20on%20Governmentware%20Seminar%20v1.4.pdf.
624 http://www.singcert.org.sg.
625 Ibid.

to safeguard Singapore's cyber security and to provide focused tracking of cyber threats. Besides the round-the-clock monitoring of critical networks, the centre will provide regular in-depth analysis of cyber-threats by incorporating information from all available sources. The NCMC will provide latest trends in cyber threats to better respond to, and even pre-empt future attacks".[626]

Law and Legislation

Computer Misuse Act 1993/1998

The Computer Misuse Act (CMA) was first enacted in 1993 and first amended in 1998. It is aimed at protecting computers, computer programs, and information stored in computers from unauthorized access, modification, use, or interception. The CMA also applies to any person, irrespective of physical location, who hacks into computers located in Singapore, and to any person in Singapore who hacks into computers outside Singapore.

The 1998 amendments also address newer forms of cyber-crime (such as Trojan horses, password trafficking, or denial of service attacks). The amended CMA also provides enhanced penalties for computer crimes proportionate to the potential and actual harm caused. The amendment gives the police powers to gain lawful access to computer material, including encrypted material.[627]

Computer Misuse (Amendment) Act 2003

The amendment to the Computer Misuse Act in 2003 will enable the minister to empower any person or organization to take necessary measures to prevent or counter any threat to a computer system that can affect the national security, essential services, defense, or foreign relations of Singapore. This is part of the government's efforts to establish a robust defense against cyber-attacks.

Like many other countries, Singapore's essential and critical services such as water, electricity, gas, telecommunications, and transportation are increas-

626 Yang, op. cit.
627 Cf. "Security Initiatives in the Computerisation of the Singapore Government".

ingly dependant on computer networks and information systems. Terrorists and criminals can exploit this dependence. Any attack on the critical infrastructure and essential services will severely disrupt the economy and threaten the national security.

Furthermore, with an increasingly computer-literate population and widespread availability of user-friendly hacker tools, more people around the world now have the necessary skills to carry out cyber-attacks. Hackers and computer viruses can flood network connections, steal or tamper with information, and disrupt essential services.

New section 15A

The new section 15A allows the minister to authorize any person or organization to take necessary measures to prevent or counter any threat that may endanger the national security, essential services, defense, or foreign relations of Singapore. The new section 15A would be invoked to deal with situations of an outright cyber-attack, or in cases where specific intelligence has been received of an imminent cyber-attack against Singapore's critical infrastructure.

The powers given to the minister under the new section 15A may not be used indiscriminately. The measures are aimed at preventing or countering any threat to a computer or computer service, or to any class of computers or computer services. The powers would be invoked only to avert threats that may endanger national security and essential services such as any service directly related to the communications infrastructure, the banking and finance sectors, and the defense and foreign relations of Singapore. The powers under the new Section 15A would not be invoked to prevent or investigate a criminal offence that does not threaten the national security or essential services. Singapore's security agencies will also be required to satisfy the minister that the cyber-threats are imminent before the powers provided by the new section 15A can be invoked.[628]

Electronic Transactions Act 1998

The Electronic Transactions Act (ETA) was enacted in 1998 to provide a legal infrastructure for electronic signatures and electronic records, and to give

628 http://www2.mha.gov.sg/mha/ibrowse.jsp?type=3&root=0&parent=0&cat=8; and http://www2.mha.gov.sg/mha/detailed.jsp?artid=936&type=4&root=0&parent=0&cat=0&mode=arc.

predictability and certainty to electronic contracts. The ETA establishes the supporting legal infrastructure for the PKI. The ETA addresses the following issues:

- Commercial code for electronic commerce transactions,
- Use of electronic applications and licenses for the public sector,
- Liability of service providers,
- Provision for a PKI.

Sweden

Critical Sectors

There is no official definition of CII or CIIP in Sweden. However, CIIP can be understood as the protection of essential electronic information services, such as IT systems, electronic communications, and radio and television services. CIIP has not only a technical, but also a human aspect. The following are regarded as critical information infrastructure sectors:

- Air Control Systems,
- Supervisory Control And Data Acquisition (SCADA) systems in use within water, transport, and industry,
- Financial Systems,
- National Command Systems,
- Telecommunication Systems,
- The Internet.[629]

* The Country Survey of Sweden 2006 was reviewed by Linda Englund, Swedish Emergency Management Agency (SEMA).

629 Information provided by expert of SEMA.

Disruption of any of these systems would have immediate serious consequences for society.

Past and Present Initiatives and Policies

CIIP issues have been on the political agenda in Sweden for many decades. Measures to increase the robustness and security of critical national infrastructures have been implemented since World War II. The vulnerability problems associated with society's increasing dependence on IT and information infrastructures were identified early on as a matter of national security. In addition, management of IT-related vulnerabilities has been discussed since the early 1970s. The present Swedish CIIP policy is derived from these historical developments and from some more recent initiatives described below.

Commission on Vulnerability and Security

Following a decision on 23 June 1999, the Swedish government authorized the minister for civil defense to appoint a special investigator to head a commission of inquiry, with a mandate to analyze and submit proposals for a more integrated approach to civil defense and emergency preparedness planning.[630] The findings and proposals of the Commission on Vulnerability and Security, as presented in May 2001, have been a most important step in the implementation of a new structure for defense and emergency preparedness planning in Sweden.

The commission suggested several strategic measures for improving the general stability of critical technical infrastructure.[631] In its final report, the commission also proposed measures designed to specifically enhance information assurance and improve protection against information operations. The commission's view was that the central government must assume responsibility in these areas. At the same time, the commission emphasized that all

630 The Swedish Commission on Vulnerability and Security. Vulnerability and Security in a New Era – A Summary (SOU 2001:41, Stockholm, 2001). http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41eng.pdf.

631 Such as cross-sector activity, security standards, Computer Emergency Response Teams, a coordinating body for IT security, an information security technical support team, an intelligence and analysis unit, research and development, international cooperation, a system for the certification of IT products, and more. Ibid., pp. 41–60.

managers and system owners are responsible for securing their own systems against computer intrusions and other types of IT-related threats. The role of the government should be to support these activities and to provide functions and facilities that exceed the financial capabilities of other sectors in society.

Bill on Swedish Security and Preparedness Policy

In March 2002, the government presented its first bill on Swedish security and preparedness policy. The bill was, to a large extent, based on the findings and proposals of the Commission on Vulnerability and Security.

The bill presented the government's framework for a new planning system to prepare for major societal crises and for activities related to a potential threat of war. Furthermore, the bill gave an account of how the crisis management structure would be strengthened. All of this has implications for the security of critical infrastructures in general, and of critical information infrastructures in particular.[632]

Committee on Information Assurance in Swedish Society

The Swedish government on 11 July 2002 instituted the Committee on Information Assurance in Swedish Society. The committee's brief was to present an assessment of information protection requirements in critical sectors of society, and to make a proposal on organizational matters of the Swedish signals protection service. In addition, the committee was asked to submit proposals regarding:

- The development of a national strategy for information assurance;
- The form and focus of future Swedish engagements in international cooperation on information assurance;
- The implementation of the "OECD Guidelines for the Security of Information Systems and Networks".

The committee is also expected to monitor the implementation of information assurance measures within state agencies in accordance with the "bill on Swedish security and preparedness policy".[633]

632 Information provided by expert of SEMA.
633 Government bills 2001/02:158.

The Committee on Information Assurance in Swedish Society has, after monitoring the implementation of the information assurance measures, presented its proposal for a national strategy on information assurance[634] and also an organization plan.[635] The Committee's proposal will be processed by the government by March 2006.
The Committee's strategy entails:

- Developing Sweden's position in the EU and in the international context;
- Creating confidence, safety, and security, and increasing the protection of integrity;
- Promoting increased use of IT;
- Preventing the occurrence of and being able to handle disruptions in information and communication systems;
- Reinforcing the work of the intelligence and security services and developing the distribution of information;
- Reinforcing existing capabilities in the field of national security.
- The strategy should also include:
- Exploiting the full potential of society;
- Focusing on important public activities;
- Increasing awareness of security risks and possibilities of protection;
- Ensuring the provision of competence.

Organizational Overview

Public Agencies

The government agencies report to their respective ministries, but are formally subordinated only to collective cabinet decisions. The various agencies and organizations in charge of critical information infrastructure protection are presented below under the heading of the ministry they are affiliated with.

634 Secure information – proposals on information security policy (SOU 2005:42).
635 Organizational consequences (SOU 2005:71).

The new bill on Swedish security and preparedness policy, which is to be presented in March 2006, contains a few changes of tasks and responsibilities for the actors within the area of information assurance. The bill contains more than just CIIP. The Committee on Information Assurance in Swedish Society has evaluated the CIIP work and suggested the changes to be introduced in the bill. The suggested changes are presented in the following chapter in connection with each actor.

Ministry of Defense

The Swedish Emergency Management Agency (SEMA)

The Swedish Emergency Management Agency (SEMA)[636] is responsible for the co-ordination of national information assurance at the policy level. This includes analyses of the development of society and the interdependency of critical societal functions. The agency further promotes interaction between the public and private sectors. The agency also coordinates and initiates research and development in the emergency management area, and has overall governmental responsibility for information assurance in Sweden. The Information Assurance and Analysis Department at SEMA manages the tasks.

In its guidelines for emergency planning for 2006 and 2007, SEMA reiterates the importance of protecting the nation's critical infrastructures. The risks of technical collapses in electricity, telecom, and IT systems that are vital for society must be given priority, according to SEMA.[637] "Within critical infrastructure, especially the technical infrastructure, actions designed to decrease the consequences of serious emergencies are given priority over preventive measures with the purpose of increasing robustness."[638]

According to the recommendations made by the Committee on Joint Radio Communication for Public Safety and Security, a new department has been formed at SEMA that handles radio communication for public safety (PSS) issues. The new PSS system is called RAKEL (Radio Communication for Efficient Command).

636 http://www.krisberedskapsmyndigheten.se/defaultEN____224.aspx.

637 SEMA guidelines for emergency planning for 2006 (summary). http://www.krisberedskapsmyndigheten.se/3404.epibrw.

638 SEMA guidelines for emergency planning for 2007 (summary). http://www.krisberedskapsmyndigheten.se/5705.epibrw.

The main activities of the Information Assurance and Analysis Department at SEMA include:

- Maintaining an updated overall picture of society's information security in terms of threats, vulnerabilities, protective measures, and risks; once a year, it presents an annual assessment of information assurance in Sweden to the government;
- Hosting various forums in order to develop a common national culture of information assurance. Certain forums are solely intended for the private sector or the public sector, respectively, while there are also combined forums for the public and private sectors;
- Developing public-private partnerships;
- Gathering, analyzing, and disseminating open-source information related to information assurance;
- The development of preventive IT security recommendations (consistent with ISO/IEC 17799) to support the IT security activities of other organizations;
- Initiating research and development in the area and summarizing risk and vulnerability assessments of different important societal systems;
- Managing the Board of Information Assurance.

The changes suggested by the Committee on Information Assurance in Swedish Society concerning SEMA are:

- Greater financial means to stimulate and initiate research in the field of information security, and participation in the EU's policy-making work to focus and implement research within the area;
- A stronger mandate to coordinate policy and administrative information security, which includes developing the national information security strategy and coordinating information security work between different actors in society. It has been suggested that SEMA have the overall responsibility for society's information security at the policy level;
- Serving as a public contact point for information security and acting as an international contact point under the government; and representing Sweden in international collaboration, where no other authorities are in charge;

- Issue regulations on a basic level of security though the supervision of the regulations to be carried out by other actors than SEMA;
- Responsibility for signals protection training within the field of information security.

SEMA/Information Assurance Council

The Information Assurance council was established to support SEMA's activities in the area of information assurance. This council will create a network of skilled experts from a variety of important organizations in the area. The council replaced the earlier Cabinet Office Working Group on Information Operations.[639] The council's primary assignment is to assist the senior management of SEMA by supplying:

- Information about trends in research and development in the area of information assurance;
- Suggestions and viewpoints concerning the direction, prioritizing, and realization of SEMA's activities in the area of information assurance.

The Swedish Defense Materiel Administration (FMV) and the Certification Body for IT Security (CSEC)

The Swedish Defense Materiel Administration (FMV)[640] is the procurement agency for the armed forces. The FMV has been involved in the area of IT security evaluations since 1989, performing in-house evaluations of equipment intended for use by the armed forces.

In the summer of 2002, FMV was tasked by the government with establishing a Swedish scheme for the evaluation and certification of IT security products to be used within Swedish governmental organizations. The Certification Body is now established as an independent function within FMV and is called the Swedish Certification Body for IT Security (CSEC). This work includes production of quality manuals, descriptions of responsibility, description of processes for licensing of evaluation laboratories, rules for implementation of certificates, and training of certification staff and evaluation companies. [641]

639 SEMA document 0160/2003: Account of Measures Taken in Assuming Responsibilities from the Working Group on Information Operations (Redovisning av åtgärder för att överta arbetsuppgifter från Ag IO 0160/2003).

640 http://www.fmv.se/default.aspx?id=121.

641 Ibid.

National Defense Radio Establishment (FRA) / Information Security Technical Support Team

The Information Security Technical Support Team is associated with the Swedish National Defense Radio Establishment (FRA),[642] which is the Swedish signals intelligence organization. It is a civilian agency directly subordinated to the Ministry of Defense. The Information Security Technical Support Team consists of 20 experts in the field of IT security. The team is specifically intended to support:

- National crisis management where IT-security qualifications are required;
- Identification of individuals and organizations involved in IT-related threats against critical systems.

On request, the team supports the Swedish authorities, agencies, and state-owned corporations that are responsible for critical functions in Swedish society with IT-security expertise and services. The customized services consist of penetration tests, forensic computer investigations, source code analysis, audits, risk analyses, etc. The team co-operates on a regular basis with the national and international IT security community.

The changes suggested by the Committee on Information Assurance in Swedish Society concerning FRA are:

- In order to reflect the changes in its tasks, FRA will change its name to the Institute for Signals Intelligence and Technical Information (IST);
- Technical responsibility for coordination in the field of information security;
- Responsibility for signals protection;[643]
- Create a group that can support initiatives in national crises with an IT component and in the case of related threats to important public systems.

642 http://www.fra.se/english.shtml.

643 The National Communications Security Agency (NCSA) will be included in IST.

The Swedish Armed Forces

The Swedish Armed Forces[644] must be able to quickly respond to different types of threats and risks. The Swedish parliament has therefore decided to develop the armed forces according to the concept of network-based defense. This places a great demand on the information infrastructure in terms of availability and security. The armed forces are therefore heavily involved in research and development in areas such as IT security and information infrastructures.

The Swedish Military Intelligence and Security Service handles operational IT security in the armed forces during peacetime. In addition, the National Communications Security Group (TSA) offers advice and inspections of cryptographic systems to Swedish defense organizations and industries.[645]

Center for Asymmetric Threat Studies (CATS)

The National Center for IO/CIP Studies (CIOS) is now broadening its perspective from Information Operations (IO) to include terrorism, e.g. cyberterrorism. In order to do so, the center's name has been changed to "Center for Asymmetric Threat Studies (CATS)". CATS is located at the Swedish National Defense College.[646] It conducts research and policy development in the fields of CIIP, IO (Information Operations), PSYOPS (pychological warfare), and CIP. Research at CATS is funded by the Ministry of Defense and the Swedish Emergency Management Agency (SEMA).

The Swedish Defense Research Agency (FOI)

The Swedish Defense Research Agency (FOI)[647] focuses on research and development in the fields of applied natural sciences and political sciences, such as security policy analysis. At the Division of Defense Analysis, the Critical Infrastructure Studies Unit (CISU) research group is carrying out a long-term research program on CIP sponsored by SEMA, in cooperation with Systems Analysis and IT Security — another FOI department. This department has acquired a deep knowledge of commercial and military IT systems and applications.

644 http://www.mil.se/?lang=E.
645 Information provided by expert of SEMA.
646 http://www.fhs.se/templates/Page____2056.aspx.
647 http://www.foi.se/FOI/templates/startpage____96.aspx.

Ministry of Industry, Employment, and Communications

The Swedish National Post and Telecom Agency (PTS)
The Swedish National Post and Telecom Agency (PTS) is a government authority that monitors all issues relating to Information and Communication Technologies (ICT) and postal services. One of its key tasks is to ensure the development of functioning postal and telecom markets. Within the PTS, the Department of Network Security is responsible for security issues concerning ICT.

The Department of Network Security is tasked with monitoring developments concerning security issues and with implementing measures to reduce the threats to ICT from sabotage and terrorism. Emergency measures are planned in consultation with the ICT operators, the Swedish armed forces, and other agencies. As an example, critical nodes in the ICT structures are hardened, and all nodes that are crucial for running the ".se" domain autonomously have been installed within Sweden's borders. The Swedish IT Incident Center (see Early Warning) is associated with this department.

Department of Justice

The Swedish National Police Board (NPB)
The Swedish National Police Board (NPB)[648] is the central administrative and supervising authority of the police service. The NPB administers the National Criminal Police and the Swedish Security Service. Within the NPB, the IT Crime Squad has expert knowledge in investigating IT crime. This group supports the local Swedish police departments in IT crime investigations, participates in the education of parts of the judicial system, and assembles and communicates information about IT crime. The Internet Reconnaissance Unit is linked to this squad.

Additionally, the Swedish Security Service (SÄPO) has the fundamental duty of preventing and detecting crimes against the security of the realm. SÄPO is engaged in four main fields: protective security (including personal protection), counter-espionage, counter-terrorism, and protection of the con-

648 http://www.polisen.se/inter/nodeid=10230&pageversion=1.html.

stitution. Whenever IT-related criminal activity touches upon these fields, the Swedish Security Service is involved.

Public-Private Partnerships

The Swedish Emergency Management Agency (SEMA)

The Swedish Emergency Management Agency (SEMA) promotes interaction between the public sector and the private sector, and works to ensure that the expertise of non-governmental organizations (NGOs) is taken into account in emergency management.

There are two advisory councils connected to SEMA: the Private Sector Partnership Advisory Council and the Board of Information Assurance. However, it has not yet been established how the CIIP public-private partnerships will be institutionalized.

The Industry Security Delegation (NSD)

The Industry Security Delegation (NSD)[649] is part of the Confederation of Swedish Enterprise,[650] whose objective is to increase cooperation between enterprises, organizations, and authorities, and to promote comprehensive views on vulnerability and security issues. The overall goal of this network structure is to enhance security and risk awareness among the general public and in the business sector. The NSD arranges courses in information assurance as well as crisis and risk management to help its members improve security.

The Swedish Information Processing Society (DFS)

The Swedish Information Processing Society (DFS)[651] is an independent organization for IT professionals with 32,000 members. The DFS owns the SBA brand of security products (the abbreviation stands for SårBarhetsAnalys, or "vulnerability assessment" in Swedish), which focus on risk analysis and information security. SBA is regarded as the de-facto Swedish standard.

649 http://www.svensktnaringsliv.se/index.asp?pn=155246.
650 Svenskt Näringsliv, http://www.svensktnaringsliv.se.
651 http://www.dfs.se.

Early Warning and Public Outreach

The Swedish IT Incident Centre (SITIC)

In May 2002, the Swedish government tasked the Swedish National Post and Telecom Agency (PTS) with establishing the Swedish IT Incident Centre (SITIC).[652] The center was officially opened on 1 January 2003 and can be considered to be the Swedish government CERT. SITIC supports national activities for the protection against IT incidents by:

- Operating a system for information exchange on IT incidents between both public and private organizations and SITIC;
- Rapidly communicating to the public information on new problems that can disrupt IT systems;
- Providing information and advice on preventive measures;
- Compiling and publishing incident statistics as input to the continuing improvements of preventive measures.

Law and Legislation

In Sweden, there are three important laws regarding CIIP in general:

- The Swedish Penal Code (SFS 1962:700);
- The Personal Data Act (SFS 1998:204);
- The Electronic Communications Act (SFS 2003:389).

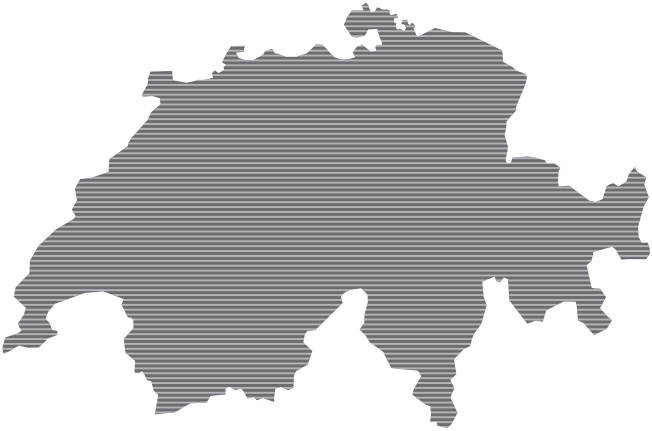
In its report, the Commission on Vulnerability and Security concluded that there was a need for legislative amendments in order to support the proposals with respect to IT security and the protection against information operations. A particular need for legislative amendments is seen in the following areas:[653]

652 http://www.sitic.se/eng/index.html.
653 Ibid.

- Statutory and administrative provisions relating to the activities of local authorities and country administrative boards during major crises;
- The possibility of reallocating resources in the health services during major crises;
- Stricter safety regulations and more effective supervision of the power supply sector.

The government has decided to review the legislation relevant to CIIP and emergency management.

Switzerland



Critical Sectors

Since the end of the Cold War, risks and vulnerabilities involving information and communications technologies have become a growing issue in the Swiss debate on security policy. The high density of information and communication technology (ICT) in Switzerland's public and private sectors offers a high potential for vulnerabilities. There is no official list of critical information infrastructure sectors. The definition of critical sectors is at the stage of planning and roughly includes the following:[654]

- (Public) Administration,
- Civil Defense, Emergency and Rescue Services,
- (Tele-) Communication,
- Energy,

* The Country Survey of Switzerland 2006 was reviewed by Michel Dufour, Dufour Consulting; Marc Henauer, Federal Police/DAP; Anton Lagger, Federal Office for National Economic Supply (NES); Ruedi Rytz, Federal Strategy Unit for Information Technology (ISB); Riccardo Sibilia, armasuisse; Oliver Vaterlaus, AWK Group; and Gérald Vernez, General Staff of the Swiss Armed Forces.

654 InfoSurance/Wirtschaftliche Landesversorgung/Informatikstrategieorgan Bund. Sektorspezifische Risikoanalysen – Methodischer Leitfaden (2002).

- Finance,
- Industry/Manufacturing,
- Media,
- Public Health,
- Transport (and Logistics),
- Water.

Past and Present Initiatives and Policies

Since the end of the 1990s, several important steps have been taken in Switzerland to improve the management of CIIP.[655]

Strategic Leadership Exercise

A key experience, and in fact the impetus for many later steps in Switzerland, was the Strategic Leadership Exercise in 1997 (SFU 97).[656] The exercise dealt with the revolution in information technologies and the related challenges to modern society, politics, economics, and finance, as well as to other critical sectors.[657] The exercise revealed that Switzerland's CI was facing new threats. One of the results was the call for an independent organization dealing with information security issues.[658]

Strategy for the Information Society Switzerland

In 1998, the Federal Council defined its "Strategy for the Information Society Switzerland". The strategy paper outlined the basis for promoting an informa-

655 See also Sibilia, Riccardo. "Informationskriegführung. Eine schweizerische Sicht". Institut für militärische Sicherheitstechnik (IMS) no. 97–6 (Zurich, 1997); Generalsekretariat VBS (ed.). Risikoprofil Schweiz. Umfassende Risikoanalyse Schweiz (draft version, Berne, August 1999); Spillmann, Kurt R., Stefan Libiszewski, Andreas Wenger, et al. "Die Rückwirkungen der Informationsrevolution auf die schweizerische Aussen- und Sicherheitspolitik". NFP 42 Synthesis, no. 11, Schweizerischer Nationalfonds (Berne, 1999); and Bircher, Daniel. "Informationsinfrastruktur – Verletzliches Nervensystem unserer Gesellschaft". In: Neue Zürcher Zeitung, 7 July 1999.

656 The SFU, which is subordinated to the Swiss Federal Chancellery, is responsible for the periodical training of federal decision-makers. http:// www.sfa.admin.ch.

657 Schweizerische Bundeskanzlei. Strategische Führungsübung 1997 – Kurzdokumentation über die SFU 97 (Berne, 1997), p. 2.

658 http://www.infosurance.ch.

tion society and identified the areas where action was most urgently needed.[659] The Federal Council also defined the four governing principles: (1) access to information for everyone, (2) empowerment for everyone to use information technologies, (3) freedom of development for the information society, and (4) acceptance of new technologies. Developments triggered by the information and communication technology were perceived as high-priority issues for Switzerland.

Security Policy Report 2000

In the Security Policy Report 2000,[660] the Swiss Federal Council recognizes CIP/CIIP as a goal of its security policy: "The Federal Council's primary objective regarding the security of this infrastructure is to maintain Switzerland's ability to decide and to act, and to create the conditions ensuring the functioning of the Swiss 'Information Society'".[661]

Concept of Information Assurance

The Information Society Coordination Group (ISCG) defined the security and availability of information infrastructures as one of the high-priority operative essentials. The key policy document, "The Concept of Information Assurance", was published in 2000. It recommended the establishment of a crisis management system of a special task force on "Information Assurance".[662] This strategy of the Swiss Federal Council was accompanied by a large number of parliamentary initiatives.

659 Informatikstrategieorgan Bund ISB. Verletzliche Informationsgesellschaft. Herausforderung Informationssicherung (Vulnerable Information Society – The Challenge of Information Assurance) (Bern, October 2002) p. 18. http://www.isb.admin.ch/imperia/md/content/sicherheit/schutz-infrastruktur/information_assurance/pia_d.pdf.

660 Sicherheit durch Kooperation. Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz (SIPOL B 2000), 7 June 1999. http://www.vbs.admin.ch/internet/vbs/de/home/departement/organisation/security/publikationen.ContentPar.0011.DownloadFile.tmp/Sicherheitspolitischer%20Bericht%202000.pdf.

661 Ibid., p. 56.

662 Information Society Coordination Group (ISCG). Konzept "Information Assurance" (Berne, May 2000). http://www.infosociety.ch/site/default.asp.

Exercise INFORMO 2001

After a two-year planning process, the Strategic Leadership Training in 2001 conducted the three-day exercise "INFORMO 2001". The goals were to review the information assurance process established after 1997 and to train a newly-established Special Task Force on Information Assurance (SONIA).[663]

Information Assurance Policy

The overall information assurance policy as defined in Switzerland over the past few years is based on four pillars.[664] The overall responsibility lies with the Federal Strategy Unit for Information Technology (ISB).

1 Prevention: Suitable preventive measures must be implemented to limit the number of incidents;
2 Early recognition: Dangers and threatening situations have to be recognized as early as possible to provide the necessary defensive measures or to avoid particularly vulnerable technology. The Reporting and Analysis Center for Information Assurance (MELANI) is the main actor in this field.
3 Crisis management: The effects of disruptions on society and the state must be kept to a minimum. The major actors in charge for this are the Special Task Force on Information Assurance (SONIA), together with MELANI and the Federal Office for National Economic Supply (NES), which includes the ICT Infrastructure Unit.
4 Technical problem solution: The technical causes of the disruption must be identified and corrected. This area is covered by MELANI together with the experts in charge in the private sector.

It is a tenet of Swiss information assurance policy that all four of the above pillars, or principles, must be taken into account to achieve a complete and strong system of CIP/CIIP.

663 http://www.sfa.admin.ch.
664 In 2002, the ISB started to develop the concept of the four pillars of Switzerland's information assurance policy. Verletzliche Informationsgesellschaft, op. cit. Updated information on the four pillars is also available at: http://www.efd.admin.ch/d/dok/faktenblaetter/efd-schwerpunkte/5_infosicherheit.htm.

Risk Analysis InfoSurance Foundation and Federal Office for National Economic Supply (NES)

The former InfoSurance Foundation[665] started its work in 2002 with the initiation of a nation-wide risk analysis covering various sectors and branches such as telecommunications, finance, energy (electricity), emergency and rescue services, transportation and logistics, and health care. The risk analysis focuses on interdependencies of information infrastructures both within and between the various sectors. The same methodological guidelines are employed for all sectors. Some of the sectoral risk analyses have been completed, while others are still being carried out. Since 2004, the Federal Office for National Economic Supply (NES) has been responsible for working out and reworking the risk analysis in cooperation with the private-sector experts.

Organizational Overview

Public Agencies

Federal Strategy Unit for Information Technology (ISB)

One of the main bodies is the Federal Strategy Unit for Information Technology (Informatikstrategieorgan Bund, ISB).[666] It is subordinate to the Swiss Federal Department of Finance (EFD). The ISB reports to the EFD and is charged with producing instructions, methods, and procedures for the federal administration's information security. It collects data on incidents within the Swiss federal government and is responsible for the Special Task Force on Information Assurance (SONIA) and for the Reporting and Analysis Center (MELANI; see also Early Warning).[667] The ISB is also responsible for the implementation of the Swiss information assurance policy.

665 http://www.infosurance.ch.
666 Informatikstrategieorgan Bund (ISB). http://www.isb.admin.ch/internet.
667 http://www.isb.admin.ch/internet.

Federal Office for Communication (OFCOM)

The Federal Office for Communication (OFCOM)[668] is the main regulatory body in the field of telecommunications and ICT in Switzerland. The OFCOM studies various aspects of the information revolution. It includes consumer protection and management of the frequency spectrum as well as conformity assessment rules in the telecommunications equipment area. The OFCOM deals with risks affecting the information society, such as the formation of a new two-tier society, information overload and the resulting inability to analyze problems and make decisions, and new opportunities for the manipulation of information of a technical, political, or economic nature.

Federal Office for National Economic Supply (NES)

The Federal Office for National Economic Supply (NES)[669], which includes the ICT Infrastructure Unit, reports to the Swiss Federal Department of Economic Affairs. Its main task is to ensure that the Swiss population is able to obtain vital goods and services at all times. The NES provides governmental support when the private sector is unable to resolve supply problems on its own. However, measures to ensure a steady flow of supplies to the national economy would only be undertaken if the free-market system were seriously disrupted. In the four pillars of the Swiss information assurance policy, the NES plays an important role in the field of damage limitation.

Federal Office of IT, Systems and Telecommunication (FOITT)

The Swiss Federal Office of IT, Systems and Telecommunication (FOITT)[670] reports to the Swiss Federal Department of Finance. Its responsibilities include security and emergency preparedness for the federal administration's information systems on an operational level.

668 Bundesamt für Kommunikation (BAKOM). http://www.bakom.ch/en/index.html.
669 Bundesamt für Wirtschaftliche Landesversorgung (BWL). http://www.bwl.admin.ch/english/default.asp.
670 Bundesamt für Informatik und Telekommunikation (BIT). http://www.efd.admin.ch/e/dasefd/aemter/bit.htm.

Coordination Unit for Cybercrime Control (CYCO)

Citizens can report suspected internet crimes, including unlawful entry into IT systems, spreading of computer viruses, destruction of data, and similar offenses to the Swiss Coordination Unit for Cybercrime Control (CYCO)[671], which is part of the Federal Office of Police (Fedpol). The offenses reported are then forwarded to the respective national or foreign prosecution authorities. CYCO also looks out for criminal content on the internet and is responsible for in-depth analysis of cyber-crime. Moreover, it cooperates closely with MELANI.

Federal Department of Defense, Civil Protection, and Sports (DDPS)

The Department of Defense, Civil Protection, and Sports (DDPS)[672] conducts information operations as a standard line of operations and prepares its forces to counter the challenge of the information revolution (this includes a concept for Networked Effects-Based Operations). Protection against information operations and information warfare is seen as crucial for the functioning of the Swiss army, but also for the Swiss society and its economy. Therefore, the lessons learned from the conceptual design of the military information operation capability will be used to prepare the civilian world to cope with this mode of conflict and the threat it constitutes. This task will be fulfilled in co-operation between the Swiss army, the private sector, academic institutions, and foreign partners.[673]

Public-Private Partnerships

Switzerland has a long-standing tradition of public-private partnerships. Historically, this is due to the tradition of part-time service in a strong militia system, both in the military and in politics, in particular in the Federal Office for National Economic Supply (NES).

671 Koordinationsstelle Internet-Kriminalität (KOBIK). http://www.cybercrime.admin.ch/e/index.htm.

672 Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS). http://www.vbs.admin.ch/internet/vbs/en/home.html.

673 http://www.vbs.admin.ch/internet/vbs/de/home/documentation/news/050715a.html.

InfoSurance Association

InfoSurance was established as a foundation in 1999 by a number of companies with the support of the Swiss government. Today, it is an association that aims to increase awareness of the information assurance issue and to establish networks of cooperation among the various players. The association aims at creating a closely-linked network that promotes the organizational and structural conditions for recognizing and analyzing Switzerland's growing dependency on information technologies and the associated risks. InfoSurance's target group consists of small and medium-sized enterprises, and the focus lies on prevention.[674]

Federal Office for National Economic Supply (NES): ICT Infrastructure Unit (ICT-I)

Another important public-private partnership is the NES. It works in close cooperation with the private sector as well as with cantonal and municipal authorities. The federal government has requested that the NES deal with all prolonged disruptions of the information and communication infrastructures affecting the whole of Switzerland (ICT Infrastructure Unit, ICT-I).[675] The NES also conducts sector-specific risk analysis in cooperation with the private-sector experts involved. These analyses were formerly conducted by the Infosurance association.

CLUSIS

The non-profit association CLUSIS[676] has existed in Switzerland since 1989 and represents about 230 members, including Swiss public administrations, IT suppliers, providers, banks, industries, consultants, etc. CLUSIS organizes seminars related to information security practices and technologies, issues whitepapers and publications, and is involved in education. The aim is to provide networking opportunities for their members and to share experiences. CLUSIS mainly covers the French and Italian parts of Switzerland.

674 http://www.infosurance.ch.
675 http://www.bwl.admin.ch/deutsch/themen-infra-ict.asp.
676 http://www.clusis.ch.

Early Warning and Public Outreach

A central office for early warning in CIIP has been established at the federal level. It is known as the Reporting and Analysis Center for Information Assurance (Melde- und Analysestelle Informationssicherung, MELANI). For this office, Switzerland has chosen a cooperation model, which means that various partners already fulfilling similar tasks will work together. In terms of functionality and efficiency, this was seen as the most suitable model for CIIP early warning in Switzerland.[677]

The Reporting and Analysis Center for Information Assurance (MELANI)

On 29 October 2003, the government decided to create an authority that would collect information on the security of the IT infrastructure, especially of the internet. This new authority, called the Reporting and Analysis Center for Information Assurance (MELANI)[678], has been operational since October 2004 and is now the core of the Swiss CIIP early warning system. It is on duty 24 hours a day. MELANI is directed by the Federal Strategy Unit for Information Technology (ISB) and is structured as a permanent body. It plays a role in all four pillars of the Swiss information assurance policy. In addition to its own investigations, it depends on close cooperation with the public and private sectors. The three partners of MELANI have the following main tasks:[679]

- The Federal Strategy Unit for Information Technology (ISB) is responsible for strategic issues and the management of MELANI;
- The Federal Office of Police (fedpol) operates the MELANI analysis center and is responsible for collecting, condensing, and presenting operational information from different sources in the public and private sectors;

677 Rytz, Ruedi and Jürg Römer. "MELANI – An Analysis Centre for the Protection of Critical Infrastructures in the Information Age". Paper for the Workshop on Critical Infrastructure Protection (CIP) in Frankfurt a. M., 29–30 September 2003 (available at http://www.isb.admin.ch), p. 4, and OFCOM. 5th Report of the Information Society Coordination Group (ISCG) to the Federal Council (June 2003), p. 49.

678 Melde- und Analysestelle Informationssicherung (MELANI). http://www.melani.admin.ch.

679 Rytz, Ruedi and Jürg Römer, op. cit., pp. 4–5, and OFCOM: 5th ISCG Report, op. cit., p. 49.

- The Swiss Education and Research Network (SWITCH) operates the Computer Emergency Response Team (SWITCH-CERT) and is responsible for dealing with technical incidents, in particular concerning the internet and computer operating systems.

MELANI's website has two domains:

- MELANI-Net offers selected operators of national, critical infrastructures analyses pertaining to early recognition of attacks as well as coordination of measures in the event of incidents (accessible only with login);
- MELANI is open to private users and small and medium-size enterprises (SMEs) in Switzerland. It offers information on threats and risks when using modern information and computer technology (such as computers, internet, mobile phones, e-banking); news about current threats and advice for protecting data; and an incident-reporting form.

Special Task Force on Information Assurance (SONIA)

The Special Task Force on Information Assurance (SONIA)[680] is also directed by the Federal Strategy Unit for Information Technology (ISB). SONIA is a crisis-management organization and constitutes the core element of the third pillar of the Swiss information assurance policy, namely damage limitation. Its main task is to advise the Swiss Federal Council and senior management representatives from the private sector in crisis situations and to act as a link between the public and private sectors.[681] SONIA would take charge after a breakdown in the information and communication infrastructure that resulted in (massive) disruptions in CI. Unlike MELANI, it is not a permanent body, but would only be convened for damage limitation in genuine crises.
SONIA is mainly supported by the following organizations:

680 Sonderstab Information Assurance (Sonia).
681 OFCOM: 5th ISCG Report, op. cit., p. 48.

- The ICT Infrastructure Unit of NES, to raise awareness and to give guidance in threat and risk analysis, and to establish contacts among the experts in charge in the private sector.
- MELANI, as a provider of reliable information about a possible imminent threat and its consequences, and as an information base in case of a crisis.[682]

SWITCH-CERT

On a technical level, the Computer Emergency Response Team of the Swiss Academic and Research Network (SWITCH-CERT) helps its customers (infrastructure operators through MELANI, universities and other institutes of learning) to manage information security problems. SWITCH represents the interests of Switzerland as a research center in numerous bodies, and therefore makes an important contribution to the development and operation of the internet in Switzerland. It works closely together with MELANI.[683]

Law and Legislation

Swiss Penal Code

A number of articles in the Swiss Penal Code are of relevance in the context of CIIP.

Article 143 (unauthorized procurement of data)

Article 143bis (unauthorized access to a computing system)
This article states that any person who, by means of a data transmission device, gains unauthorized access to a computing system belonging to others that is specially protected against access by the intruder shall be punished by imprisonment or a fine if a complaint is made.[684]

682 Haefelfinger, Rolph L. "The Swiss Perspective on Critical Infrastructure". Presentation at the PfP Seminar on Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century (Stockholm, 17–18 November 2003).
683 http://www.switch.ch/about.

Article 144 (damage to property)
The article states that any person who damages, destroys, or renders unusable any property belonging to others, shall be punished by imprisonment or a fine if a complaint is made.[685]

Article 144bis (damage to data)
The article states that any person who alters, deletes, erases, or renders unusable data stored or transferred by electronic or similar means without authorization, shall be punished by imprisonment or a fine if a complaint is made.[686]

Article 147 (fraudulent use of a computer)
The article states that any person who, with the intention of unlawfully obtaining financial rewards for himself or another, interferes with an electronic procedure through the unauthorized use of data, shall be punished by community service of up to five years or imprisonment.[687]

Switzerland's laws against virus creation and the use of malicious software in general are widely applicable. However, the structure of the Swiss legal system makes prosecution difficult, due to the complexities of different laws (comprising laws on both the federal and cantonal level) and law enforcement procedures. Although the Swiss Penal Code is up to date, only a few cases have been prosecuted so far.

In November 2001, the Federal Council accepted the "Convention on Cybercrime of the Council of Europe".[688] It should be noted that the Swiss Penal Code already conforms with the corresponding international articles on infringements of copyright, computer-related fraud, child pornography, and offenses related to unauthorized intrusion into protected computer systems.

684 Based on the official English translation of the Swiss Penal Code.
685 Based on the official English translation of the Swiss Penal Code.
686 Based on the official English translation of the Swiss Penal Code.
687 Based on the official English translation of the Swiss Penal Code.
688 ISPS News (Infosociety.ch) press release: Gemeinsam die Cyber-Kriminalität bekämpfen. Bundesrat genehmigt Konvention des Europarats. http://www.infosociety.ch/site/default.asp.

United Kingdom

Critical Sectors

In the United Kingdom, the Critical National Infrastructure (CNI) comprises those parts of the infrastructure for which "the continuity is so important to national life that loss, significant interruption, or degradation of service would have life-threatening, serious economic or other grave social consequences for the community or would be of immediate concern to the Government."[689] Many of the critical services that are essential to the well-being of the UK depend on IT and are provided by both the public and private sectors. The term "national" has been adopted to indicate infrastructures that are critical to the UK's national interest.[690]

The ten sectors and 39 sub-sectors that comprise the CNI reflect the government's current classification of what is critical to UK interests in terms of vulnerabilities to physical and electronic attack and from the perspective

* The Country Survey of the United Kingdom 2006 was reviewed by John Neil Park of the National Infrastructure Security Co-ordination Centre (NISCC).

689 http://www.niscc.gov.uk/niscc/aboutCNI-en.html.

690 Information provided by NISCC expert.

of civil contingency planning. This comprehensive list is therefore used by all UK agencies involved in CIP, CIIP, or emergency management:[691]

- Communications (Data Communications, Fixed Voice Communications, Mail, Public Information, Wireless Communications),
- Emergency Services (Ambulance, Fire and Rescue, Marine, Police),
- Energy (Electricity, Natural Gas, Petroleum),
- Finance (Asset Management, Financial Facilities, Investment Banking, Markets, Retail Banking),
- Food (Produce, Import, Process, Distribute, Retail),
- Government and Public Services (Central Government, Regional Government, Local Government, Parliaments and Legislatures, Justice, National Security),
- Public Safety (Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism; Crowds and Mass Events),
- Health (Health Care, Public Health),
- Transport (Air, Marine, Rail, Road),
- Water (Mains Water, Sewage).

Past and Present Initiatives and Policies

e-commerce@its.best.uk

The UK approach to the information society was laid out in 1998 by the Department of Trade and Industry's "Competitiveness White Paper" that noted the major role played by ICT in facilitating economic growth.[694] In September 1999, the Performance and Innovation Unit (now the Cabinet Office's Strategy Unit)[695] issued "e-commerce@its.best.uk", a report outlining the organizational and policy framework for achieving these goals.[696] The report's recommenda-

691 Ibid.
694 Department of Trade and Industry. UK Digital Content: An Action Plan for Growth (1998). http://www.dti.gov.uk/comp/competitive/wh_int1.htm.
695 http://www.strategy.gov.uk.
696 Performance and Innovation Unit Report: e-commerce@its.best.uk (September 1999). http://www.strategy.gov.uk.

tions have been implemented under a national strategy known as UK Online, which gives access to government information and services online.[697]

UK Online Strategy

The UK Online Strategy is overseen by the e-minister and the e-envoy, who report directly to the prime minister. The e-envoy is responsible for ensuring that all government services are available electronically and supports government plans to develop the UK as a world leader for electronic business.[698] The "UK Online Action Plan" includes 113 detailed recommendations covering 26 commitments to ensure that the UK is at the forefront of the knowledge economy revolution.[699]

Progress Report on Electronic Security

The e-minister and the e-envoy delivered their progress report on electronic security to the prime minister on 3 March 2003.[700] The key developments highlighted in the report were:

- The National Hi-Tech Crime Unit (NHTCU) has developed a confidentiality charter to address the concerns of business, which has traditionally been reluctant to report IT incidents;
- The Office of the e-Envoy/Central Sponsor for Information Assurance (CSIA) has published a complete set of security frameworks describing measures that organizations should take to secure their electronic service delivery systems against assessed risks;
- The Office of the e-Envoy/CSIA has also published advice on the selection of biometrics products, which are of increasing interest;
- The Office of the e-Envoy has published guidelines for the registration of individuals and organizations with governmental electronic services, and a generic Information Security Policy Document that public-sector organizations can use to develop their own security policies;

697 http://www.direct.gov.uk/Homepage/fs/en.

698 http://archive.cabinetoffice.gov.uk/e-envoy/index-content.htm; and http://www.direct.gov.uk/Homepage/fs/en.

699 Ibid.

700 Monthly Report from the e-Minister and e-Envoy (3 March 2003). http://archive.cabinetoffice.gov.uk/e-envoy/index-content.htm.

- CSIA is supporting the National Infrastructure Security Co-ordination Centre (NISCC) in establishing the first Warning, Advice and Reporting Point (WARP) in partnership with London Connects, the agency responsible for delivering electronic government (e-government) services in London.

In the meantime, the Office of the e-Envoy has ceased to exist. The Cabinet Office has now taken on its function.

CIIP Policy Guidelines

The British government aims at protecting the CNI from two kinds of threat: terrorist attacks against installations and equipment on the one hand, and electronic attacks against computers or communications systems on the other hand.

The government has produced an information assurance strategy called "Information Assurance Governance Framework — Working in partnership for a secure and resilient UK information infrastructure". The document, published on the internet on 22 November 2005, complements counter-terrorism strategies, national security considerations, and measures against high-tech crime. The aim of the strategy is to provide ongoing assurance to the government that the risks to information systems underpinning key public interests are appropriately managed. Most importantly, the strategy recognizes that within an increasingly interdependent and interconnected information infrastructure, the government must concern itself with the confidentiality, availability, and integrity of all information systems. The Central Sponsor for Information Assurance (CSIA), a unit within the UK Cabinet Office, is the coordinating body for the strategy, working alongside other key government bodies.

Organizational Overview

In the UK, the main responsibility for CIIP lies with the home secretary.[701] However, a number of other departments play a role in the protection of the various CNI sectors and contribute resource and expertise to the British CIIP effort. These contributions are coordinated by an interdepartmental center that reports to the Home Office — the National Infrastructure Security Co-ordination Centre (NISCC). Policy is formulated and developed at a working level through a dialog between several government departments and bodies: NISCC; the Central Sponsor for Information Assurance (CSIA); the Civil Contingencies Secretariat (CCS); the Cabinet Office Security Policy Division; and the Home Office itself. The various roles and responsibilities of these governmental bodies are described below.

While NISCC has the lead in coordinating CIIP efforts within the government and with the private sector, other responsibilities reside with a number of bodies:

- CIIP is a subset of CIP: the provision of physical protective security advice to the CNI is the responsibility of the Security Service and the police;
- CIIP (focusing only on the CNI) is also a subset of the wider information assurance strategy dealing with all aspects of the information society. Responsibility for this lies with the Central Sponsor for Information Assurance;
- The coordination of the government's contingency and emergency response effort (regardless of the cause of the disruption) is the responsibility of the Civil Contingencies Secretariat within the Cabinet Office.

Public Agencies

National Infrastructure Security Co-ordination Centre (NISCC)

The protection of the CNI from electronic attack has been the responsibility of the National Infrastructure Security Co-ordination Centre (NISCC) since

701 http://www.homeoffice.gov.uk.

20 December 1999. NISCC is an interdepartmental center that coordinates and develops existing work within government departments and agencies as well as CNI organizations in the private sector.

NISCC operates under a director who reports to an executive board made up of contributors from the Cabinet Office, the Communications Electronics Security Group (CESG — the government's technical authority on information security), the Home Office, and the Security Service. Two stakeholder groups representing the private and public-sector organizations responsible for the CNI also provide directional input to NISCC through the director and the executive board.

NISCC aims to establish partnerships with CI providers. It has various duties towards its CNI partners across the UK:

- Promoting dialog with owners of CI systems to identify the most critical systems;
- Issuing alerts or warnings of attack;
- Providing assistance in response to serious attacks;
- Collecting, analyzing, and disseminating information about the threat;
- Undertaking research into vulnerabilities;
- Offering specialist protective security advice and expertise.[702]

NISCC provides a range of government and other organizations with access to resources, expertise, and knowledge. It either carries out research itself or sponsors work in a variety of fields connected with electronic attack and information security. It bases its threat assessments on a variety of sources, including sensitive intelligence, overseas security and intelligence partners, open-source material, and the reports of those who have experienced electronic attack.

NISCC passes information, such as warnings of specific threats and vulnerabilities, to CNI partners so that operators can install suitable defenses, and offers periodic assessments of the nature of the threat from electronic attack. NISCC information on vulnerabilities and alerts is disseminated through UNIRAS, the UK government CERT, a component of the NISCC.[703]

702 http://www.niscc.gov.uk.
703 http://www.niscc.gov.uk/niscc/aboutCNI-en.html.

NISCC works with vendors and researchers to co-ordinate the release of vulnerabilities in a controlled way, so that "fixes" are in place before the software weaknesses are publicly disclosed. This work enhances the understanding of the potential impact of vulnerabilities.

Other Government Departments and NISCC

The following government departments contribute to the CIIP effort through NISCC, in addition to their own wider departmental roles and responsibilities:

- The Cabinet Office contributes policy and coordination; its own units — the Civil Contingencies Secretariat (CCS) and the Central Sponsor for Information Assurance (CSIA) — work closely with the NISCC.
- The Communications-Electronics Security Group (CESG) is the information assurance arm of the Government Communications Headquarters (GCHQ), and is the national technical authority on information security. The CESG aims to protect the communications and information of central government departments, agencies, and other parts of the national information infrastructure by developing technical means of countering assessed threats. The CESG delivers information-assurance policy and offers technical recommendations and authoritative advice on assessing current and foreseeable risks.[704]
- The Department of Trade and Industry (DTI) has several CIIP-related responsibilities, and assists the NISCC by promoting ISO-17799; by having departmental responsibility for the energy and telecommunications sectors; and by encouraging information assurance for SMEs. Fact-sheets and guides on various information security topics can be downloaded for free from the DTI homepage.[705]
- The Home Office is the reporting line for NISCC; it chairs the NISCC Management Board; and its press office responds to press enquiries on NISCC- or CIIP-related topics.

704 http://www.gchq.gov.uk/about/cesg.html.
705 http://www.dti.gov.uk/industries/information_security/downloads.html.

- The Ministry of Defence (MoD) contributes technical and research efforts; as part of the CNI, the MoD's own hierarchical set of CERTS work closely with UNIRAS. The Defence Research Centre (DSTL) carries out research into CIIP for both the MoD and NISCC.
- Police: the crime prevention and attack investigation roles of police high-tech crime units complement the CIIP effort of NISCC. In particular, the National High Tech Crime Unit (NHTCU) is a close partner of NISCC. NISCC itself is not a criminal investigation or police authority; and where a CII incident requires a police response, the NHTCU would lead.
- The Security Service contributes expertise on threat investigation, intelligence, and protective security to the NISCC. Its CIIP contribution to the NISCC complements its physical counter-terrorist protective security role, as described above.
- The Security Service's National Security Advice Centre (NSAC) contributes to the protection of key government assets and the UK's Critical National Infrastructure (CNI) in general, such as transport, power, and water, and to the reduction of their vulnerability to terrorism and other threats. Much of NSAC's advice is relevant to a broad range of other organizations, private and public, and is now available in the Security Advice section of its website. NSAC's remit extends to advice on physical and personnel protective security. NSAC works closely with the National Infrastructure Security Coordination Centre (NISCC).[706]

Central Sponsor for Information Assurance (CSIA)

The Central Sponsor for Information Assurance (CSIA) was officially formed as a unit within the UK Cabinet Office on 1 April 2003. CSIA promotes information assurance and information risk management across government as well as for industry and the public. The unit's responsibilities are:

- To provide a nationwide strategic direction for Information Assurance (IA);
- To co-ordinate and complement the activities of parties contributing to IA;
- To sponsor activities that benefit IA;

706 http://www.mi5.gov.uk/output/Page76.html.

- To accredit pan-government systems and, in some cases, such as the Government Secure Intranet (GSI), own the risk to shared information;
- To identify and address vulnerabilities in national telecommunications systems, and to resolve them in conjunction with other organizations such as the NISCC.

In 2004, CSIA published a comprehensive document on "Protecting our information systems – Working in Partnership for a secure and resilient UK information infrastructure".[707] The document sets out the government's approach to dealing with the various risks and threats facing information systems across the UK. It supports the UK Government Strategy for Information Assurance.

Civil Contingencies Secretariat (CCS)

The Civil Contingencies Secretariat (CCS) is part of the Cabinet Office. It was established in July 2001, and reports to the prime minister through the security and intelligence coordinator and permanent secretary to the Cabinet Office. It was set up to improve the resilience of central government and the UK. Resilience is defined as the ability to handle disruptive challenges that can lead to or result in crisis. Disruptive challenges may arise from many causes – including, but not limited to, individual crises.

Like all Cabinet Office Secretariats, the CCS supports ministers collectively. Specifically, it services the Civil Contingencies Committee, which is chaired by the home secretary and deals with managing and exercising arrangements to handle individual crises as they arise. The CCS is organized around three divisions: An assessments division, which evaluates potential and evolving threats; an operations division, which develops and reviews departmental continuity and contingency plans; and a policy division, which gives the Cabinet Secretariat support in consequence management.

The aim of the CCS is to improve the UK's resilience to disruptive challenge by working with others inside and outside government on the anticipation, preparation, prevention, and resolution of threats. Its current objectives are:

707 http://www.cabinetoffice.gov.uk/csia/documents/pdf/CSIA_booklet.pdf.

- To identify and assess potential and imminent disruptive domestic challenges and assist in the development of an integrated response;
- To build partnerships with other organizations to develop and share best practices in horizon-scanning, and to develop the knowledge of the UK's critical networks and infrastructures;
- To ensure that the government can continue to function and deliver public services during crises; to ensure, in collaboration with departments and other secretariats in the Cabinet Office, that plans and systems to cover the full range of potential disruption are in place and exercised;
- To improve resilience to disruption across government and the public sector, by supporting ministers in developing policy, agreeing priorities, and planning assumptions, and by ensuring that core response capabilities are developed accordingly;
- To improve — at all levels of government, the wider public sector, and the private and voluntary sectors — the capability to prepare for, respond to, and manage potential challenges by developing key skills and awareness.

The Emergency Planning College is an integral part of the CCS. It has a key role to play in the development and promulgation of the UK's resilience doctrine, and in the development of cross-organizational communities to deliver it.

Public-Private Partnerships

NISCC's Public-Private Partnerships

In addition to its assurance advice to specific CNI companies, the National Infrastructure Security Co-ordination Centre (NISCC) actively promotes two types of information-sharing initiatives.

The first type of initiative consists of Information Exchanges, where the NISCC facilitates and attends periodic confidential industry forums. Currently, representatives from over 144 private companies share information with each other and with the government under the initiative. There are currently seven exchanges: aviation, government, managed-service providers, telecommunications industry, finance, those sectors that use process control

or Supervisory Control and Data Acquisition (SCADA) technologies, and vendors. Sensitive information is shared in person at Information Exchange meetings, but is anonymized when passed to other Information Exchanges, or to a wider CIIP audience.[708]

Warning, Advice, and Reporting Points (WARPs) are an NISCC initiative designed to create and foster small, community-based, interlinked information-sharing cells. They offer a cost-effective alternative to CERTs and ISACs. Currently, there are eight operational WARPs. The model is widely promoted beyond the CNI and has been adopted into other initiatives.[709]

Information Assurance Advisory Council (IAAC) and other Public-Private Partnerships

There is a wide range of private-sector bodies that work with the public sector to promote information assurance.

The Information Assurance Advisory Council (IAAC), founded in 2000, is not part of the UK government, but has government representation. It fosters public-private partnerships between corporate leaders, policy-makers, law enforcement, and the research community to address the challenges of information infrastructure protection. The IAAC makes policy recommendations to government and corporate leaders at the highest levels.[710] The IAAC facilitates cross-sectoral dialog, information exchange, and the emergence of new trusted long-term partnerships. The IAAC has active links with the NISCC, the Department of Trade and Industry (DTI), and the Office of Science and Technology (OST), as well as with the private sector and the military. The IAAC has five working groups dealing with threat assessment, risk assessment, standards, research and development, and education and outreach.[711]

708 http://www.niscc.gov.uk/niscc/infoShareConcepts-en.html.
709 http://www.niscc.gov.uk/niscc/warpInfo-en.html.
710 http://www.iaac.org.uk.
711 Parsons, T. J. "Protecting Critical Information Infrastructures. The Co-ordination and Development of Cross Sectoral research in the UK". Plenary address at "The Future of European Crisis Management" (Uppsala, March 2001). http://www.krisestyring.dk/krisestyring/uppsala/uppsala.pdf.
712 http://www.bcs.org/bcs.
713 http://www.ncc.co.uk/index.cfm.
714 http://www.iwf.org.uk.

Other public-private partnerships include the British Computer Society (BCS),[712] the Internet Security Forum, the National Computing Centre,[713] the Internet Watch Foundation,[714] and the Confederation of British Industry.[715]

Early Warning and Public Outreach

Unified Incident Reporting and Alert Scheme (UNIRAS)

UNIRAS is the UK Government Computer Emergency Response Team (CERT) and is run by the National Infrastructure Security Co-ordination Centre (NISCC). It draws on technical support from the Communications-Electronics Security Group (CESG), the UK's national technical security authority. Its original customers were government departments and agencies, but in the last few years, this group has been expanded to include companies holding sensitive government contracts, and most recently CNI organizations. UNIRAS has three main tasks:

- Response to electronic attacks and other significant IT security incidents;
- Warning about IT security incidents and vulnerabilities;
- Gathering information about IT-security incidents.

UNIRAS provides ad-hoc advice on specific problems to individual members and warnings of IT security vulnerabilities by issuing "Alerts" and "Briefings". These alerts and briefings are sent to the UNIRAS community by e-mail, but also posted on the UNIRAS website so that any company can make use of them.[716]

715 http://www.cbi.org.uk/home.html.
716 http://www.uniras.gov.uk/niscc/index-en.html.
717 http://www.first.org.
718 http://www.ti.terena.nl.

Ministry of Defence Computer Emergency Response Team (MOD-CERT)

The UK Ministry of Defence (MOD) is a member organization of both the international Federation of Incident Response Security Teams (FIRST)[717] and the Trusted Introducer (TI)[718] scheme, both of which provide a mechanism for sharing information on computer security incidents among the communities concerned. MODCERT consists of a central co-ordination center and a number of monitoring and reporting centers, Warning, Advice, and Reporting Points (WARPs), and incident response teams. It also works closely with the government CERT, UNIRAS.[719]

ITsafe: IT Security Awareness for Everyone

The ITsafe ("IT security awareness for everyone") website[720] was launched in February 2005. ITsafe is run by a small government team that looks at information from NISCC, publicly available sources, and international partners for relevant issues. ITsafe is funded by the Home Office and coordinated by the Central Sponsor for Information Assurance (CSIA) within the Cabinet Office.

It is a government initiative that aims to provide home users and micro businesses with plain advice on how to protect their computers, mobile phones, and other devices against malicious attack. The website includes a glossary of technical terms and provides free e-mail and text messaging services for everybody, including:

- Alerts: E-mails about the most critical risks,
- Bulletins: E-mails about other major risks,
- Text Messaging: Alerts sent to mobile phones.
- ITsafe News: This monthly newsletter provides summaries of bulletins and other news, including advisories from the ITsafe website.[721]

719 http://www.mod.uk/cert.
720 http://www.itsafe.gov.uk.
721 http://www.itsafe.gov.uk/signup/index.html.

The ITsafe Warning Service complements the new GetSafeOnline Public-Private initiative, which provides a variety of advice for online users of computers.[722]

GetSafeOnline

The UK government and business have joined together to launch a new initiative designed to educate the public about IT security. GetSafeOnline[723] is the result of collaboration between the government and private-sector companies, and is sponsored by CSIA, DTI, the Home Office, NISCC, and private sponsors from the technology, retail, and finance sectors.[724] The website has been available since October 2005. It offers comprehensible advice on safe internet use for the home user and for micro-businesses. The aim of the service is to reduce occurrences of ID theft, viruses, and spam by educating internet users.[725]

Law and Legislation

The UK has created a legal framework to protect information systems, such as the Telecommunications (Fraud) Act 1997; the Data Protection Act 1998; the Electronic Communications Bill 2000; and the Terrorism Act 2000, which makes the deliberate interference in or disruption of electronic systems a criminal act.

Computer Misuse Act 1990

Chapter 18

1. Unauthorized access to computer material

(1) A person is guilty of an offence if–

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

722 http://www.itsafe.gov.uk/partners/landing-gso.html.
723 http://www.getsafeonline.org.
724 http://www.getsafeonline.org/nqcontent.cfm?a_id=1073.
725 http://www.getsafeonline.org/nqcontent.cfm?a_id=1366.

(2) The intent a person has to have to commit an offence under this section need not be directed at–

(a) any particular program or data;
(b) a program or data of any particular kind; or
(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

2. Unauthorized access with intent to commit or facilitate commission of further offences

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above («the unauthorised access offence») with intent–

(a) to commit an offence to which this section applies; or
(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences–

(a) for which the sentence is fixed by law; or
(b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—
(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

3. Unauthorized modification of computer material

1) A person is guilty of an offence if–
(a) he does any act which causes an unauthorised modification of the contents of any computer; and
(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing–
(a) to impair the operation of any computer;
(b) to prevent or hinder access to any program or data held in any computer; or
(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at–
(a) any particular computer;
(b) any particular program or data or a program or data of any particular kind; or
(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any

computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable–
(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and
(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.[726]

Police and Justice Bill 2006

The Police and Justice Bill was introduced in the House of Commons on 25 January 2006. This Public Bill includes a proposal of amending the Computer Misuse Act 1990[727] and prepares for a ratification of the Council of Europe Convention on Cybercrime.[728] The Police and Justice Bill includes increasing the maximum sentence for hacking from five to ten years, and classifying Denial of Service (DoS) attacks as a criminal offence. The bill also contains provisions to ban the development, ownership and distribution of "hacker tools".[729]

726 http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm.
727 Part 5 Articles 33–36.
728 http://www.cybercrimelaw.net/countries/uk.html.
729 NISCC Monthly Bulletin, January 2006, p. 4. http://www.niscc.gov.uk./niscc/docs/re-20060131-00112.pdf?lang=en.

United States

Critical Sectors

Critical Infrastructure Protection (CIP) in the US refers to the protection of infrastructure critical to the people, economy, essential government services, and national security. The main goal of the US government's efforts is to ensure that any disruption of the services provided by this infrastructure is infrequent, of minimal duration, and manageable.[730]

In the US, critical infrastructures are defined[731] according to the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001", section 1016(e): "[…] the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[732]

* The Country Survey of the United States 2006 was reviewed by Scott C. Algeier, Executive Director IT-ISAC, and Erica B. Russel, Deputy Coordinator for International Critical Infrastructure Protection Policy, Department of State.

730 Moteff, John D. CRS (Congressional Research Service) Report for Congress. Critical Infrastructures: Background, Policy, and Implementation (updated 4 February 2002). http://www.fas.org/irp/crs/RL30153.pdf.

731 The White House. Homeland Security Presidential Directive/HSPD-7 (Washington, 17 December 2003). http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

732 http://www.epic.org/privacy/terrorism/hr3162.html.

On December 17, 2003, US President George Bush issued Homeland Security Presidential Directive 7/HSPD-7 clarifying executive agency responsibilities for identifying, prioritizing, and protecting critical infrastructure. This directive requires that the Department of Homeland Security (DHS) and other federal agencies collaborate with private-sector entities in sharing information and protecting critical infrastructure. HSPD-7 adopts the critical infrastructure and key asset categories in the "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets".[733] However, HSPD-7 does revise the list of lead federal agencies and associated critical infrastructures included in the Presidential Decision Directive/PDD-63 to reflect the role of the DHS as an independent cabinet department. Although HSPD-7 specifies a list of infrastructures, it leaves open the possibility that the list could be expanded. According to the directive, the DHS "shall [...] evaluate the need for and coordinate the coverage of additional critical infrastructure and key resources categories over time, as appropriate" (Section 15). HSPD-7's list of critical infrastructures is the most recent and still in force:[734]

- Information Technology,[735]
- Telecommunications,[736]
- Chemicals,[737]
- Transportation Systems (including Mass Transit, Aviation, Maritime, Ground/Surface, and Rail and Pipeline Systems),[738]
- Emergency Services,[739]
- Postal and Shipping Services,[740]
- Agriculture, Food (Meat, Poultry, Egg Products),[741]

733 The White House. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Washington, February 2003). http://www.whitehouse.gov/pcipb/physical_strategy.pdf.
734 Moteff, John and Paul Parfomak. CRS (Congressional Research Service) Report for Congress. Critical Infrastructure and Key Assets: Definition and Identification (1 October 2004), p. 9–10. http://www.fas.org/sgp/crs/RL32631.pdf.
735 Responsible: Department of Homeland Security (DHS).
736 Ibid.
737 Ibid.
738 Ibid.
739 Ibid.
740 Ibid.
741 Responsible: Department of Agriculture.

- Public Health, Healthcare, and Food (other than Meat, Poultry, Egg Products),[742]
- Drinking Water and Waste Water Treatment Systems,[743]
- Energy, including the Production Refining, Storage, and Distribution of Oil and Gas, and Electric Power (except for commercial nuclear power facilities),[744]
- Banking and Finance,[745]
- National Monuments and Icons,[746]
- Defense Industrial Base.[747]

Past and Present Initiatives and Policies

There have been several efforts since the 1990s to better manage Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) in the US. CIIP plays an important role in the overall US security strategy. The US government views CIIP as an element of its homeland security strategy. Where traditionally, national security has been recognized as the responsibility of the federal government and is underpinned by the collective efforts of the military, the foreign policy establishment, and the intelligence community with respect to defense, homeland security is viewed as a shared responsibility that requires coordinated action across many sectors.[718]

The US government is especially committed to CIIP, as evidenced by President George Bush signing a US$37.4 billion Homeland Security appropriations bill for 2004. US$839.3 million was allocated specifically to the Information Analysis and Infrastructure Protection Directorate, which has responsibility for cyber-security as well as for the telecommunications and IT sector. Among other measures, this money will fund research and development in examining network weaknesses and evaluating threats and vulnerabilities.

742 Responsible: Department of Health and Human Services.
743 Responsible: Environmental Protection Agency.
744 Reponsible: Department of Energy.
745 Responsible: Department of Treasury.
746 Responsible: Department of the Interior.
747 Responsible: Department of Defence.
748 Ibid.

The following government efforts are or were aimed at developing initiatives and creating appropriate policies to address CIIP.

Presidential Commission on Critical Infrastructure Protection (PCCIP)

Based on the recommendations of the Critical Infrastructure Working Group (CIWG), President Bill Clinton set up the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996, the first national effort to address the vulnerabilities of the information age.

The PCCIP included representatives from all relevant government departments as well as from the private sector. The PCCIP presented its report to the president in October 1997.[749] The commission's most important decision was to foster cooperation and communication between the private sector and the government. The commission no longer exists, as its functions have been redirected per HSPD-7.

Presidential Decision Directives (PDD) 62 and 63

Clinton followed the recommendations of the PCCIP and issued Presidential Decision Directives (PDD) 62 and 63 in May 1998.[750] Those directives established policy-making and oversight bodies making use of existing government agency authorities and expertise. PDD-63 set up groups within the federal government to develop and implement plans to protect government-operated infrastructure, and called for a dialog between the government and the private sector to develop a "National Infrastructure Assurance Plan".[751]

National Plan for Information Systems Protection

On 7 January 2000, Clinton presented the first comprehensive national plan for CIIP — focusing on securing the cyber-components of critical infrastructures,

749 The President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures (Washington, October 1997).

750 Clinton, William J., Protecting America's Critical Infrastructures: Presidential Decision Directive 63. (Washington, 22. May 1998) http://www.usdoj.gov/criminal/cybercrime/white_pr.htm.

751 Ibid.

but not the physical components – called "Defending America's Cyberspace. National Plan for Information Systems Protection – An Invitation to Dialogue Version 1.0".[752] This plan reinforced the perception of cyber-security as a responsibility shared between the government and the private sector.

Homeland Security Executive Orders

In the aftermath of 11 September 2001, President George Bush signed two executive orders (EO) affecting CIP. With EO 13228, entitled "Establishing the Office of Homeland Security and the Homeland Security Council" and issued on 8 October 2001, the Office of Homeland Security was established, headed by the assistant to the president for homeland security.[753] One of the functions of the assistant to the president is to coordinate efforts to protect the country and its CI from terrorist attacks. The EO further established the Homeland Security Council, which advises and assists the president in all aspects of homeland security.

The second executive order, EO 13231 "Critical Infrastructure Protection in the Information Age", established the President's Critical Infrastructure Protection Board. The board's responsibility is to "recommend policies and coordinate programs for protecting information systems for critical infrastructure".[754] Finally, the EO also established the National Infrastructure Advisory Council (NIAC), a presidential advisory committee of owners and operators of the nation's critical infrastructures.[755]

Homeland Security Presidential Directive/HSPD-7

On 17 December 2003, Bush released "Homeland Security Presidential Directive/HSPD-7", which supersedes PDD 63 of May 1998, and any presidential directives issued prior to this HSPD-7.

752 Clinton, William J., Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue. Version 1.0 (Washington, 2000).

753 Bush, George W. Executive Order 13228. Establishing the Office of Homeland Security and the Homeland Security Council (Washington, 8 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13228.htm.

754 Bush, George W., Executive Order 13231. Critical Infrastructure Protection in the Information Age (Washington, 16 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

755 Ibid.

This new directive established a national policy for federal departments and agencies to identify and prioritize US critical infrastructure and key resources and protect them from terrorist attack. It identified the government agencies responsible for coordinating the protection of specific critical infrastructure sectors. A key element of this directive is the designation of federal sector-specific agencies that are charged with collaborating with specific elements of the private sector.

Also, the HSPD-7 required that that by July 2004, the heads of all federal departments and agencies develop plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate, including identification, prioritization, protection, and contingency planning.[756]

Finally, HSPD-7 designated the secretary of homeland security as "the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources".

National Strategies

On 14 February 2003, the White House released two presidential national strategies that are follow-on documents to the National Strategy for Homeland Security, which was released in July 2002.

The main aim of the National Strategy to Secure Cyberspace is to set national policies to engage US citizens in securing the portions of cyberspace they own, operate, control, or with which they interact.

The main aim of the National Strategy for Physical Protection of Critical Infrastructure and Key Assets is to reduce the nation's vulnerability to acts of terrorism by reducing the vulnerability of national critical infrastructure and key assets to physical attack.

National Strategy for Homeland Security

As a result of 11 September 2001, the Office of Homeland Security in July 2002 issued the "National Strategy for Homeland Security"[757] to secure the US

756 http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

757 Office of Homeland Security. National Strategy for Homeland Security, (Washington, July 2002). http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

homeland from terrorist attacks. It provides direction to the federal government departments and agencies that have a role in homeland security. One of the six "critical mission areas" identified in the strategy is protecting critical infrastructure and key assets. The document states that if terrorists were to attack one or more pieces of the national critical infrastructure, entire systems might be disrupted and significant damage caused to the nation. Therefore, it is essential to protect the components and interconnecting systems that make up the US critical infrastructure. To reach this aim, the strategy depicts eight major initiatives:

- To unify US infrastructure protection efforts in the Department of Homeland Security;
- To build and maintain a complete and accurate assessment of US critical infrastructure and key assets;
- To enable effective partnership between state and local governments and the private sector;
- To develop a national infrastructure protection plan;
- To secure cyberspace;
- To harness the best analytic and modeling tools to develop effective protective solutions;
- To guard US critical infrastructure and key assets against "inside" threats; and
- To cooperate with the international community to protect the transnational infrastructure.[758]

National Strategy to Secure Cyberspace

The "National Strategy to Secure Cyberspace (NSSC)" recognizes that securing cyberspace is an extraordinary challenge that requires a coordinated effort from all parts of society and government. In order to achieve this goal and to engage the public in securing cyberspace, a draft version of the NSSC was initially released for public comment, and ten town hall meetings were held around the US to gather input on its development. This careful vetting process is a clear sign that cyberspace security is viewed as an issue that requires a public-

758 Ibid., pp. 29–36.

private partnership, since the government neither owns nor operates most of the cyber-infrastructure.

The NSSC defines cyberspace as an "interdependent network of information technology infrastructures" and depicts cyberspace as the nervous system or control system of society. The NSSC outlines an initial framework for both organizing and prioritizing national efforts in combating cyber-attacks committed by terrorists, criminals, or nation-states, while highlighting the role of public-private engagement.

Consistent with the National Strategy for Homeland Security, the strategic objectives of the NSSC are:

- To prevent cyber-attacks against the national CI;
- To reduce the national vulnerability to cyber-attacks;
- To minimize damage and recovery time from cyber-attacks.

The strategy recognizes that, as owners and operators of much of the internet infrastructure, the private sector is best equipped and structured to respond to cyber-threats. Therefore, public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets

The "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" states that the CI sectors of the US provide the foundation for national security, governance, economic vitality, and "the American way of life". An attack on the nation's critical infrastructures and key assets could not only result in large-scale human casualties and property destruction, but also damage the national prestige, morale, and confidence, as experienced in the 11 September 2001 attacks. As a result, the following strategic objectives are considered:

- To identify and assure the protection of those infrastructures and assets that are deemed most critical in terms of national-level consequences for public health and safety, governance, economic and national security, and public confidence;

- To provide timely warning;
- To assure the protection of other infrastructures and assets that may become terrorist targets over time.

By pursuing these objectives, coordinated action is required on the part of federal, state, and local governments, as well as the private sector and concerned citizens. The Department of Homeland Security (DHS) provides overall cross-sector coordination in this new organizational scheme, acting as the primary liaison and facilitator for cooperation among federal agencies, state and local government, and the private sector. Cross-sector initiatives should be fostered in the areas of planning and resource allocation, in information-sharing, in personnel security (including background checks where appropriate) and awareness, in research and development, and in modeling, simulation, and analysis.[759]

National Infrastructure Protection Plan (NIPP)

The DHS is developing (under the authority of HSPD-7) a new National Infrastructure Protection Plan (NIPP) to outline roles and responsibilities for specific government agencies, the private sector, and state and local governments. The plan was released for public comment in November, and will likely be finished by March 2006. When completed, the NIPP will represent the "ready state" of preparedness for owners and operators of the critical infrastructures. By setting national preparedness goals for preventing, detecting, deterring, and defeating terrorist attacks on the critical infrastructures, the NIPP will supplement the National Response Plan, which deals with responses to and recovery from failures of critical infrastructures and national disasters.[760]

759 The White House. Physical Protection, op. cit.

760 Department of Homeland Security. Draft National Infrastructure Protection Plan (NIPP) Base Plan (2 November 2005). http://www.fas.org/irp/agency/dhs/nipp110205.pdf.

Organizational Overview

Public Agencies

Early Days

In the early days, two agencies had primary responsibility for coordinating US CIP policy: The Critical Infrastructure Assurance Office (CIAO), which used to be part of the Department of Commerce, and the National Infrastructure Protection Center (NIPC), formerly a division within the Federal Bureau of Investigation (FBI). However, in accordance with the various presidential directives discussed above and the creation of the DHS, the functions of the CIAO and the NIPC have been absorbed by the DHS.

Critical Infrastructure Assurance Office (CIAO)
The Critical Infrastructure Assurance Office (CIAO) was created in May 1998 and is now part of the Directorate for Information Analysis and Infrastructure Protection (IAIP). The Planning and Partnerships Office (PPO) within the IAIP assumed many of the responsibilities previously held by the CIAO, such as raising issues that cut across industry sectors and ensuring a cohesive approach to achieving continuity in delivering critical infrastructure services. Its main tasks are:

- To coordinate and implement the national strategy;
- To assess the government's own risk exposure and dependencies on CI;
- To raise awareness and public understanding of and participation in CIP efforts;
- To coordinate legislative and public affairs to integrate infrastructure assurance objectives into the public and private sectors.

National Infrastructure Protection Center (NIPC)
In 1998, the Office of Computer Investigations and Infrastructure Protection (OCIIP) was expanded to become the inter-agency National Infrastructure

Protection Center (NIPC). The NIPC was located at the FBI headquarters and is now part of the DHS IAIP.

Department of Homeland Security (DHS)

The attacks of 11 September 2001 provided the impetus to restructure the overall organizational framework of CIIP in the US. The most important change was the establishment of the Department of Homeland Security (DHS)[731] encompassing the following critical infrastructure protection roles:

- Developing a comprehensive national plan for securing the key resources and critical infrastructures of the US;
- Providing crisis management in response to attacks on critical information systems;
- Providing technical assistance and emergency recovery plans to the private sector and other government entities;
- Coordinating with other agencies of the government to provide specific warning information and protective measures, and to fund research and development;
- To circulate information regarding cyber-security to the private sector;
- To fund research and development.

The DHS brought together 22 existing federal agencies in the largest federal reorganization since 1947. The department is divided into five major divisions or "Directorates": (1) Border and Transportation Security; (2) Emergency Preparedness and Response; (3) Science and Technology; (4) Information Analysis and Infrastructure Protection; and (5) Management. In addition to these five directorates, several other critical agencies have been amalgamated with the new department or are being newly created, such as the US Coast Guard, the US Secret Service, the Bureau of Citizenship, and the Immigration Services. In addition, the DHS maintains a special liaison office for the private sector, again highlighting the essential focus on public-private collaboration.

761 http://www.dhs.gov.

In the spring of 2005, DHS Secretary Michael Chertoff outlined a plan to reorganize the department to include a new assistant secretary for cyber-security and telecommunications, as well as a new Preparedness Directorate. Some of the secretary's proposals require congressional approval, but it is expected that a majority of his proposals, including the creation of the assistant secretary for cyberspace and telecommunications, will take effect when President Bush signs the Homeland Security Authorization Bill. It is therefore expected that various roles and responsibilities will change as the DHS secretary's proposals are implemented, but the following discussion reflects the organization of the department through the summer of 2005.

The next section provides an overview of key public actors in CIIP today. Due to the consolidation brought about by the formation of the DHS, many of these entities are now part of that department. It is important, however, to note that there are other governmental entities and agencies besides the DHS that focus on homeland security.

DHS/Directorate for Information Analysis and Infrastructure Protection (IAIP)

As one of the five major divisions of the US Department of Homeland Security, the Directorate for Information Analysis and Infrastructure Protection (IAIP)[762] is responsible for identifying and assessing current and future threats and vulnerabilities to the homeland, issuing timely warnings, and taking preventive and protective action. The directorate focuses special attention on the protection of critical infrastructure and cyber-security.

The IAIP leads and coordinates the national effort to secure the nation's infrastructure and fosters an active partnership with the private sector. In creating the IAIP, the government's goal was to establish a central contact point for state, local, and private entities to coordinate protection activities with the federal government.

The IAIP has unified and focused the key cyber-security activities of the Critical Infrastructure Assurance Office (CIAO), formerly part of the Department of Commerce; the National Infrastructure Protection Center (NIPC), formerly a subdivision of the FBI; and the Federal Computer Incident Response Center (FedCIRC), formerly of the General Service Administration. Because CI relies heavily on information and telecommunication services

762 http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.

and interconnections, the IAIP also assumed the functions and assets of the National Communications Systems of the Department of Defense, which coordinates emergency preparedness for the telecommunications sector and some responsibilities of the Energy Security and Assurance Program of the Department of Energy.[763]

The IAIP directorate currently consists of four divisions. These include the Infrastructure Coordination Division (ICD), the National Cyber Security Division (NCSD), the Protective Services Division (PSD), and the National Communications System (NCS).[764]

Homeland Security Council

The Homeland Security Council is an executive entity charged with advising the president on homeland security matters. In order to more effectively coordinate the government's homeland security policies and functions, the council assesses the objectives, commitments, and risks and oversees and reviews the homeland security policies of the government. The council makes recommendations to the president based on these activities.

The council comprises a Principals Committee as well as coordination committees. The secretary of homeland security, the secretary of the treasury, the secretary of defense, the attorney-general, the secretary of health and human services, the secretary of transportation, the budget director for central intelligence, the FBI director, the Federal Emergency Management Agency (FEMA) director, the chief of staff to the president, and the chief of staff to the vice-president compose the Principals Committee.

One of the coordination committees within the council focuses on CI. It deals primarily with the protection of both physical and virtual infrastructure.[768]

US Department of State

With respect to the formulation of an international CIP program in the US, the Department of State has overall statutory authority to conduct foreign affairs, and therefore takes the lead in the interagency process of coordinating

763 Ibid.
764 Information provided by US expert involved.
768 http://www.whitehouse.gov.

international CIP matters. The Department of State works together with other departments and agencies (including the Departments of Homeland Security, Justice, Defense, Commerce, Energy, Treasury, and Transportation, as well as the intelligence community, and others) to coordinate their objectives in an overarching strategy. Further activities of the Department of State include chairing the International CIP Interagency Working Group, which has key coordination tasks, and monitoring the implementation of agreements.[769]

Congressional Focus

Both Houses of Congress have created bodies to focus on CIIP issues. As part of the House of Representatives' Committee on Homeland Security, the House Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity examines the following:

- Development of strategies to protect against terrorist attack;
- Prioritizing risks through analytical tools and cost-benefit analyses;
- Prioritizing investment in critical infrastructure protection across all sectors;
- Defeating terrorist efforts to inflict economic damage through threats and violence;
- Mitigation of potential consequences of terrorist attacks on critical infrastructure;
- Border, port, and transportation security;
- In the wake of an attack on one sector, ensuring the continuity of other sectors including critical government, business, health, financial, commercial, and social service functions;
- Security of computer, telecommunications, information technology, industrial control systems, electronic infrastructure, and data systems;
- Protecting government and private networks and computer systems from domestic and foreign attack;
- Preventing potential injury to civilians or to physical infrastructure resulting, directly or indirectly, from cyber-attacks;

769 http://www.state.gov/t/pm/ppa/icipt; and Russell, Erica B. "International and Interagency Critical Infrastructure Protection Coordination". Presentation at the PfP seminar on "Critical Infrastructure Protection and Civil Emergency Planning – New Concepts for the 21st Century" (Stockholm, 17–18 November 2003). http://www.krisberedskapsmyndigheten.se.

- With respect to each of the foregoing, assessing the impact of potential protective measures on the free flow of commerce and the promotion of economic growth.[770]

Within the Senate Committee on the Judiciary, the Subcommittee on Terrorism, Technology, and Homeland Security has oversight of laws related to government information policy, electronic privacy, security of computer information, and the Freedom of Information Act. The House Government Reform Committee has similar, but not identical, jurisdiction.

The Senate Homeland Security and Government Affairs Committee has overall jurisdiction, for the Senate, on most homeland security issues, including critical infrastructure protection. Its Subcommittee on Federal Financial Management, Government Information, and International Security has jurisdiction on matters related to cyber-security.

Government Accountability Office (GAO)

The Government Accountability Office (GAO; previously: General Accounting Office)[771] is the investigative arm of Congress. It is an independent and nonpartisan body that studies how the federal government spends taxpayers' dollars. Congress often asks the GAO to study the programs and expenditures of the federal government. The GAO advises Congress and the heads of executive agencies such as the Environmental Protection Agency (EPA), the Department of Defense (DoD), and the Department of Health and Human Services (HHS) about ways to make government more effective and responsive.[772]

The GAO has released several reports and testimonies addressing critical infrastructure protection and information security. For example:

- In July 2004, the GAO reported on "Critical Infrastructure Protection and Improving Information Sharing with Infrastructure Sectors". In this report, the GAO recommends that the DHS proceed with the development of an information-sharing plan that defines roles and

770 http://hsc.house.gov/content.cfm?id=17.
771 http://www.gao.gov/about/what.html.
772 The GAO has no direct authority over any federal or state agency. Instead, it researches issues and develops policy recommendations for the consideration of policy-makers.

responsibilities and establishes appropriate policies for interacting with ISACs and the various stakeholders involved.[773]

- In May 2005, the GAO reported on "Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems", addressing the problems of spam, phishing, and spyware and the resulting security risks to federal information systems.[774]
- In May 2005, the GAO reported on "Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilites." The following issues were identified as key challenges facing the DHS: achieving organizational stability; gaining organizational authority; overcoming hiring and contracting issues; increasing awareness about cyber-security roles and capabilities; establishing effective partnerships with stakeholders and sharing information with these stakeholders.[775]
- In May 2005, the GAO report "Information Security: Federal Agencies Need to Improve Controls over Wireless Networks" advised federal agencies to implement various controls, including policies, practices, and tools, to secure their wireless networks.[776]

Defense Community

In response to the May 1998 "Presidential Decision Directive/NSC-63 (PDD-63)", the Department of Defense (DoD) assigned the additional duty of Critical Infrastructure Assurance Officer (CIAO) to the position of the DoD Chief Information Officer (CIO). In addition, each branch of the armed services established CIAOs, typically as an additional duty for the respective department's CIO. The armed services' CIAOs are responsible for developing a plan for

773 United States Government Accountability Office (GAO). Critical Infrastructure Protection and Improving Information Sharing with Infrastructure Sectors (GAO-04–780, July 2004). http://www.gao.gov/new.items/d04780.pdf.

744 United States Government Accountability Office (GAO). Report to the Congressional Requesters, Information Security. Emerging Cybersecurity Issues Threaten Federal Information Systems (GAO-05-231, May 2005). http://www.gao.gov/new.items/d05231.pdf.

745 United States Government Accountability Office (GAO). Critical Infrastructure Protection. Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilites (GAO-05-434, May 2005). http://www.gao.gov/new.items/d05434.pdf.

746 United States Government Accountability Office (GAO). Information Security: Federal Agencies Need to Improve Controls over Wireless Networks (GAO-05-383, May 2005). http://www.gao.gov/new.items/d05383.pdf.

protecting their department's critical virtual and physical infrastructure and for coordinating remedial efforts, and report to the DoD CIO/CIAO. Further, regional and functional commanders-in-chief have begun identifying and securing their critical, operationally relevant assets and related infrastructure components.

Initially, the DoD and the individual services' internal vulnerability assessment teams, as well as the external Joint Program Office for Special Technology Countermeasures conducted scheduled vulnerability assessments for their military installations on a regional basis to identify single points of service that could be vulnerable through natural causes, human error, or deliberate attack.

The DoD coordinates its internal and international cyber-security and information assurance programs in its Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD/NII).[777]

With the establishment of the Department of Homeland Security (DHS), the DoD has established the position of an assistant secretary for homeland defense. The DoD's Defense Planning Guidance for the fiscal year 2004 defines the military's role in homeland defense as the military protection of US territory, the domestic population, and critical defense infrastructure against external threats and aggression.

Further, this guidance also calls for the DoD to routinely study the activities of foreign states to deter potential aggressors and to prepare US military forces for action, if needed. The functions of the previous DoD and armed services CIAOs have been integrated into the DHS under the IAIP directorate with the Planning and Partnerships Office (PPO) within DHS-IAIP, assuming many of the responsibilities previously held by the military CIAOs.

In addition to the lead in CIIP taken by the various DHS offices, the White House, Congress, and the defense community, each critical sector has a lead agency that can regulate or suggest practices for CIIP. For example, the lead agency for the energy sector is the Department of Energy. The Department of Energy regulates the nation's nuclear power plants, and has mandated certain computer security rules for the plants. Further, the Department of the Treasury has responsibility for the financial services sector.

777 http://www.defenselink.mil/nii/index.html.

On 19 December 2005 an "Information Assurance Workforce Improvement Program" was released by the DoD CIO. The manual sets the requirements for training and certification of information assurance professionals within the department.[778]

Computer Crime and Intellectual Property Section (CCIPS)

The Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the Department of Justice is responsible for implementing the department's national strategies in combating computer and intellectual property crimes worldwide. The Computer Crime Initiative is a comprehensive program designed to combat electronic penetrations, data theft, and cyber-attacks on critical information systems. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.[779]

Public-Private Partnerships

One cornerstone of US CIP policy is active cooperation between the public and private sectors. One of the DHS's main tasks is to facilitate partnership efforts between the government and the private sector. It also develops relationships with and among state, local, and private entities.

To date, a number of unresolved issues have prevented comprehensive sharing between the public and private sectors. For example, unresolved legal issues — involving the Freedom of Information Act (see below) as well as liability issues — have hampered effective information-sharing. According to experts, resolving these issues should enhance information-sharing and spur the growth of ISACs.[780]

778 Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. Information Assurance Workforce Improvement Program (DoD 8570.01-M, 19 December 2005). http://www.dtic.mil/whs/directives/corres/pdf/d85701_081104/d85701p.pdf.

779 http://www.usdoj.gov/criminal/cybercrime/index.html.

780 Interview with a representative of the US Chamber of Commerce, June 2002.

Office of the Private Sector, Department of Homeland Security

The DHS has demonstrated its commitment to working with the private sector and strengthening public-private partnerships by establishing the Office of the Private Sector.[781] This office provides businesses with a direct line into the department. It acts both as an advocate for the private sector by informing the secretary of their concerns, and as a clearinghouse by directing businesses to the appropriate agency or directorate. The office is coordinated by the special advisor to the secretary at the DHS's Office of the Private Sector.

Although the Office of the Private Sector is a relatively new post, it is growing steadily in significance and responsibility. The department plans to develop regional divisions next year, and the Office of the Private Sector will play an important part in community outreach. With over 25 million businesses to coordinate, the office faces a tremendous task.

Information Sharing and Analysis Centers (ISACs)

Today, most critical infrastructure industry sectors have established their own Information Sharing and Analysis Center (ISAC). Private-sector ISACs are membership organizations managed by the private sector. Each ISAC has a board of directors that determines its institutional and working procedures. The function of an ISAC is to collect, analyze, and share security, incident, and response information among ISAC members and with other ISACs, and to facilitate information exchange between the government and the private sector. The following list gives an overview of important existing ISACs:

- A number of the nation's largest banks, security firms, insurance companies, and investment companies have joined in a limited liability corporation to form a Financial Services Information Sharing and Analysis Center (FS/ISAC).[782]
- The telecommunications industry has established an ISAC through the National Coordinating Center (NCC). Each member firm of the NCC monitors and analyzes its own networks. Incidents are discussed within

781 http://www.dhs.gov/dhspublic/display?theme=37.
782 http://www.fsisac.com.

the NCC, and members decide whether the suspect behavior is serious enough to report to the appropriate federal authorities.[783]

- The electric power sector has created a decentralized ISAC through its North American Electricity Reliability Council (NERC). Much like the NCC, the NERC already monitors and coordinates responses to disruptions in the nation's supply of electricity.[784] The government and industry work together in the NERC to ensure the resiliency of the electricity infrastructure in case of potential physical and cyberspace attacks.[785]
- The IT-ISAC started operations in March 2001. Members include 20 major hardware, software, and e-commerce firms, including Cisco Systems, Microsoft, Intel, Computer Associates, Symantec, Computer Sciences Corporation, and Oracle. The ISAC is overseen by a board made up of members, and its operations center is managed by Internet Security Systems.[786]
- Other ISACs include the Surface Transportation ISAC,[787] the Oil and Gas ISAC,[788] the Water Supply ISAC, the Chemicals Industry ISAC, the Emergency Fire Services ISAC, the Emergency Law Enforcement ISAC, the Food ISAC, the Health ISAC, and the Multi-State ISAC.
- In addition to the individual sector ISACs, several ISAC leaders have convened as an ISAC Council. This council strives to strengthen the relationship between the ISAC community and government, and to solve problems common to all ISACs.

InfraGard

InfraGard is a partnership between industry and the US government as represented by the FBI. The InfraGard initiative was developed to encourage the exchange of information by members of the government and the private sector. With help from the FBI, private-sector members and FBI field representatives form local chapter areas. These chapters set up their own boards to share

783 http://www.ncs.gov/ncc.
784 http://www.nerc.com; Energy Information Sharing and Analysis Center, http://www.energyisac.com.
785 http://www.nerc.com/cip.html.
786 https://www.it-isac.org.
787 http://www.surfacetransportationisac.org.
788 http://www.energyisac.com.

information among their membership. This information is then disseminated through the InfraGard network and analyzed by the FBI.[789]

National Cyber Security Alliance (NCSA)

The National Cyber Security Alliance (NCSA) is a cooperative effort between industry and government organizations to foster awareness of cyber-security through educational outreach and public awareness. Its goal is to raise citizens' awareness of the critical role that computer security plays in protecting the nation's internet infrastructure, and to encourage computer users to protect their home and small-business systems.[790] It offers computer security advice and tools for private users as well as small businesses on its website. The NCSA is sponsored by a variety of organizations.

Partnership for Critical Infrastructure Security (PCIS)

The Partnership for Critical Infrastructure Security (PCIS) grew out of initiatives outlined in Presidential Decision Directive 63 (PDD 63). It is a private-sector coalition composed of sector coordinators of the nation's critical infrastructures. The PCIS works to develop joint policies to secure CI and examines cross-sector issues.

On 18 September 2002, many private-sector entities released plans and strategies for securing their respective infrastructures. The PCIS has played a unique role in facilitating private-sector contributions to this strategy.

In October 2005, the National Infrastructure Advisory Council (NIAC) recommended that the PCIS serve as the cross-sector coordinating mechanism, as part of the DHS partnership model.

Cyber Incident Detection & Data Analysis Center (CIDDAC)

The Cyber Incident Detection & Data Analysis Center (CIDDAC)[791] is the first private, non-profit group to set up a cyber-crime detection network outside of the US government's own efforts. The purpose of CIDDAC is to manage

789 http://www.infragard.net.
790 http://www.staysafeonline.info.
791 http://www.ciddac.org.

an automated reporting infrastructure for cyber-attacks that supports the protection of the national infrastructure. CIDDAC combines private, public, and government perspectives to facilitate automated real-time sharing of cyber-attack data. Thirty undisclosed organizations are working with CIDDAC on its pilot scheme. Each will be provided with CIDDAC's Remote Cyber Attack Detection Sensor, which will feed intrusion data into the CIDDAC center, where it can be evaluated and passed on the law enforcement agencies.

National Cyber Security Partnership (NCSP)

The National Cyber Security Partnership (NCSP) is a voluntary coalition of industry trade associations committed to working on cross-sector cyber-security issues in a collaborative manner. NCSP members include representatives of software makers, hardware manufacturers, and the end-user community, including colleges and universities. NCSP founding members include the US Chamber of Commerce, TechNet, the Business Software Alliance, and the Information Technology Association of America (ITAA).

Following the release of the 2003 White House National Strategy to Secure Cyberspace, the NCSP sponsored the National Cyber Security Summit to develop shared strategies and programs to better secure and enhance the US critical information infrastructure. The partnership established five task forces of cyber-security experts from industry, academia, and the government.[792]

Institute for Information Infrastructure Protection (I3P)

The Institute for Information Infrastructure Protection (I3P), managed by Dartmouth College, is a consortium of leading national cyber-security institutions, including academic research centers, government laboratories, and non-profit organizations. Founded in September 2001, the institute's main role is to coordinate a national cyber-security research and development program and to help build bridges between academia, industry, and the government. The I3P identifies and addresses critical research problems in CIIP and opens information channels between researchers, policy-makers, and infrastructure operators.[793]

792 http://www.cyberpartnership.org/init.html.
793 http://www.thei3p.org.

Early Warning and Public Outreach

Information-sharing is one of the driving factors behind effective early-warning networks. Many entities focused on informatio3n-sharing are also engaged in early-warning activities.

Federal Bureau of Investigation (FBI)

The 1997 PCCIP Report stated that efforts were required to establish a system of surveillance, assessment, early warning, and response mechanisms.[794] According to some reports, the Clinton administration envisaged an enormous database of every hacking or computer-hijacking incident. They hoped to create by 2003 a constantly updated tool to forecast, identify, and combat cyber-attacks that would be developed and maintained in close cooperation between the private and the public sector. The FBI was chosen to serve as the preliminary national warning center for infrastructure attacks and to provide information on law enforcement and intelligence. Under PDD 63, the National Infrastructure Protection Center (NIPC) as part of the FBI was given responsibility for developing analytical capabilities to provide information on changes in threat conditions and newly identified system vulnerabilities, as well as timely warnings of potential and actual attacks.[795] The NIPC, as discussed above, was incorporated into the DHS. The comprehensive early-warning system is now likely to be channeled through the US CERT. The FBI still retains its responsibilities for addressing cyber-crime.

Directorate for Information Analysis and Infrastructure Protection (IAIP)

The Department of Homeland Security's Directorate IAIP[796] was set up with a special focus on systematically analyzing all information and intelligence on potential terrorist threats within the US. This division compiles and analyzes information from multiple sources, including the CIA, the FBI, the Defense Intelligence Agency (DIA), and the National Security Agency (NSA), and is-

794 President's Commission on Critical Infrastructure Protection, Critical Foundations, op. cit.
795 Clinton, Presidential Decision Directive 63, op. cit.
796 http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.

sues early warnings of terrorist attacks.[797] In case of an attack, the IAIP would aim to:

- Provide warning of threats against the US, including physical and virtual attacks;
- Issue threat advisories through the Homeland Security Advisory System;
- Provide information about terrorist threats to the public, private industry, state, and local government.[798]

National Cyber Security Division (NCSD)

In June 2003, the National Cyber Security Division (NCSD) was created under the IAIP to combat internet-based attacks against government and critical private-sector backbone networks. The NCSD's main missions are to implement the National Strategy to Secure Cyberspace and to implement protective measures to secure cyberspace and to reduce the cyber-vulnerabilities of critical infrastructures.

The NCSD builds upon the existing capabilities transferred to the DHS from the former Critical Infrastructure Assurance Office (CIAO), the National Infrastructure Protection Center (NIPC), the Federal Computer Incident Response Center (FedCIRC), and the National Communications System (NCS).

In January 2004, the "National Cyber Alert System", an operational system delivering timely information to better secure US computer systems, was announced. As part of this program, DHS is making available a series of information products targeted at home users and technical experts in businesses and government agencies. These e-mail bulletins will provide timely information on computer security vulnerabilities, the potential impact of threats and actions required to mitigate them, and best practices for PC security.

Managed by the United States Computer Emergency Readiness Team (US-CERT) — a partnership between NCSD and the private sector – the National Cyber Alert System provides the first service for relaying graded computer security update and warning information to all users.

797 http://www.whitehouse.gov/deptofhomeland/sect6.html.
798 http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0094.xml.
799 http://www.cert.org.

Federal Computer Incident Response Center (FedCIRC)
The responsibility for detecting and responding to cyber-attacks on federal agencies while they are in progress lies with the Federal Computer Incident Response Center (FedCIRC), which gives agencies the tools to detect and respond to such attacks, and coordinates response and detection information. The FedCIRC was incorporated into the IAIP as part of the DHS in March 2003 and is now part of the National Cyber Security Division (NCSD).

The Bush administration is expected to issue a guideline for federal agencies to report computer security incidents to the FedCIRC. The guideline is expected to outline the type of information required in an incident report that will give FedCIRC the data it needs to track and analyze incident reports.

CERT Coordination Center (CERT/CC), Carnegie Mellon University

The CERT/CC is located at the Software Engineering Institute (SEI), a federally funded research and development center operated by Carnegie Mellon University. It was established in 1988 after the Morris worm crashed 10 per cent of the world's internet systems. CERT/CC acts as a coordination hub for experts during security incidents, and works to prevent future incidents.[799]

The CERT/CC acts through several mechanisms. First, its experts research and assess network vulnerabilities and develop risk assessments. Second, they disseminate information to the public through regular security alerts and presentations to the public. Finally, members of the CERT/CC participate in various security groups to improve internet security and network survivability. The CERT/CC is also a primary contributor to the US-CERT.

US-CERT

On 15 September 2003, the Department of Homeland Security, in conjunction with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University, announced the creation of the US-CERT. The US-CERT works with the National Cyber Security Division (NCSD) of the IAIP to prevent and mitigate cyber-attacks and to reduce vulnerabilities to cybernetic attacks. Together, they have set up the National Cyber Alert System, a trusted warning system offered by the government to help home users and technology experts.

It will send e-mails about major virus outbreaks and other internet attacks as they occur, along with detailed instructions to help computer users protect themselves.

The US-CERT initiative is designed to utilize the CERT/CC's capabilities to help accelerate the nation's response to cyber-attacks and vulnerabilities. The initiative also enables the DHS to provide expanded analysis, warning, and response coordination.[800]

Internet Security Alliance

The Internet Security Alliance[801] was created in April 2001 to provide a forum for information-sharing on information security issues. It represents the interests of the industry vis-à-vis legislators and regulators and aims to identify and standardize best practices in internet security and network survivability while creating a collaborative environment to develop and implement information security solutions. The Internet Security Alliance is a non-profit collaboration between the Electronic Industries Alliance (EIA), a federation of trade associations, and Carnegie Mellon's CyLab. CyLab works closely with the CERT Coordination Center (CERT/CC). Internet Security Alliance members have a single portal for up-to-the-minute threat reports, best security practices, risk management strategies, and more, which gives them the edge in the competitive and volatile environment of the internet.[802]

Information-Sharing and Analysis Centers (ISACs)

The Information Sharing and Analysis Centers (ISACs) were planned to help create an early-warning database. The idea is that private-sector owners and operators will survey incidents and pass the information on to a central point of contact for information-sharing, and then distribute it to the ISAC membership (see the chapter on "Public-Private Partnerships" above).

800 http://www.uscert.gov.
801 http://www.isalliance.org.
802 Ibid.

OnGuardOnline.gov

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help users be on guard against internet fraud, to secure their computers, and to protect their personal information. The comprehensive website has tips, articles, videos, and interactive activities. The Federal Trade Commission (FTC) maintains OnGuardOnline.gov with contributions from various government departments, including the DHS.[803]

Law and Legislation

Federal Advisory Committee Act (FACA) 1972

One obstacle to fully implementing a robust and public private partnership is the 1972 Federal Advisory Committee Act (FACA). The FACA (Public Law 92-463, 5 U.S.C., App) was enacted by Congress in 1972. Basically, this act is designed to prevent any person or company (or groups of them) from having undue influence in government decision-making. Its purpose was to ensure that advice rendered to the executive branch by the various advisory committees, task forces, boards, and commissions formed over the years by Congress and the president be both objective and accessible to the public. The act not only formalized a process for establishing, operating, overseeing, and terminating these advisory bodies, but also created the Committee Management Secretariat (MCC), whose task it is to monitor and report executive branch compliance with the act.[804]

In the field of CIP/CIIP, the delicate issue is that CIP is based on partnership with the DHS, which requires meetings. If these meetings are open to the public and subject to other government restrictions, the industry will be unwilling to be frank or overly commit itself, since businesses would be putting sensitive information in the public domain.

803 http://onguardonline.gov/index.html.

804 http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8203&channelPage=/ep/channel/gsaOverview.jsp&channelId=-13170.

In the US, the challenge has been to ensure that the private sector and its representatives have the opportunity to provide comments and input on CIP policy without violating FACA considerations. One solution to this is found in Section 871 of the Homeland Security Act, which gives the secretary of homeland security the authority to create FACA-exempt advisory panels. The National Infrastructure Advisory Council (NIAC) has issued a recommendation in which it urged the secretary to use this authority, specifically in the case of the sector coordinating councils that most critical infrastructure sectors have established.[805]

Computer Fraud and Abuse Act (CFAA) 1986

In the US, legislative awareness of computer crimes grew dramatically in the early 1980s as computers became increasingly important for the conduct of business and politics. The Computer Fraud and Abuse Act (CFAA) of 1986 was the conclusion of several years of research and discussion among legislators.[806] It established two new felony offenses of unauthorized access to "federal interest" computers[807] and unauthorized trafficking in computer passwords. Violations of the CFAA include intrusions into government, financial, medical, and "federal interest" computers.

The Computer Abuse Amendments Act of 1994 expanded the 1986 CFAA to address the transmission of viruses and other harmful code. The measures provided by this act were further tightened on 26 October 2001 by the USA PATRIOT anti-terrorism legislation.[808] Violations of the CFAA are investigated by the National Computer Crimes Squad at the FBI and supported by its Computer Analysis and Response Team (CART), a specialized unit for computer forensics.[809]

805 Information provided by US expert involved.

806 http://www4.law.cornell.edu/uscode/18/1001.html.

807 "Federal interest computers" are defined as two or more computers involved in a criminal offense, if they are located in different states.

808 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. For the full-text version, see: http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf. Privacy and civil liberty advocacy groups have expressed concern over the USA PATRIOT Act and a number of other legislative developments.

809 http://www.fbi.gov/hq/lab/org/cart.htm. Of further importance is also the recent enactment of the Gramm-Leach-Bliley (GLB) Act and the regulations for implementing it, which address privacy concerns by setting forth a range of requirements to protect customer information. For the text of the GLB Act, see: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

Homeland Security Act 2002

Much of the federal legislation concerning CIP/CIIP was written before the emergence of "cyber-threats". Thus, it is questionable whether a timely and efficient response would be possible under the existing legal frameworks at both federal and state/local levels.[810]

While the overall act established the Department of Homeland Security (DHS), Title II of the Homeland Security Act (of 2002) specifically addresses information analysis and infrastructure protection. It created the IAIP Directorate, transferred the various agencies (like CIAO, NIPC, and others mentioned above) into the DHS, and established the categories of information to which the secretary of homeland defense has access. In order to adequately protect the nation, the secretary has access to certain intelligence analysis, infrastructure vulnerabilities, and any "raw" data that the president discloses to the secretary.

Critical Infrastructure Information Act: Procedures for Handling Critical Infrastructure Information

The Homeland Security Act of 2002 contained a provision called the "Critical Infrastructure Information Act", which was designed to encourage the private sector to voluntarily share information with the DHS. In April of 2003, the DHS released regulations for the implementation of this program, which the DHS has named the "Protected Critical Infrastructure Information Program (PCII)". These regulations, which were authorized in the Homeland Security Act of 2002, provide rules for the receipt, care, and storage of critical infrastructure information, the maintenance of security and confidentiality, and methods for dealing with proprietary or business-sensitive information. The basic concept of the regulations again underscores the fundamental principles of public-private partnership. Their goal is to encourage the private sector to share sensitive security information with the DHS without fear that the information

810 President's Commission on Critical Infrastructure Protection, Critical Foundations, op. cit., p. 81.
811 Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 18,524 (2003) (to be codified at 6 C.F.R. §29).
812 Terrorism Risk Insurance Act of 2002, Pub. L. No. 107–297, 116 Stat. 2322 (2002).

will be made public. It stipulates that business-sensitive information that businesses voluntarily submit to the DHS may be labeled CII and exempted from disclosure under the Freedom of Information Act (FOIA). Under this program, CII that the DHS shares with state and local governments would be protected from state freedom of information act laws. The final rules implementing this program have not yet been issued. This change in the law has potentially broad effects and requires a change of culture, as disclosure of information held by the government has traditionally been favored in the US.

Freedom of Information Act (FOIA)

CIIP is an important issue in the US, primarily because many of the critical sectors are regulated by the government, but controlled by private entities. As part of the regulation, the private entities must regularly file reports and disclose sensitive information to the government. This could place such information in jeopardy, since under the Freedom of Information Act (FOIA), the public can request such information from the government. However, a FOIA exemption was included in the Homeland Security Act of 2002. Any information regarding critical infrastructures (including security systems, warnings, or interdependency studies) is exempt from disclosure.

After the attacks of 11 September 2001, the Federal Energy Regulatory Commission (FERC) removed certain information from its website and its public reading room. This included detailed maps and other information about electric power facilities and natural gas pipelines. Although exempt from FOIA procedures, this information had traditionally been open and available to anyone who requested it. In February 2003, the FERC ruled that individuals wanting access to this information would have to apply for it. The application requirements include identification information, and take the need/purpose of the information into account. Access is granted on a case-by-case basis, and only to individual applicants.

Terrorism Risk Insurance Act 2002

The "Terrorism Risk Insurance Act of 2002" is a new law that creates a federal program for public and private compensation for insured losses resulting from acts of terrorism. All commercial insurance providers must offer terrorism risk insurance, and the federal government agrees to underwrite some of the losses in the event that a terrorist event takes place. Under this law, an act of terrorism includes any act of violence against elements of the infrastructure.[812] This could include catastrophic network assaults as well as physical attacks.

Part II

International Organizations and Forums

European Union (EU)

The European Union is a key player at the international level concerning information assurance. CIIP, the information society, and information security are considered essential issues. Therefore, the EU has launched initiatives and research programs to examine various aspects of the information revolution and its impact on education, business, health, and communications.

The terrorist attacks in Madrid in 2004 and London in 2005 have highlighted the risk of terrorist attacks against European infrastructures in a broader sense. The damage or loss of a piece of infrastructure in one state may have negative effects on several others, and on the European economy as a whole. The following chapter gives a short overview of important steps taken by the EU in the field of CIP and CIIP.[813]

Critical Sectors

The Communication of the Commission of the European Communities (EU Commission) on "Critical Infrastructure Protection in the Fight Against Terrorism", adopted on 20 October 2004, provides a definition of critical infrastructures (CI), enumerates the critical sectors identified, and discusses the criteria for determining potential CI.[814] In the Communication, CI are defined as follows: "Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy and key government services."

In the follow-up publication of the EU Commission, the "Green Paper on a European Program for Critical Infrastructure Protection" (Green Paper on

* The European Union Survey of 2006 was reviewed by Marcelo Masera, European Commission, Joint Research Centre, and Ronald De Bruin, European Network and Information Security Agency (ENISA). The Chapter on Law and Legislation was contributed by Martin Wählisch, Humboldt University Berlin.

813 http://www.europa.eu.int/information_society/index_en.htm.

814 Commission of the European Communities. Critical Infrastructure Protection in the Fight against Terrorism (Brussels, 20 October 2004), COM(2004)702 final., pp. 3–5. http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf.

EPCIP),[815] CIIP is defined as: "The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of CII in case of failures, attacks or accidents above a defined minimum level of services and aim at minimizing the recovery and damage. CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with CIP from a holistic perspective."[816]

The "Green Paper on EPCIP" identifies the following critical sectors and their products and services:

- Energy (Oil and Gas Production, Refining, Treatment and Storage, including Pipelines; Electricity Generation; Transmission of Electricity, Gas and Oil; Distribution of Electricity, Gas and Oil),
- Information and Communication Technologies, (Information System and Network Protection; Instrumentation Automation and Control Systems (SCADA etc.); Internet; Provision of Fixed Telecommunications; Provision of Mobile Telecommunications; Radio Communication and Navigation; Satellite Communication; Broadcasting),
- Water (Provision of Drinking Water; Control Water Quality; Stemming and Control of Water Quantity),
- Food (Provision of Food and Safeguarding Food Safety and Security),
- Health (Medical and Hospital Care; Medicines, Serums, Vaccines and Pharmaceuticals; Bio-Laboratories and Bio-Agents),
- Financial (Payment Services/Payment Structures (private); Government Financial Assignment),
- Public and Legal Order and Safety (Maintaining Public and Legal Order, Safety and Security; Administration of Justice and Detention),
- Civil Administration (Government Functions; Armed Forces; Civil Administration Services; Emergency Services; Postal and Courier Services),
- Transport (Road Transport; Rail Transport; Air Traffic; Inland Waterways Transport; Ocean and Short-Sea Shipping),

815 Commission of the European Communities. Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM(2005) 576 final, p. 19.

816 Ibid. p. 19.

- Chemical and Nuclear Industry (Production and Storage/Processing of Chemical and Nuclear Substances; Pipelines of Dangerous Goods (Chemical Substances)),
- Space and Research (Space; Research).[817]

Although most infrastructures are owned and operated by the private sector, the EU Commission declared in its Communication 574/2001 of 10 October 2001: "The reinforcement of certain security measures by the public authorities in the wake of attacks directed against society as a whole and not at the industry players must be borne by the State. The public sector has therefore a fundamental role to play too."[818]

To determine the criticality of an infrastructure is a complex task. The EU Commission suggests that the following three factors be taken into consideration when identifying potential critical infrastructures:

- Scope: the loss of a critical infrastructure element is rated by the extent of the geographic area (international, national, provincial/territorial, or local) that could be affected by its loss or unavailability.
- Magnitude: the degree of the impact or loss can be categorized as "none", "minimal", "moderate", or "major". Among the criteria for assessing the potential magnitude of an incident are: public impact (number of citizens affected, loss of life, medical illness, serious injury, evacuation); economic impact (GDP effect, significance of economic loss and/or degradation of products or services); environmental impact (effect on the public and the environment); interdependency (with other critical infrastructure elements); and finally, political impact (confidence in the ability of the government to cope).
- Effects of time: this criterion ascertains at what point the loss of an element could have a serious impact (e.g., immediately, within 24 to 48 hours, within one week).

However, in most cases, psychological effects also need to be taken into consideration.[819]

817 Green Paper on CIP, op. cit., p. 24.
818 CIP in the Fight against Terrorism, op. cit., p. 4.
819 Ibid., pp. 3–5.

Initiatives and Policies

Green Paper on a European Programme for CIP (EPCIP)

The EC Communication on "CIP in the Fight Against Terrorism" mentioned above discusses the EU Commission's current efforts in the field of CIP and proposes additional measures to strengthen existing instruments, mainly by the establishment of a "European Programme for Critical Infrastructure Protection (EPCIP)". On 24 November 2005, the EU Commission published a "Green Paper on a European Programme for Critical Infrastructure Protection",[820] which outlines options to enhance prevention, preparedness, and responses in protecting the EU's critical infrastructure. The Green Paper provides options on how the EU Commission may respond to the EU Council's request to establish an EPCIP and a Critical Infrastructure Warning Information Network (CIWIN), and constitutes the second phase of the consultation process that began with the Commission Communication on CIP that was adopted in October 2004.

The Green Paper addresses such key issues as:

- EPCIP's protection aim;
- Key principles;
- The type of framework needed;
- Definitions and a comprehensive list of EU Critical Infrastructures (ECI);
- ECI versus National Critical Infrastructures (NCI);
- The role of CI owners, operators, and users;
- The role of CIWIN, and the evaluation and monitoring of critical infrastructure (interdependencies).

The options presented by the Green Paper on EPCIP are a combination of measures and should be seen as complementary measures to current national efforts. The EU Commission expects to receive concrete feedback concerning the policy options outlined in the Green Paper. Depending on the outcome of

820 Green Paper on CIP, op. cit.

the consultation process, an EPCIP policy package may be proposed during 2006.[821]

Critical Infrastructure Warning Information Network (CIWIN)

In order to facilitate the exchange of information on shared threats and vulnerabilities within the EU, the EU Commission is setting up the Critical Infrastructure Warning Information Network (CIWIN). This EU network aims at helping member states, EU institutions, and owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities, and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.[822]

The EU Commission suggests the following three possible options for the development of the CIWIN in its Green Paper:

- The CIWIN could take the shape of a forum limited to the exchange of CIP ideas and best practices in support of CI owners and operators;
- The CIWIN could be a rapid alert system (RAS) linking member states with the EC;
- CIWIN could be a multi-level communication and alert system with two distinct functions: a rapid alert system (RAS) linking member states with the EU Commission, and a forum for the exchange of CIP ideas and best practices.

Regardless of the option finally chosen, the CIWIN will complement existing networks and not duplicate them.[823]

821 Ibid. pp. 2–3.

822 CIP in the fight against terrorism, op. cit., p. 10. The US has a similar system, known as the Critical Infrastructure Warning Information Network (CWIN), that has been operational since 2003. http://www.gao.gov/new.items/d05434.pdf.

823 Green Paper on CIP, op. cit.

European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) was created on 14 March 2004. By deciding on 5 June 2003 to set up ENISA as a legal entity, the EU reinforced its efforts to enhance European coordination on information security.

ENISA aims at ensuring a high level of network and information security within the community. Thus, the agency will contribute to the development of network and information security for the benefit of the citizens, consumers, enterprises and public sector organizations of the EU. This will also contribute to the smooth functioning of the Internal Market.

The agency assists the EU Commission, the member states and, consequently, the business community in meeting the requirements of network and information security, including present and future EU legislation. ENISA will ultimately serve as a center of expertise both for member states and for EU institutions to seek advice on matters related to network and information security.

The work program for 2005 included several deliverables. The European Network and Information Security Agency (ENISA) has created a "Who is Who Directory on Network and Information Security" with contact information for authorities acting in the field of network and information security in the member states. ENISA has also published an "Inventory of CERT Activities in Europe" and issues a quarterly newsletter. In addition, ENISA organizes workshops for outreach and dissemination of good practices in the member states. Moreover, ENISA will define customized information packages, including good practices for specific target groups (e.g. SMEs and home users). Finally, ENISA has created a network of liaison officers, which helps ENISA to exchange information and cooperate on a day-to-day basis with member states.

In line with its work program for 2005, ENISA has set up the Permanent Stakeholders' Group (PSG). It brings together experts from the industry, academia, and user communities, and has become an invaluable tool for ENISA's cooperation with these communities. Moreover, three working groups have been established in the fields of CERT cooperation, awareness-raising, and technical and policy aspects of risk assessment and risk management.[827]

Research and Development

Information Society Technologies (IST) FP6 and FP7

The overall objective of the IST (Information Society Technologies) efforts within the EU's Sixth Framework Program (FP6) is to contribute directly to realizing European policies for the Information Society as agreed at the Lisbon European Council of 2000, the Stockholm European Council of 2001, and the Seville European Council of 2002, and as reflected in the eEurope Action Plan. The IST component of FP6 (running from 2002 to 2006) aims at ensuring European leadership in the generic and applied technologies at the heart of the knowledge economy. The IST research efforts within FP6 reinforce and complement the eEurope 2005 objectives. In the EU's current research program, IST has the first priority in terms of funding.[829] Among the strategic objectives of IST FP6 are: A global dependability and security framework; semantic-based knowledge systems; networked business and government; e-safety for road and air transport; e-health; cognitive systems; embedded systems; improving risk management; and e-inclusion. As in FP5, the focus of these projects is mainly on technical issues, whereas policy aspects (such as organizational aspects, ethical questions, etc.) concerning CIIP are hardly discussed and somewhat undervalued in the strategic objectives.

Although the current FP6 runs until 2006, debates have already started on the budget, structure, and research priorities of FP7. Under FP7, which begins in 2007 and runs until 2013, the EU Commission wishes to identify topical areas of interest that will be continued after the end of FP6, as well as new and emerging topics, including space and security.[830]

827 http://www.enisa.eu.int.; European Network and Information Security Agency (ENISA). Who is Who Directory on Network and Information Security (Version 1.0, December 2005). http://www.enisa.eu.int/doc/pdf/deliverables/ENISA_Who-is-Who-Directory_v1.0.pdf.; European Network and Information Security Agency (ENISA). ENISA Inventory of CERT Activities in Europe (Version 1.0, December 2005). http://www.enisa.eu.int/doc/pdf/deliverables/enisa_cert.pdf.

829 http://europa.eu.int/information_society/research/index_en.htm.

830 http://europa.eu.int/comm/research/future/themes/index_en.cfm.

European Security Research Programme (ESRP)

The goal of European security research is to make 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.[831] For projects in the field of security research, the following priority missions are identified:

- Optimizing the security and protection of networked systems;
- Protecting CI against terrorism (including bio-terrorism and incidents involving biological, chemical, and other substances);
- Enhancing crisis management (including evacuation, search and rescue operations, control, and remediation);
- Achieving interoperability and integration of systems for information and communication;
- Improving situation awareness (e.g. in crisis management, anti-terrorism activities, or border control).[832]

Furthermore, the EU Commission set up the European Security Research Advisory Board (ESRAB) on 1 July 2005. The ESRAB is attached to the EU Commission and can be consulted on any questions related to the content and implementation of the European Security Research Program. ESRAB carries out its work in full awareness of the European policy context, in particular of the research and development activities carried out at the national level and in support of European research policy initiatives.[833]

831 http://www.europa.eu.int/comm/enterprise/security/index_en.htm.

832 http://icadc.cordis.lu/fep-cgi/srchidadb?CALLER=NEWS_SECURITY&ACTION=D&RCN=23324&DOC=6&CAT=NEWS&QUERY=1.

833 Official Journal of the European Union. Commission Decision of 22 April 2005 establishing the European Research Advisory Board (2005/516/EC).

Critical Information Infrastructure Research Co-ordination (CI2RCO)

The EU has set up a task force[834] to explore the measures taken by its 25 member states to combat (cyber-) threats against critical infrastructure. As part of the EU's CI2RCO (Critical Information Infrastructure Research Coordination) project, announced in April 2005, the task force aims to identify research groups and programs focusing on IT security in critical infrastructures, such as telecommunications networks and power grids. The scope of the cooperation goes beyond the EU; the task force also wants to include the US, Canada, Australia, and Russia. The CI2RCO project is a Co-ordination Action co-funded under the IST FP6. The main objectives of the CI2RCO project are:

- Encouraging a coordinated Europe-wide approach for research and development on CIIP;
- Establishing a European Research Area (ERA) on CIIP as part of the larger IST strategic objective of integrating and strengthening the ERA in terms of dependability and security.[835]

CI2RCO will focus on activities and actions across the EU-25 and Associate Candidate Countries. Among other information, the CI2RCO website features the "European CIIP Newsletter" and upcoming events in the area of CIIP.[836]

Law and Legislation

In its legislation on CIIP, the EU went back to the basic principles already enshrined in European law, particularly with regard to the confidentiality of communications and the legal conditions for interception, traffic data retention, legality of content, or intellectual property.[837]

834 The European task force includes the Fraunhofer Institute for Secure Information Technology (FhG-SIT), the German Aerospace Center (DLR); the Industrieanlagen-Betriebsgesellschaft (IABG) company; the Italian National Agency for New Technologies, Energy and the Environment (ENEA); the Netherlands Organization for Applied Scientific Research (TNO); the École Nationale Supérieure des Télécommunications; and consulting firm Ernst Basler+Partner.

835 http://www.attrition.org/pipermail/isn/2005-April/001454.html.

836 http://www.ci2rco.org/index.asp.

837 Esterle, Alain, Hanno Ranck and Burkard Schmitt (edited by Burkard Schmitt). Information security. A new challenge for the EU. Chaillot Paper no. 76 (Paris, March 2005). http://www.iss-

Data Protection Directive 1995

The Data Protection Directive (95/46/EC)[838] provides a regulatory framework to guarantee the secure and free movement of personal information across the national borders of EU member countries, and also establishes a baseline of security controls protecting this information. The Data Protection Directive requires that any third country to which data is transferred provide "adequate" data protection.[839]

Directive on Electronic Signature 1999

In to the area of e-commerce, the Directive on Electronic Signatures (1999/93/CE)[841] has been duly incorporated into the national legislation of member states.[842] This directive outlines requirements for certificates, certification service providers, and secure signature-creation devices, and provides recommendations for secure signature verification. The directive recognizes the potential variety of technologies used to generate signatures, but does not establish detailed technical standards or propose best practices. It also lays the groundwork for the international recognition of certificates.

Directive on Privacy Protection in the Electronic Communications Sector 2002

Directive 95/46/EC has been complemented by Directive 97/66[843] on the protection of personal data in the field of telecommunications and, of even

eu.org/chaillot/chai76.pdf. Overview of all legislative documents on EU data protection: http://europa.eu.int/information_society/policy/ecomm/info_centre/documentation/legislation/index_en.htm, and http://www.europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm.

838 http://europa.eu.int/scadplus/leg/en/lvb/l14012.htm. Status of implementation of Directive 95/46: http://www.europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.htm.

839 Cf. the US Safe Harbor Arrangement as a streamlined process for US companies to comply with the directive, developed by the US Department of Commerce in consultation with the EU. http://www.export.gov/safeharbor.

840 Ibid., Article 15.

841 http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/esignatures_en.pdf.

842 Status of notification of legal acts implementing the electronic signatures directive: http://europa.eu.int/information_society/eeurope/2005/all_about/trust/esignatures/index_en.htm.

843 http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf.

greater relevance, by the EU Directive on Privacy Protection in the Electronic Communications Sector[844] (2002/58/CE).

The directive clarifies policies on spamming, electronic data collection, and retention by requiring the member countries to adopt legislation providing data confidentiality, limiting the traffic data storage, and providing exceptions for reasons of national security. Moreover, the directive specifies that traffic data is to be deleted or depersonalized as soon as it is no longer needed for sending or preparing invoices, but nonetheless allows member states the possibility "of adopting legislative measures providing for the retention of data for a limited period".[845] These measures must be "appropriate or proportionate, within a democratic society, to safeguard national security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of electronic communication

Framework Directive 2002

The objective of the Framework Directive (2002/21/EC)[846] is to establish a harmonized framework for the regulation of electronic communications networks and services. It lays the foundation in the form of horizontal provisions serving the other measures: the scope and general principles, basic definitions, general provisions on the national regulatory authorities, the new concept of significant market power, and rules for granting certain indispensable resources such as radio frequencies, or rights of way.

Council Framework Decision on Attacks Against Information Systems 2005

The European Council Framework Decision on attacks against information systems (2005/222/JHA)[847] of February 2005 aims to strengthen criminal judicial cooperation on attacks against information systems by developing effective tools and procedures. The criminal offences punishable under the framework

844 http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.
845 Ibid., Article 13.
846 http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_108/l_10820020424en00330050.pdf.
847 http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.

decision are: illegal access to information systems, illegal system interference (the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, degrading, altering, suppressing, or rendering inaccessible computer data) and illegal data interference. The member states will have to make provisions for such offences to be punished by effective, proportionate, and dissuasive criminal penalties. To enhance cooperation, the member states must establish operational points of contact that are available 24 hours a day and seven days a week.

Directive on Data Retention 2005

In December 2005, the European Parliament agreed on a Directive on the Retention of Data processed in connection with the provision of public electronic communication services (Commission proposal COM(2005)0438).[848] This legislation, which allows the individual governments to decide how long data should be retained as long as the period is between six and 24 months, is likely to take effect during 2006,[849] although it may face legal challenges in several countries. The measures, drafted by the United Kingdom after the London terrorist bombings in July 2005, require companies to keep a wide range of data, including incoming and outgoing phone numbers; the duration of phone calls; data that can be used to trace fixed or mobile telephone calls; information about text messages; IP addresses, which identify a computer's coordinates on the internet; login and logoff times; and details of e-mail traffic – but not the actual content of communications. Details of connected calls that are unanswered, which can be used to send signals to accomplices or to detonate bombs, will also be archived where that data exists. Independent authorities will be designated to monitor the use of the data, which will have to be deleted at the end of the period unless it is kept for anti-terror investigation purposes.

848 This directive amends Directive 2002/58/EC: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0438en01.pdf.

849 They still need to be formally approved by EU member states. Information about the first reading: http://www.europarl.eu.int/omk/sipade3?TYPE-DOC=TA&REF=P6-TA-2005-0512&MODE=SIP&L=EN&LSTDOC=N.

Group of Eight (G8)

Since 1995, the Group of Eight (G8) has become increasingly involved in issues relating to cyber-crime, the information society, and critical infrastructure protection. At the Halifax summit in 1995, a group of senior experts was set up with the task of reviewing and assessing existing international agreements and mechanisms to fight organized crime. This G8 Senior Experts Group took stock extensively and critically before drawing up a catalog of 40 operative recommendations. These recommendations were approved at the G8 summit in Lyon in 1996. The G8 Senior Expert Group, known since then as the Lyon Group, was one of the first international political forum to fully recognize the significance of high-tech crime. The Lyon Group has since developed into a permanent multi-disciplinary body with numerous specialized sub-working groups. Since October 2001, the Lyon Group meetings have been held together with the Roma Group dealing with combating terrorism (Lyon/Roma Group).[850]

A further important stage for the G8 and CIP/CIIP was in spring 2000. On 15–17 May 2000, government officials and industry participants from G8 countries and other interested parties attended the "G8 Paris Conference on Dialogue Between the Public Authorities and Private Sector on Security and Trust in Cyberspace".[851] The aim was to discuss common problems and to find solutions associated with high-tech crime and the exploitation of the internet for criminal purposes. The G8 member states were convinced that a dialog between governments and the private sector was essential in the fight against the illegal or prejudicial use of ICT, and they agreed on defining a clear and transparent framework for addressing cyber-crime.[852]

Okinawa Charter on Global Information Society

The Okinawa Charter on Global Information Society was published in July 2000.[853] The charter states that ICT is one of the most potent forces shaping the 21st century, enabling many communities to address social and economic

* The Group of Eight Survey of 2006 was reviewed by Harry Hoverd, Home Office, UK.

850 http://www.auswaertiges-amt.de/www/en/aussenpolitik/vn/lyon_group_html.

851 http://www.g8.utoronto.ca/crime/paris2000.htm.

852 Ibid.

853 http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm.

challenges with greater efficiency. One of the key principles and approaches of the charter is that international efforts to develop a global information society must be accompanied by coordinated action to foster a crime-free and secure cyberspace. In this respect, the Okinawa charter refers to the "OECD Guidelines for Security of Information Systems". Moreover, in the Okinawa Charter, the G8 asked both the public and private sectors to make efforts to bridge the international information and knowledge gap.

G8 Principles for Protecting Critical Information Infrastructures

G8 members met in Paris in March 2003 for the first multilateral meeting devoted to CIP/CIIP. Top-level experts from G8 member states, together with the major CIP/CIIP operators (e.g., France Telecom for France) came together to define common principles for the protection of vital CI/CII.[854] The 11 clearly defined CIIP principles were adopted on 5 May 2003 by the G8 Justice and Interior Ministers. They cover the following topics:

- Countries should have emergency warning networks regarding cyber-vulnerabilities, threats, and incidents.
- Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their CII, and the role each must play in protecting them.
- Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.
- Countries should promote partnerships among stakeholders, both public and private, to share and analyze information on their critical infrastructure in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.
- Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

854 http://www.g7.utoronto.ca/summit/2003evian/press_statement_march24_2003.html.

- Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.
- Countries should trace attacks on critical information infrastructures and, where appropriate, disclose the results to other countries.
- Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an attack on the information infrastructure, and should encourage stakeholders to engage in similar activities.
- Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the "Council of Europe Cybercrime Convention" of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate.
- Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, by sharing and analyzing information regarding vulnerabilities, threats, and incidents, and by coordinating investigations of attacks on such infrastructures in accordance with domestic laws.
- Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.[855] With the adoption of these principles, the G8 member states suggested that the emergence of a new "security culture" should encourage them to strengthen international co-operation, to implement the best professional practices in the field of computerized surveillance and alert, to conduct common exercises to test the reaction capabilities in case of incidents, to make other countries aware of the problems, and to invite them to adopt the same main courses of action.[856] The 11 principles are intended to guide national responses to CIIP. However, to this end, it is crucial that the principles be communicated to all parties concerned.

855 http://www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf.

856 "G8 Principles for Protecting Critical Information Infrastructures". In: NISCC Quarterly (April-June 2003), p. 9. http://www.niscc.gov.uk/Quarterly/NQ_APRIL03_JUNE03.pdf.

The essential elements of the principles of protecting CII were adopted by the 78th United Nations General Assembly.[857] Resolution 58/199 of January 2004, entitled "Creation of a global culture of cyber security and the protection of critical information infrastructures", is complemented by the annex "Elements for protecting CII", which is based on the 11 principles defined by the G8 in 2003.[858]

The G8 Justice and Home Affairs Ministers (the Ministerial meeting of the Lyon/Roma Group) met in Washington in May 2004 and endorsed "Best Practices for Network Security, Incident Response and Reporting to Law Enforcement". This guide assists network operators and system administrators in responding to computer incidents.[859]

High-Tech Crime Sub-Group Activities

One of the sub-groups of the Lyon Group, called the High-Tech Crime sub-group, deals with issues concerning CIIP. The sub-group's goal for CIIP work is to identify and to find a way to protect the infrastructure that G8 countries are dependent on, and to provide a more unified approach to multinational companies who deal with a number of G8 countries for setting up an international information-sharing mechanism. Furthermore, the High-Tech Crime sub-group is active in a number of areas including:

- A CIIP handbook of national contact points. This International CIIP Directory is compiled and maintained by the National Infrastructure Security Co-ordination Centre (NISCC, UK), and its scope is limited to national governmental organizations. The directory is not available publicly, commercially, or to industry (except on government business);
- CIIP conferences;

857 http://www.usdoj.gov/ag/events/g82004/Communique_2004_G8_JHA_Ministerial_051204.pdf.

858 http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf and http://www.eda.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/cybsec.ContentPar.0086.UpFile.tmp/xy_yymmdd_0123456789_l.pdf, p.3.

859 http://www.usdoj.gov/ag/events/g82004/G8_Best_Practices_Network_Security.pdf.

- A summary of domestic legal frameworks and avenues of co-operation for addressing illegal internet content;
- Best practice for law enforcement in addressing criminal misuse of wireless networks;[860]
- A summary of countries' national legislation regarding law enforcement treatment of encrypted evidence and current trends in criminal use of encryption;
- A standard template for making and responding to requests for 24/7 high-tech investigative assistance;
- A work plan for tackling viruses, worms, and other malicious code.

During its presidency of the G8 for the year 2005, the UK has defined the improvement of the international co-operation in the CIIP field as a main objective.[861]

From 15–17 June 2005, a meeting of the justice and home affairs ministers was held in Sheffield. On the basis of this meeting, the justice and home affairs ministers published a communiqué on CIIP. The communiqué refers to the "Unified Response Tabletop Exercise" hosted in New Orleans by the G8 High-Tech Crime sub-group in May 2005, where different experts in law enforcement, watch and warning, and industry met to find solutions to challenges in the field of CIIP. The communiqué also outlines where further action is required:

- To continue to enhance communication and information-sharing between watch and warning organizations and law enforcement agencies;
- To ensure that all G8 countries have, and encourage other countries to develop, watch and warning organizations able to detect vulnerabilities and threats;
- To ensure that law enforcement agencies can quickly respond to serious cyber-threats and incidents;
- To continue and strengthen cooperation with the private sector;

860 http://www.homeoffice.gov.uk/documents/G8-WLANBstPrcNov04.pdf?version=1.
861 http://www.niscc.gov.uk/niscc/docs/re-20050401-00470.pdf?lang=en.

- To continue to conduct national and multinational training and exercises.

At the same meeting in Sheffield in June 2005, the High-Tech Crime sub-group further released a paper on "Best Practices for law enforcement interaction with victim-companies during a cyber-crime investigation".[862]

862 http://www.libertysecurity.org/article396.html.

North Atlantic Treaty Organisation (NATO)

The Ministerial Guidance for NATO Civil Emergency Planning (CEP) for 2005 and 2006 includes several references to critical infrastructure protection. The Senior Civil Emergency Planning Committee (SCEPC) has agreed to continue to examine ways to assist nations in improving their preparedness for the protection of civilian populations from terrorist attacks against critical infrastructure. Moreover, the SCEPC hast tasked its eight Planning Boards and Committees (PB&Cs) to continue to examine critical infrastructure protection from a functional perspective, and to provide integrated contributions from the areas of expertise of all Planning Boards and Committees.

Civil Communication Planning Committee (CCPC)

The Civil Communication Planning Committee (CCPC) is responsible for reviewing existing and planned electronic public and non-public communication infrastructures, services, associated facilities, postal services, and any related services with a view to determining their ability to meet the requirements of all vital users (civil and military) during emergencies. Recommendations are made to nations, taking into consideration new and emerging technology, national legislation and arrangements, and the role of international organizations in this field.

The CCPC has published a number of documents and studies on civil communications infrastructures, such as:

- Critical telecommunications infrastructure protection;[863]
- CEP consequences of disruption of critical postal infrastructure;[864]
- New risks and threats to civil telecommunications;[865]
- CEP requirements for coordinated national telecommunications regulatory measures;

* This chapter was reviewed and updated by Evert G. J. Somer, Civil Emergency Planning, NATO Headquarters, Brussels.

863 EAPC(CCPC)D(2002)8.

864 EAPC(CCPC)D(2003)2.

865 EAPC(CCPC)WP(2002)1, REV1.

- New risks and threats to the postal services.[866]

In addition, the CCPC has contributed to the "North Atlantic Council's Action Plan on Cyber Defense", such as:

- CEP consequences of the introduction of the Computer Emergency Response Teams (CERTs)/CEP consequences regarding cyber-attacks and information warfare on critical civil communication infrastructure;
- Identification and assessment of the interdependencies of other critical infrastructures on civil communication networks;
- Impact of information society developments and related opportunities for NATO CEP.

Civil Protection Committee (CPC)

In 2001, the Civil Protection Committee (CPC) established an Ad Hoc Group (AHG) to work on issues related to CIP. One of the first tasks of this AHG was to conduct a mapping survey of critical infrastructure. Nations were invited to indicate how they were structurally organized to deal with critical infrastructure protection, and to give indications about their state of readiness in terms of planning and infrastructure mapping.[867] Based on this initial mapping, definitional and conceptual work was undertaken by the AHG on CIP, resulting in a Critical Infrastructure Protection Concept Paper, approved by the SCEPC on 6 November 2003.

The Concept Paper not only proposed a way for work to be carried out by the CPC in this field, but also contained a road map detailing immediate, mid-term, and long-term actions. Also attached were a scenario to further explain the concept, and a glossary of frequently-used CIP terms.

Most recently, the CPC conducted a seminar with the theme "Critical Infrastructure Protection (CIP) — Education", which aimed to raise awareness of the importance of CIP. The primary results expected from the seminar were sets of teaching points that could form part of a CIP course curriculum and recommendations for next steps regarding the CIP concept. Such a course curriculum is now being developed by the AHG.

866 EAPC(CCPC)D(2003)1.
867 EAPC(CPC)N(2002)6.

Industrial Planning Committee (IPC)

In 2003, an Industrial Planning Committee (IPC) seminar in Slovakia was attended by senior officials and representatives from EAPC governments, industry, and trade. It focused on "Industrial Interdependencies". The aim of the seminar was to examine industrial interdependencies and resulting vulnerabilities, and to discuss potential preventive and/or consequence-management measures. These issues were introduced by plenary presentations, including two case studies – a Canadian paper on industrial interdependencies and a Slovak case study on aspects of electricity, water, gas, and chemical utilities. Other presentations looked at:

- Preventive measures for the protection of critical infrastructure;
- The military experience in infrastructure protection in France;
- Protecting critical infrastructure during disasters.

Following this initial seminar, and based on a questionnaire circulated in April 2003[868] and replies to it,[869] the IPC agreed to develop a guide containing criteria for identifying critical infrastructure in industry and the energy sector, and to compile active and passive methods of critical infrastructure protection.

Food and Agriculture Planning Committee (FAPC)

The Food and Agriculture Planning Committee (FAPC) looks at how CIP impacts on food, agriculture, and water production. In particular, the FAPC looks at threats, risks, and vulnerabilities affecting the water sector. In this, the FAPC has chosen a multi-disciplinary training approach, which will make better use of the wealth of knowledge of all NATO experts by bringing them together to work on this subject under exercise conditions. Other planning boards and committees, particularly the Transport and Telecommunications Committees, work jointly with the FAPC.

868 EAPC(IPC)N(2003)6.
869 EAPC(IPC)WP(2003)2.

Civil Aviation Planning Committee (CAPC)

The Civil Aviation Planning Committee (CAPC) has begun identifying critical infrastructure vulnerabilities and possible protective measures in the area of civil aviation. While the protection of airports, equipment, and resources is primarily a national responsibility, the Civil Aviation Working Group has discussed minimum standards that can help to make national efforts more effective. Any large-scale military deployment would require the transport capabilities of the civil aviation sector and the related infrastructure elements, which together with the air traffic control network, the power grid, fuel supplies, and supporting surface transportation are essential parts of NATO's deployment capability.

Planning Board for Inland Surface Transportation (PBIST)

The Planning Board for Inland Surface Transportation (PBIST) has conducted exploratory and definitional work on problems that may result from attacks on critical inland surface transport infrastructure. A PBIST report emphasizes that the civilian transport infrastructure is considered an attractive target, as global trade depends heavily on transportation.[870] The report aims to reach conclusions on threats to the inland transport infrastructure, characteristics of likely targets, possible protective measures, and the potential role of the PBIST.

Planning Board for Ocean Shipping (PBOS)

At the behest of the NATO Council and the SCEPC, the Planning Board for Ocean Shipping (PBOS) continues to serve as the NATO focal point for advice and assistance on the protection of civilian maritime assets against acts of terrorism. This work includes: monitoring the work and activities of other international bodies, gathering and exchanging information from international and national sources, and providing advice and assistance as necessary.

870 EAPC(PBIST)D(2003)8.

Coordination

Overall responsibility for coordinating CIP work lies with the SCEPC. However, on the initiative of the CPC, representatives of the Planning Boards & Committees (PB&Cs) meet on a regular basis to discuss various issues related to CIP. These meetings are an opportunity for all PB&Cs to present work that is under way and/or planned within their respective areas of interest, in addition to fostering closer cooperation and coordination.

Organisation for Economic Co-operation and Development (OECD)

The Organisation for Economic Co-operation and Development (OECD) is increasingly becoming involved in the issue of CIIP. The OECD is also committed to the fight against cyber-crime in two ways: it produces documentation (resolutions and recommendations) to help governments and businesses in this fight, and it raises awareness through the publication of information and statistics. There is a consensus among the member countries that secure and reliable (information) infrastructures and services are a necessary requirement for trustworthy e-commerce, secure transactions, and personal data protection. This is the main reason why the OECD Working Party on Information Security and Privacy (WPISP) promotes a global approach to policy-making in these areas to help build trust online.[871] In addition, the Committee for Information, Computer and Communications Policy (ICCP) analyzes the broad policy framework underlying the e-economy, information infrastructures, and the information society.[872]

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

The events of 11 September 2001 in the US marked a turning point for the OECD's efforts for CIIP. In order to improve measures against cyber-crime, computer viruses, and hacking, the OECD drew up new guidelines. At their 1037th session on 25 July 2002, the OECD members adopted the new "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security"[873]. The guidelines are not binding. However, they are the result of a consensus between OECD governments and of discussions involv-

* The OECD Survey of 2006 was reviewed by Peter Lübkert, Anne Carblanc, and Laurent Bernat, Organisation for Economic Co-operation and Development (OECD).

871 http://www.oecd.org/topic/0,2686,en_2649_34255_1_1_1_1_37409,00.html.

872 http://www.oecd.org/department/0,2688,en_2649_34223_1_1_1_1_1,00.html.

873 http://www.oecd.org/documentprint/0,2744,en_2649_33703_15582250_1_1_1_37409,00.html.

ing representatives of the information technology industry, business users, and civil society.[874] The OECD invites governments in other countries to adopt a similar approach to CIIP. Furthermore, the private-sector representatives are asked to improve security in their own environment, and so to provide security information and updates to the users. The individual users are urged to be more aware and responsible, and also to take the best preventive measures possible to decrease the risks to CI/CII. The OECD Guidelines include the following complementary principles at policy and operational levels:

- Awareness: Participants should be aware of the need for security of information systems and networks and of options to enhance security.
- Responsibility: All participants are responsible for the security of information systems and networks.
- Response: Participants should act in a timely and co-operative manner to prevent, detect, and respond to security incidents.
- Ethics: Participants should respect the legitimate interests of others.
- Democracy: The security of information systems and networks should be compatible with the essential values of a democratic society.
- Risk assessment: Participants should conduct risk assessment.
- Security design and implementation: Participants should incorporate security as an essential element of information systems and networks.
- Security management: Participant should adopt a comprehensive approach to security management.
- Reassessment: Participants should review and reassess the security of information systems and networks and make appropriate modifications to security policies, practices, measures, and procedures.[845]

874 http://www.oecd.org/documentprint/0,2744,en_2649_34255_1946997_1_1_1_37409,00.html.

875 OECD Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security (2002), pp. 10–12. http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf.

"Culture of Security" Website

In December 2003, the OECD launched the "Culture of Security" website as part of the organization's initiative to promote a global culture of security. The site primarily provides member and non-member governments with an international information-exchange tool on initiatives to implement the OECD Security Guidelines. The OECD website provides an overview of:

- National implementation initiatives: Activities in various countries to apply the OECD Security Guidelines at the national level;
- Selection of practical tools: Countries are developing varied and useful tools to encourage awareness, education, and individual responsibility;
- International co-operation: Action taken by governments and international organizations at the regional or international levels to co-operate among themselves and/or with other participants.[876]

OECD Forums and Workshops

Other OECD efforts concerning CIIP included the OECD-APEC Global Forum on Policy Frameworks for the Digital Economy, held in Honolulu in January 2003, and the OECD Global Forum on Information Systems and Network Security, which was convened in Oslo in October 2003. The Honolulu Forum emphasized the importance of the security of information systems and networks, as well as the need for the OECD to implement the OECD Security Guidelines. Furthermore, it emphasized the importance of preparing for the World Summit on the Information Society (WSIS) in December 2003 in Geneva (Switzerland) . Many Asia-Pacific Economic Cooperation (APEC) member countries were invited to the Oslo conference due to an agreement made in Honolulu to increase the co-operation between the OECD and APEC. This is another major step towards international and transnational management of CIIP efforts.

876 http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase.

Among the main intended policy impacts of the Oslo Forum are:

- Raising awareness of the importance of secure information systems and networks for safeguarding critical infrastructures, as well as business and consumer information;
- Increasing knowledge of the OECD Security Guidelines;
- Encouraging the development and the promotion of security architectures for organizations that effectively protect information systems;
- Exploring the use of technology and security standards in safeguarding IT infrastructures.

In September 2005, an OECD-APEC Workshop on Security of Information Systems and Networks was held in Seoul (South Korea). Topics discussed included spyware, reaching out to SMEs and individuals, promoting effective global incident response (e.g., the roles of governments and CERTs/CSIRTs), emerging security threats and the technologies being developed to address them, as well as the role of research and development, and finally, a comparison of legislative and policy approaches to improve management and the security of information systems and networks.[877]

877 http://www.oecd.org/document/25/0,2340,en_2649_201185_35481241_1_1_1_1,00.html.

United Nations (UN)

Issues related to CIIP have been discussed by the United Nations (UN) and its system of organizations since the end of the 1980s. However, formal CIIP efforts are a more recent phenomenon. Several initiatives have since been undertaken towards better work coordination. Among these are initiatives taken by UN institutions, several UN resolutions, and the results of the World Summit on the Information Society (WSIS).

UN Institute for Disarmament Research (UNIDIR) Workshop

An important first step was the organization of a workshop in July 1999 by the UN Institute for Disarmament Research (UNDIR) in Geneva. The main topic was how to better achieve worldwide information security and assurance in a global digital environment. In this context, a variety of issues, such as the Revolution in Military Affairs (RMA) and the proliferation of offensive tools for attacking information systems and networks, were discussed in Geneva. There was consensus among the participants that the vulnerability of national and international information infrastructures to cyber-attacks was increasing, and that international cooperation had to be improved in order to meet this challenge. One other conclusion was that the issue of CIIP is not only of military or strategic importance, but that it is mainly a political, economic, and social issue.[878] Hence, it is crucial to achieve cooperation between public and private actors as well as between nations.

UN General Assembly Resolutions

In December 2000 and 2001, the 55th and 56th UN General Assemblies issued Resolutions 55/63 and 56/121 on "Combating the criminal misuse of

* The United Nations Survey of 2006 was reviewed by Robert Shaw and Christine Sund, International Telecommunication Union (ITU).

878 Dependability Development Support Initiative (DDSI): International Organisations and Dependability-related Activities (draft, 31 May 2002), p. 66. http://www.ddsi.org/Documents/CR/DDSI_International_organisations.pdf.

879 UN General Assembly Resolution 55/63 and 56/121 (23 January 2002). Combating the criminal misuse of information technologies. http://www.un.org/documents.

information technologies".[879] This was another important step in the efforts of the UN concerning CIIP. These resolutions emphasize in particular that the Commission on Crime Prevention and Criminal Justice is intended to make law enforcement more efficient and effective. Furthermore, the importance of cooperation among countries and between the public and private sectors was stressed once again. The resolutions also mention the Cyber Crime Convention of the Council of Europe and the work done by the G8 as crucial milestones in the international field.[880]

In December 2002, the 57th UN General Assembly issued Resolution 57/239 on the "Creation of a global culture of cyber-security".[881] This resolution emphasizes that effective cyber-security not only requires action at the governmental level, but must be supported throughout society. Therefore, it points out the different actors responsible in the field of cyber-security, namely, governments, businesses, and other organizations, as well as individual owners and users of information technologies. The resolution further recognizes once more the importance of international cooperation. The annex outlines nine complementary elements required to create a global culture of cyber-security. They range from awareness of the need for security of information systems and networks, to identifying adequate action in the field of CIIP (taking into account ethical and democratic principles), to security management and reassessment.[882]

In December 2003, the 28th UN General Assembly issued Resolution 58/199 on the "Creation of a global culture of cyber-security and the protection of critical information infrastructure".[883] This resolution points out the increasing links among most countries' critical infrastructure and the growing number and variety of threats facing them. The resolution's annex outlines 11 principles for protecting CII, which are based on those adopted by the G8 Justice and Interior Ministers in Paris in 2003. The UN General Assembly invites member states and international organizations to consider these principles for protecting CII, as well as to share their best practices

880 Ibid.

881 UN General Assembly Resolution 57/239 (31 January 2003). Creation of a global culture of cybersecurity. http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf.

882 Ibid.

883 UN General Assembly Resolution 58/199 (30 January 2004). Creation of a global culture of cybersecurity and the protection of critical information infrastructures. http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.

and measures that could assist other actors in their efforts to achieve cybersecurity. Furthermore, the resolution asks that these principles be taken into account in preparations for the second phase of the World Summit on the Information Society (WSIS) in Tunisia in November 2005. Finally, the UN General Assembly outlines the necessity of involving the developing and the least developed countries in CIIP, which means that that the transfer of information technology and capacity-building efforts need to be strengthened.[884]

UN ICT Task Force

The establishment of the UN ICT Task Force in November 2001, in response to a request by the UN Economic and Social Council, was a further important step. The task force was mandated to mobilize worldwide support for attaining the Millennium Development Goals with the use of ICT. In September 2002, the task force published a guide called "Information Security – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security".[885] This publication depicts the problem of information insecurity in general, and provides possible solutions for prevention and response to security incidents (including standards and best practices).[886]

In April 2004, a seminar on "Policy and security issues in information technology" was held at the UN Headquarters. Part of the seminar series was on policy awareness and training in information technology, organized by the ICT Task Force and the UN Institute for Training and Research (UNITAR).[887]

UN and the World Summit on the Information Society (WSIS)

Recognizing that confidence and security in the use of information and communication technologies (ICT) are the main pillars of the information society, the first phase of the World Summit on the Information Society (WSIS) in

884 Ibid.

885 Gelbstein, Eduardo and Ahmad Kamal. Information Insecurity – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security (New York, 2002). https://unp.un.org/details.aspx?entry=E04291#.

886 Ibid.

887 http://www.unicttaskforce.org/perl/documents.pl?id=1352.

December 2003 urged governments, in cooperation with the private sector, to consider legislation that allows for effective investigation and prosecution of misuse and strengthens institutional support at the international level. As a result, a number of recommendations were made in the WSIS Geneva 2003 first phase Declaration of Principles and Plan of Action[888] that relate to building confidence and security in the use of ICTs and promoting a global culture of cyber-security.

The outcomes of the second phase of the WSIS, held in Tunisia in November 2005, are summarized in the Tunis Agenda and Tunis Commitment. All governments, according to the Tunis Agenda,[889] should have an equal role and responsibility in internet governance, but must also ensure the internet's stability, security, and continuity. It calls for enhanced cooperation to enable all governments to carry out these responsibilities, including the development of globally applicable principles on public policy issues associated with the coordination and management of critical internet resources.

The Tunis Agenda also recognizes the need for "national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data." It underlines "the importance of the security, continuity and stability of the Internet, and the need to protect the Internet and other ICT networks from threats and vulnerabilities." It further emphasizes "the need for a common understanding of the issues of Internet security, and for further cooperation to facilitate outreach, the collection and dissemination of security-related information and exchange of good practice among all stakeholders on measures to combat security threats, at national and international levels."

The annex to the Tunis Agenda offers an indicative list of possible moderators and facilitators for each of the 11 action lines in the WSIS Geneva Plan of Action. The International Telecommunication Union (ITU) is named as sole facilitator for the action line related to "Building confidence and security in the use of ICT".[890]

888 World Summit on the Information Society (WSIS) Outcome Documents (Declaration of Principles, Action Plan, Tunis Commitment and Tunis Agenda). http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160|2266|2267.

889 World Summit on the Information Society (WSIS) Tunis Agenda. http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

890 WSIS Geneva Plan of Action, action line C5 on "Building confidence and security in the use of ICTs".

International Telecommunication Union (ITU)

The International Telecommunication Union (ITU) is an international organization (specialized agency) within the United Nations System where governments and the private sector coordinate global telecom networks and services. In accordance with UN strategic initiatives, the ITU Plenipotentiary Conference in Marrakesh 2002 adopted ITU Resolution 130. This document highlighted the need to strengthen the role of the ITU in information and communication network security and to intensify work within existing ITU study groups, and invited ITU Member States and Sector Members to participate actively in the ongoing work of the relevant ITU study groups. It also called on them to continue to publicize the need to defend information and communication networks against the threat of cyber-attack, and to cooperate with other entities in these efforts. Related ITU World Telecommunication Standardization Resolutions from 2004 include: Resolution 50 on "Cybersecurity", Resolution 51 on "Combating spam" and Resolution 52 on "Countering spam by technical means".[891].

There are currently more than 70 ITU recommendations focusing on security. Through its standards, development, and policy research activities, the ITU has a long-standing track record in security for information and communication systems and aims to continue to contribute to increase confidence and security in the use of ICTs and promoting a global culture of cyber-security.

ITU WSIS Thematic Meeting on Cybersecurity

The ITU was the leading UN agency in the organization of the World Summit on the Information Society (WSIS). In July 2005, the ITU WSIS Thematic Meeting on Cybersecurity was held in Geneva. The event examined the recommendations of the first phase of WSIS, which relates to building confidence and security in the use of ICTs and the promotion of a global culture of cyber-security. Six broad themes were considered in promoting international dialog and cooperative measures among governments, the private sector, and

891 Some ITU resolutions and initiatives related to cyber-security are available at: http://www.itu.int/osg/spu/cybersecurity/ituevents.html.

other stakeholders as well as promotion of a global culture of cyber-security. These include information-sharing on national and regional approaches, good practices, and guidelines; developing watch, warning, and incident response capabilities; technical standards and industry solutions; harmonizing national legal approaches and international legal coordination; privacy, data and consumer protection, and cyber-security.[892]

One of the findings of the Geneva meeting on cyber-security was that most of the challenges related to protecting information systems are non-technical. Instead, they tend to revolve around the management of highly complex systems, where interdependencies, as well as the potential magnitudes and consequences of disruptions, are not yet well understood. Moreover, it was stated that complexity is the worse enemy of security. Another challenge lies in the implementation of security measures, which lag behind for several reasons. For instance, incentive structures to encourage individuals and the private sector to improve CIIP may be achieved in the form of insurance requirements, liability, standards, deductions, or tax credits. The potential liability of software developers for bugs in their products was also discussed. Finally, the need for assisting developing economies in adopting security standards was identified.[893]

World Telecommunication Day

Each year on 17 May, the ITU celebrates World Telecommunication Day, which commemorates the ITU's founding in 1865 as well as its long history of fulfilling its mission of "Helping the World Communicate". Based on a decision of the ITU's governing council, the theme of World Telecommunication Day[894] is "Promoting Global Cybersecurity". In preparation, ITU plans an awareness-raising campaign in support of this objective and looks forward to working further in close cooperation with the many entities involved in global cyber-security issues.

892 http://www.itu.int/osg/spu/newslog/CategoryView,category,Privacy.aspx and http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.

893 Chairman's Report Version 2. ITU WSIS Thematic Meeting on Cybersecurity (ITU Headquarters, Geneva, 28 June-1 July 2005), pp. 19–20. http://www.itu.int/osg/spu/cybersecurity/chairmansreport.pdf.

894 Following the WSIS Tunis phase and the resulting Tunis Agenda, World Telecommunication Day will be observed as World Information Society Day, pending approval by the UN General Assembly.

The World Bank Group

The growing incidence of computer and cyber-crime has a particularly strong bearing on the financial sector. In view of the growing amount of financial data stored and transmitted online, the ease of computer intrusions has added to the severity of the problem. Therefore, the World Bank Group has taken several steps over the last few years the face the challenges of information security, especially in developing countries.[895]

The Global Information and Communication Technologies Department (GICT)

The Global Information and Communication Technologies Department (GICT)[896] promotes access to information and communication technologies in developing countries. It serves as the World Bank Group's core department for investment, policy, and programs related to information and communications technologies. The GICT's aim is to expand access to a range of information infrastructure networks and support the development and application of information technologies to reduce poverty and improve people's lives. The GICT has four teams:

- The Policy Division provides policy and regulatory advice to governments on telecommunications, postal and broadcast services, and e-applications.
- The Communications Investment Division provides loans and equity financing to businesses in the private sector manufacturing telecommunication, broadband connectivity, broadcast and media, and satellite equipment.
- The Portfolio and Technology Investment Division provides equity, mezzanine, and loan financing to a variety of technology firms, including technology services, business process outsourcing, software development, chip design, and e-government applications.

895 http://info.worldbank.org/ict/index.cfm.
896 http://info.worldbank.org/ict/index.cfm.

- The Information for Development Program (infoDev)[897] provides grants to innovative projects, generates knowledge, and disseminates lessons learned. The principal focus of infoDev's activities in 2004–2005 was on how ICTs can substantially advance progress toward the Millennium Development Goals (MDGs). InfoDev also maintains a website focusing on IT security issues. Its first product is the "Information Technology Security Handbook".[898]

Information Technology Security Handbook

The "Information Technology Security Handbook",[899] funded by the Information for Development Program (infoDev Program) of the World Bank Group, provides technology-independent best practices and recommendations in the field of IT security. The handbook was published in 2003 and, as the technology evolves, the accompanying website[900] provides updates as appropriate. The book addresses private users of IT, small and medium organizations, government, and technical administrators, especially in developing countries. The handbook is based on the premise that use of ICT is on the rise, while the knowledge of IT security practices is lagging behind.

After a general introduction to IT security, the Information Technology Security Handbook deals with topics such as:

- Security for individuals: keeping personal computers, data and operating systems, and applications secure; malicious software; securing services over networks; tools to enhance security; and the role of encoding and encryption.
- Security for organizations: risk evaluation and mitigation; planning; organizational security policy and personnel security; security outsourcing; mobile risk management; and best practices.

897 http://www.infodev.org.

898 http://info.worldbank.org/ict/gict.cfm and http://www.infodev-security.net/handbook.

899 The International Bank for Reconstruction and Development/The World Bank (infoDev). Information Technology Security Handbook (Washington 2003). http://www.infodev-security.net/handbook.

900 http://www.infodev-security.net.

- Information security and government policies: various arrangements for protecting government systems; laws and legislation; and government policy in promoting better security in the private sector.
- IT security for technical administrators: physical security; information security; identification and authentication; server security; network security; attack and defenses; and detecting and managing breakins.[901]

Technology Risk Checklist

The World Bank published a report on "Electronic Security: Risk Mitigation in the Financial Transactions" in June 2002, building on previous papers that identified e-security as a key component to the delivery of e-finance benefits. This paper and its technical annexes identify and discuss eight key pillars for a secure electronic environment.[902]

In January and May 2004, a follow-up publication was published, entitled "Technology Risk Checklist".[903] The World Bank publication describes 13 layers of e-security, covering both hardware and software pertaining to network infrastructures. These layers cover risk management, policy management, cyber-intelligence, access controls and authentication, firewalls, active content filtering, intrusion detection systems (IDS), virus scanners, encryption, vulnerability testing, systems administration, incident response plans (IRP), and wireless security.[904]

901 Ibid.
902 The World Bank. Electronic Security: Risk Mitigation in the Financial Transactions. Public Policy Issues, (June 2002). http://www.digitaldefense.net/white_papers/Risk_Mitigation_in_Financial_Transactions_version_2.pdf.
903 The World Bank. Technology Risk Checklist, (May 2004, Version 7.3). http://www.infragard.net/library/pdfs/technologyrisklist.pdf.
904 Ibid., pp. 2–4.

Conclusion

Analysis and Conclusion

For a number of years, policy-makers at the highest levels have been expressing their concern that insecure information systems threaten economic growth and national security. As a result of these concerns, a complex and overlapping web of national, regional, and multilateral initiatives has emerged. The International CIIP Handbook provides an overview of issues of high importance in the field of critical information infrastructure protection (CIIP), serves as a reference work for the interested community, and provides a basis for further research by compiling relevant material. Despite the sometimes substantial differences between these governmental protection policies, they offer a wealth of empirical material from which a variety of lessons can be distilled for the benefit of the international community.

For each survey, five focal points of high importance covering conceptual and organizational aspects of CIIP were considered. In the following, we will wrap up each of these five points: the definition of critical sectors and the CIP/CIIP conceptual framework; past and present initiatives and policies; organizational structures; early warning approaches and public outreach; and law and legislation. Finally, we shall discuss how the surveyed national efforts will contribute towards a global culture of cyber-security.

Critical Sectors

Variations between countries can be seen not only in the definition of critical sectors, but also in the definition of CIP and CIIP. Some countries, such as Australia, Canada, Germany, the Netherlands, New Zealand, the UK, or the US, provide clear definitions of CIP, while other countries — for example Austria, the Republic of Korea, or Russia —, offer none at all. Everywhere, CIIP is seen as a subset of CIP, including protection, detection, response, and recovery activities at both the physical and the virtual levels. However, a clear distinction between CIP and CIIP is lacking in most countries, and one finds both terms being used interchangeably.

The choice of the "sector" as a unit of analysis is a pragmatic approach that roughly follows the boundaries of existing business/industry sectors. In designating critical sectors, many countries have followed the example of the Presidential Commission on Critical Infrastructure Protection (PCCIP),

which was the first official publication to identify critical infrastructures with specific business sectors or industries.[905] This approach also reflects the fact that the majority of infrastructures is owned and operated by private actors.

Accordingly, government officials acknowledge the need for partnerships between infrastructure owners and operators on the one hand and the government on the other. The decision on which infrastructures and sectors to include in the list of critical assets also requires input from private sector experts, besides experts and officials at various levels of government. More often than not, expert groups address the issue, either in larger or smaller groups.[906] Usually, a component or a whole infrastructure is defined as "critical" due to its strategic position within the whole system of infrastructures, and especially due to the interdependency between the component or the infrastructure and other infrastructures.

It is broadly acknowledged, however, that the focus on sectors is far too artificial to represent the realities of complex infrastructure systems. For a more meaningful analysis, it is therefore deemed necessary to evolve beyond the conventional "sector"-based focus and to look at the services, the physical and electronic (information) flows, their role and function for society, and especially the core values that are delivered by the infrastructures. Therefore, experts groups often focus on four steps in the identification of what is critical: 1) critical sectors, 2) sub-sectors for each sector on the basis of organizational criteria, 3) core functions of the sub-sectors, and 4) resources necessary for the functioning of the sub-sectors.[907]

Table 1 shows which country defines which sectors as critical. One must be careful, however, to avoid misleading comparisons: While for instance Australia, Canada, the Netherlands, Japan, the UK, and the US are very precise in identifying critical sectors and sub-sectors as well as products and services that these sectors provide, other countries, such as Austria, the Republic of Korea, Russia, or Sweden, have no official list of CI sectors.

905 President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures (Washington, October 1997). Publication quoted in the following as PCCIP.

906 Dunn, Myriam. "Part II: Analysis of Methods and Models for CII Assessment". In: Dunn, Myriam and Isabelle Wigert. The International Critical Information Infrastructure Protection (CIIP) Handbook 2004 (Zurich, Center for Security Studies, 2004), pp. 219–297.

907 Ibid., pp. 227–228.

Variations in terminology can be explained by differences in conceptualizations of what is critical, but also by country-specific peculiarities and traditions. Individual sectors, for example "Social Security/Welfare", "Insurance", or "Civil Defense", are influenced by socio-political factors and traditions, while others, for example "Water/Flood Management" in the case of the Netherlands, are subject to geographical and historical preconditions. Some sectors have newly been added after disturbing incidents. This is the case for the categories of "National Icons and Monuments" or the "Post Systems", introduced after 11 September 2001, or the "Meteorological Services", identified as a specific critical sub-sector in Canada after an ice storm in 1998 that severely affected Eastern Canada and Quebec. In spring of 2005, the Japanese Committee for Essential Issues on Information Security recommended the expansion of the existing list of critical infrastructure sectors to include "Medical Services", "Water", and "Distribution",[908] likely as a consequence of the avian influenza scare.

The most frequently mentioned critical sectors in all countries are listed below. These are the core sectors of modern societies, and possibly the areas where a large-scale interruption would be most devastating:

- Banking and Finance,
- Central Government/Government Services,
- (Tele-) Communication/Information and Communication Technologies (ICT),
- Emergency/Rescue Services,
- Energy/Electricity,
- Health Services,
- Transportation/Logistics/Distribution, and
- Water (Supply).

This comparison shows that the concept of criticality is undergoing constant change, and that the criteria for determining which infrastructures qualify as critical have expanded over time; the PCCIP, for example, defined assets whose prolonged disruptions could cause significant military and economic disloca-

908 Yoshida, Mabito. "Information Security Policies in Japan". Presentation held at the ITU WSIS Thematic Meeting on Cybersecurity (Geneva, 29 June 2005). http://www.itu.int/osg/spu/cybersecurity/presentations/session7_yoshida.pdf.

Country / Sector	AUS	A	CAN	F	FIN	GER	IND
Air Control Systems / Space							
Banking and Finance	●	●	●	●	●	●	●
Chemical and Nuclear Industry							
Central Government / Government Services	●		●			●	
Civil Defense							
(Tele)Communications / ICT	●	●	●	●	●	●	●
Dams							
(Higher) Education							
Energy / Electricity	●	●	●	●	●	●	●
Emergency / Rescue Services	●	●	●			●	
Food / Agriculture	●		●		●	●	
Hazardous Materials / CBRN			●				
Health Services	●	●	●	●	●	●	
(Defense) Industry / Manufacturing	●		●	●	●		
Information Services / Media / Broadcasting	●	●	●		●		
Insurance	●					●	●
Justice / Law Enforcement						●	●
Military Defense / Army / Defense Facilities	●	●				●	●
National Icons and Monuments	●		●				
Nuclear Power (Plants)				●		●	
Oil and Gas Supply	●		●			●	●
Police Services	●	●	●				
Post Systems		●					
Prominent Public Places / High Profile Events							
Public Administration		●			●	●	
Public Order / Public Safety				●			
Sewerage / Waste Management	●		●				
Social Securtiy / Welfare		●					
Transportation (air, sea, land) / Logistics / Distribution	●	●	●	●	●		●
Utilities	●	●			●	●	
Water (Supply)	●	●	●	●	●	●	
Water / Flood Management							

Table 1: Overview of the Critical Sectors and Sub-sectors Identified by Surveyed Countries

IT	JAP	KOR	MAL	NL	NO	NZ	RU	SE	SING	SWIT	UK	USA	Total
								●					1
●	●	●	●	●	●	●	●	●	●	●	●	●	20
				●									1
	●	●	●	●	●	●		●			●	●	12
										●			1
●	●	●	●	●	●	●	●	●	●	●	●	●	20
												●	1
												●	1
●	●	●	●	●	●	●	●	●	●	●	●	●	20
●		●	●		●	●				●	●	●	12
				●							●	●	7
											●	●	3
●	●		●	●	●				●	●	●	●	15
			●				●			●		●	8
		●	●	●			●	●		●	●		11
												●	4
				●		●					●	●	6
		●	●	●	●		●						9
												●	3
												●	3
●	●	●		●	●	●	●				●	●	13
					●						●		5
												●	2
									●				1
●				●						●	●	●	8
●				●							●		4
●			●		●						●		6
					●	●							3
●	●	●	●	●	●	●	●		●	●	●	●	18
					●								5
●	●		●	●	●				●	●	●	●	15
				●									1

tion as critical.[909] Today, critical infrastructures in the US also include national monuments (e.g., the Washington Monument), where an attack might cause a large loss of life or adversely affect the nation's morale.[910] This development shows two differing, but interrelated perceptions of criticality:[911]

Criticality as systemic concept: This approach assumes that an infrastructure or an infrastructure component is critical due to its structural position in the whole system of infrastructures, especially when it constitutes an important link between other infrastructures or sectors, and thus reinforces interdependencies.

Criticality as a symbolic concept: This approach assumes that an infrastructure or an infrastructure component is inherently critical because of its role or function in society; the issue of interdependencies is secondary – the inherent symbolic meaning of certain infrastructures is enough to make them interesting targets.[912]

The symbolic understanding of criticality allows the integration of non-interdependent infrastructures as well as objects that are not man-made into the concept of critical infrastructures, including significant personalities or natural and historical siteswith a strong symbolic character. Additionally, the symbolic approach allows us to define essential assets more easily than the systemic one, because in a socio-political context, the defining element is not interdependency as such, but the role, relevance, and symbolic value of specific infrastructures.[913]

The emphasis on the interconnectedness of various sectors, in connection with this symbolic understanding, creates a specific set of problems for decision-makers: Basically, everything is networked, and even a discrete event of

909 PCCIP, 1997, op. cit. Appendix B, Glossary, B-2.

910 Moteff, John, Claudia Copeland, and John Fischer. Critical Infrastructures: What Makes an Infrastructure Critical? CRS (Congressional Research Service) Report for Congress RL31556 (30 August 2002). http://www.fas.org/irp/crs/RL31556.pdf.

911 Metzger, Jan. "The Concept of Critical Infrastructure Protection (CIP)". In: Bailes, A. J. K. and Isabelle Frommelt (eds.). Business and Security: Public-Private Sector Relationships in a New Security Environment (Oxford: Oxford University Press, 2004), pp. 197–209.

912 For an example (critical assessment without interdependencies), see: United States General Accounting Office (GAO). Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations; House Committee on Government Reform. Homeland Security: Key Elements of a Risk Management, Statement of Raymond J. Decker, Director Defense Capabilities and Management (12 October 2001), p. 6. http://www.gao.gov/new.items/d02150t.pdf.

913 Metzger, op. cit.

little apparent significance could potentially set off unpredictable cascading effects throughout a large number of sectors. When the concept of criticality, and accordingly the scope of what is to be secured, is expanded from interconnected physical networks like the electrical grid and road networks to include everything with emotional significance, ranging from schools to national monuments, almost everything becomes an "infrastructure" and everything is potentially critical. In this situation, decision-makers must be careful not to follow the natural impulse to secure everything that could possibly be at risk, because total protection will never be possible. Prioritization must be based on careful risk assessment that comprises calculations of the likelihood of a given threat source displaying a particular potential vulnerability, and the resulting impact of that adverse event.[914]

However, even though risk analysis is extremely well established and used in different communities, it has many shortcomings. This issue is addressed in additional detail in Vol. II by Myriam Dunn, who argues that shortcomings include the lack of data to support objective probability estimates, persistent value questions, and conflicting interests within complex decision-making processes. There are both theoretical and practical difficulties involved in estimating the probabilities and consequences of high-impact, low-probability events — and this is the scenario we are dealing with in the context of CIIP. It also appears that there is no way of cataloguing objects, vulnerabilities, and threats on a strategic policy level, such as the economy at large, in a meaningful way. Existing risk analysis methodology further fails to address interdependencies directly, which is a major shortcoming.

In general, threat assessment in connection with actor-centered research has been largely neglected in the field of CIIP. Many aspects of the threat appear unsubstantiated at a closer look: due to the lack of experience, statements on the scope of the danger often seem purely speculative. This could be resolved with more research into the changes in the threat environment and its impacts on CIIP. Threat issues are also addressed in additional detail in Vol. II by Clay Wilson, Michel J.G. van Eeten, Emery Roe, Paul Schulman, and Mark de Bruijne.

914 Stoneburner, Gary, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30 (Washington: US Government Printing Office, January 2002), p. 8. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Past and Present Initiatives and Policies

During the late 1990s, decision-makers launched myriad initiatives to come to terms with the newly perceived risks of information and communication technologies. Many of the national CIIP efforts were triggered by the Presidential Commission on Critical Infrastructure Protection (PCCIP) set up by US president Bill Clinton in 1996, and to some extent by the preparations for anticipated problems on the threshold of the year 2000 (Y2K problem). This led to the establishment of (interdepartmental) committees, task forces, and working groups. Their mandate often included scenario work, the evaluation of a variety of measures, or assessments of early warning systems. These efforts resulted in policy statements — such as recommendations for the establishment of independent organizations dealing with information society issues — and reports laying down basic CIIP policies.

In the aftermath of 11 September 2001 ("9/11"), several countries launched further initiatives to strengthen and allocate additional resources to their CIP/CIIP efforts. Prior to 9/11, for many people, critical infrastructure protection was synonymous with cyber-security. The attacks of 9/11, however, highlighted the fact that terrorists could cause enormous damage by attacking critical infrastructures directly and physically, and thus demonstrated the need to re-examine physical protection, especially in the US.[915] The undue prioritization of the cyber-dimension, so it seemed after 9/11, had led to a shift in focus from the virtual to the physical domain, and from CIIP to CIP.

It is obvious that governmental cyber-security policies are at various stages of implementation — some are enforced, while others are just a set of suggestions — and come in various shapes and forms, ranging from a regulatory policy focus concerned with the smooth and routine operation of infrastructures and questions such as privacy or standards, to the inclusion of cyber-security into more general counter-terrorism efforts. In countries such as France, New Zealand, and Sweden, CIIP efforts are mainly led by the defense establishment, whereas in other countries, such as the UK or Switzerland, approaches to CIIP are jointly led by the business community and public agencies. Furthermore, in Australia as well as in the US and New Zealand, CIIP is integrated into the overall counterterrorism efforts, where the intelligence community plays an important role. In India, the Republic

915 Moteff et al. op. cit., p. 3.

of Korea, Japan, Singapore, Finland, India, and Malaysia, the fostering of the information society and economic growth through safe information infrastructures is at the forefront.

Russia represents a special case due to the close link between information security and state secrecy. In the Russian view, information assurance not only includes (technical) information security, but also control over the free flow of information and over the exchange of information (especially of information that may harm the state) and the safeguarding of state secrets. In addition to the physical or virtual information systems and flows, the state also wants to protect the actual content of the information.

In all countries, CIIP is only one aspect of the overall topic of information security. Most countries consider CIIP to be a national-security issue of some sort. In parallel, however, they often pursue a business continuity strategy under the "information society" label. The law enforcement/crime prevention perspective is also found in all countries. Furthermore, data protection issues are a major topic for civil rights groups. While all of the perspectives can be found in all countries, the emphasis given to one or more of the perspectives varies to a considerable degree. This issue is also addressed in Vol. II by Isabelle Abele-Wigert, who shows how practical and academic dialog is hampered by vastly differing terminology and viewpoints of what constitutes the problem.

All countries examined have recognized the importance of public-private partnerships (PPP). Governments actively promote information-sharing with the private sectors, since large parts of critical infrastructures are owned and operated by the business sector. Different types of such partnerships are emerging, including government-led partnerships, business-led partnerships, and joint public-private initiatives. In Switzerland, the Republic of Korea, the UK, and the US, strong links have already been established between the private business community and various government organizations. One of the future challenges in many countries will be to achieve a balance between security requirements and business efficiency imperatives. Satisfying shareholders by maximizing company profits has often led to minimal security measures. This is because like many political leaders, business leaders tend to view cyber-attacks on infrastructures as a tolerable risk. Additionally, public-private partnerships are mainly based on trust, so that information-sharing is arguably one of the most significant issues in CIIP.

Despite the general consensus on the positive aspects of PPPs, their implementation remains a problem. The issue of PPPs is also addressed in Vol. II by Jan-Joel Andersson and Andreas Malm. They show that it is relatively easy for the government and private actors in a PPP to agree on the existence of a problem and on the need for a remedy. It is, however, much harder to agree on actual measures to be taken, on the actors responsible for implementing them, on the party that will assume legal responsibility for such measures, and on the party that will bear the costs for implementing them.

Organizational Overview

Only in a few countries have central governmental organizations been created to deal specifically with cyber-security issues. Mostly, responsibility lies with multiple authorities and organizations in different governmental departments. Very often, responsibility for CIIP protection is given to well-established organizations or agencies that appear suitable for the task. Depending on their key assignment, these agencies bring their own perspective to bear on the problem and shape policy accordingly. The establishment of these organizational units and their location within the government structures are influenced by various factors such as civil defense tradition, the allocation of resources, historical experience, and the general threat perception of key actors in the policy domain.

The following is a short overview of country-specific findings with regard to organizational structure in CIIP:

- In *Australia*, several organizations are responsible for CIP/CIIP. Since terrorism has been identified as the most likely threat to arise against Australia's critical infrastructure (considering attacks on both virtual and physical structures), CIIP has been seen as part of the country's overall counter-terrorism effort. Therefore, the Critical Infrastructure Protection Group's members also include the Defence Signals Directorate, the Australian Security Intelligence Organisation, and the Australian Federal Police. All of these are operational military, security, and policing intelligence services. The e-Security Coordination Group (ESCG) is the standing interdepartmental committee with responsibility for e-security policy, whilst the Information Infrastructure Protection Group (IIPG) examines NII strategic policy.

- In *Austria*, there is no single authority responsible for CIP/CIIP – all ministries have their own specific security measures to defend against outside attack and to prevent the unauthorized usage of data. However, the Federal Chancellery fulfils a coordinating task. CIIP is mainly perceived as an issue of data protection, as the Austrian E-Government Program, the Official Austrian Data Security Website, or the Pilot Project Citizen Card indicate.
- In *Canada,* Public Safety and Emergency Preparedness Canada (PSEPC), is the key organization responsible for both CIP/CIIP and Civil Emergency Planning. Hence, Canada has a centralized organizational model for CIP/CIIP. Industry Canada also contributes to CIIP programs and initiatives in particular.
- In *Finland*, CIIP is seen as a data security issue and as a matter of economic importance, closely related to the development of the Finnish information society. Several organizations deal with CIIP, including the Finnish Communications Regulatory Authority (FICORA), the National Emergency Supply Agency (NESA), and the Steering Committee for Data Security in State Administration (VAHTI).
- In *France*, CIIP is seen both as a high-tech crime issue and as a matter of developing the information society. Overall responsibility for CIIP lies with the General Secretary of National Defense (SGDN), a secretary attached to the Prime Minister's Office.
- In *Germany*, the Federal Office of Information Security (BSI), which is part of the Ministry of the Interior, is the lead authority for CIIP matters within the organizational structure. Moreover, the Federal Agency of Civil Protection and Disaster Response (BBK), the Federal Law Enforecement Agency (BKA), and the Federal Police (BPOL) are important actors.
- In *India*, CIIP is seen as an essential part of the country's aim to become an information technology superpower. Without information security, the IT business will not be able to prosper. The National Information Board (NIB) is at the very top of the national information security structure.
- In *Italy*, CIIP is part of the advancement of the information society. There is no single authority dealing with CIIP. A Working Group on CIIP was recently set up at the Ministry for Innovation and Technologies that includes representatives of all ministries involved in the

management of critical infrastructures and many Italian infrastructure operators and owners as well as some research institutes. Besides the Working Group on CIIP, the Ministry of Innovation and Technologies, the Ministry of Communication, and the Ministry of the Interior (Postal and Communications Police) are the main Italian government bodies dealing with CIIP.

- In *Japan,* CIIP is an essential issue for becoming an advanced IT society and to provide a safe e-business and e-government environment. Within the Japanese government, the IT Strategic Headquarters within the Cabinet Secretariat plays an important role in the field of CIIP and is the main actor for central government policy issues. Also within the Cabinet Secretariat is the newly established National Information Security Center (NISC); and the newly established Information Security Policy Council (ISPC) is part of the IT Strategic Headquarters.
- In the *Republic of Korea*, CIIP is considered essential for realizing a safe "u-Korea", where information technologies will penetrate almost all aspects of public life. The National Cyber Security Center (NCSC) coordinates the efforts of the various government departments and agencies involved in CIIP. The Ministry of Information and Communication and the Korea Internet Security Center (KISC; KrCERT/CC) within the Korean Information Security Agency (KISA) make efforts to foster a culture of safe internet and telecommunication networks.
- In *Malaysia*, security issues in the public sector are administered by the Malaysian Administrative Modernization and Management Planning Unit (MAMPU). One group within MAMPU is the ICT Security Division, which also operates as a CERT for the government. The Malaysian Communications and Multimedia Commission (MCMC) has a coordinating role.
- In *The Netherlands,* responsibility for CII lies with a number of authorities, but the Ministry for Interior and Kingdom Relations coordinates CIP/CIIP policy across all sectors and responsible ministries (government CIIP). The Ministry of Economic Affairs/Directorate General Telecom and Post is responsible for the protection policy for telecommunications and the internet.
- In *New Zealand*, the Centre for Critical Infrastructure Protection (CCIP), located at the Government Communications Security Bureau, is the central institution dealing with CIIP. The main actor in charge

of formulating New Zealand's security policy, including CIIP, is the Domestic and External Secretariat (DESS), which is the support secretariat for the Officials Committee for Domestic and External Security Co-ordination (ODESC).

- In *Norway*, the national key player in Civil Emergency Planning, the Directorate for Civil Defense and Emergency Planning (DSB), subordinated to the Ministry of Justice and Police, is also a key player for CIP/CIIP-related issues. The overall authority for ICT security is the Ministry of Modernization, while the Ministry of Defense is responsible on the military side.
- In *Russia*, the main CIIP organizations are the Security Council, the Federal Security Service (FSB), the Federal Guard Service, the Federal Technical and Export Control Service as well as the Ministry of Information Technologies and Communications.
- In *Singapore*, the Infocomm Development Authority of Singapore (IDA) is the chief technology officer of the Singapore government covering planning, policy formulation, regulation, and cooperation with the private sector in the field of ICT. The National Infocomm Security Committee (NISC) and the Technology Crime Division (TCD) within the Singapore Police Forces also play important roles.
- In *Sweden*, a number of organizations are involved in CIP/CIIP. The Swedish Emergency Management Agency (SEMA) at the Ministry of Defense has a key role.
- In *Switzerland*, there are a number of different organizational units dealing with CIP/CIIP. Public-private partnerships are among the central pillars of Switzerland's CIIP policy. The Federal Strategy Unit for Information Technology (ISB) is responsible for the implementation of the Swiss information assurance policy and for the Reporting and Analysis Center for Information Assurance (MELANI). MELANI is the core of the Swiss CIIP early warning system.
- In the *United Kingdom*, the key interdepartmental organization dealing with CIP/CIIP is the National Infrastructure Security Co-ordination Centre (NISCC). The NISCC has strong ties with the private sector and runs the UK CERT "UNIRAS". The Central Sponsor for Information Assurance (CSIA) and the Civil Contingencies Secretariat (CCS) are also important CIIP actors at government level.

- In the *United States*, the Department of Homeland Security (DHS) has the leading role in CIP/CIIP. However, several other organizational units are also involved in CIP/CIIP. Public-private partnerships, e.g., Information Sharing and Analysis Centers (ISACs), are regarded as key elements of CIP/CIIP policy.

Early Warning and Public Outreach

The earlier a potential risk is identified, the greater the chance to act in a timely, resource-efficient, and strategically adequate manner. Therefore, timely warning of attacks is an indispensable component of ensuring that a breakdown of important infrastructure, or even only of certain components of ICT, will be limited to an incident that is short, rare, controllable, geographically isolated, or with as little consequences as possible for the national economy and security.

Early warning systems are designed for the following purposes, namely: understanding and mapping the hazard; monitoring and forecasting impending events; processing and disseminating understandable warnings to political authorities and the population, and undertaking appropriate and timely actions in response to the warnings. In CIIP, early warning is focused mainly on IT security incidents. The general trend in CIIP early warning points towards establishing central contact points for the security of information systems and networks. Among the existing early-warning organizations are various forms of Computer Emergency Response Teams (CERTs), e.g., special CERTs for government departments, CERTs for small and medium-sized businesses, CERTs for specific sectors, and others. CERT functions include handling of computer security incidents and vulnerabilities or reducing the probability of successful attacks by publishing security alerts. The issue is further addressed in Vol. II. by Thomas Holderegger, who examines early warning players in the CIIP sector and specifies their tasks and responsibilities, with a specific focus on the role of the nation state.

In some countries, permanent analysis and intelligence centers have been developed in order to make tactical or strategic information available to the decision-makers within the public and private sectors more efficiently. Tasks of early-warning system structures include analysis and monitoring of the situation as well as the assessment of technological developments. Examples can

be found in Canada (Government Operations Centre, GOC), in Switzerland (Reporting and Analysis Center for Information Assurance, MELANI), in the UK (National Information Security Coordination Center, NISCC), and in the US (Directorate for Information Analysis and Infrastructure Protection, IAIP). Furthermore, there is cross-border cooperation in early warning between Australia and New Zealand. Such international cooperation is sensible in view of the cross-boundary nature of cyber-threats, which are inherently transnational. Internationally, CERTs primarily exchange information at the Forum of Incident Response and Security Teams (FIRST).

Often, these entities manage outreach, cyber-security awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key stakeholders. Generally, many private enterprises, public entities, and home users lack the resources to adequately manage cyber-security risks. Many entrepreneurs and home users are unaware of the extent to which their individual cyber-security preparedness affects overall security, and internet users must be made aware of the importance of sound cyber-security practices and require more user-friendly tools to implement them. Public outreach efforts therefore entail cataloguing existing best practices, developing strategies to market those practices to specific audiences, creating incentive plans to ensure acceptance of those practices, contributing to the development of a national advertising campaign, and developing a strategy to communicate to public and private CEOs across the country about the importance of cyber security and their role in enhancing it.

Legal Issues

Although many countries have been concerned with the protection and security of information (infrastructures) and related legislation for some years, they have begun to review and adapt their cyber-security legislation only after 9/11. Because national laws are developed autonomously, some countries have preferred to amend their penal or criminal code, whereas others have passed specific laws on cyber-crime.

The following is an overview of important common issues currently discussed in the context of legislation procedures in the countries covered in the handbook:

- Data protection and security in electronic communications (including data transmission, safe data storage, etc.);
- IT security and information security requirements;
- Fraudulent use of computer and computer systems, damage to or forgery of data, and similar offences;
- Protection of personal data and privacy;
- Identification and digital signatures;
- Responsibilities in e-commerce and e-business;
- International harmonization of cyber-crime law;
- Minimum standards of information security for (e-)governments, service providers, and operators, including the implementation of security standards such as BS7799, the code of practice for information security management ISO/IEC 17799, the Common Criteria for Information Technology Security Evaluation ISO/IEC 15408, and others;
- Public key infrastructure and its regulation.

Across all boundaries, there are two main factors that influence and sometimes even hinder efficient law enforcement — one with a national, the other with an international dimension:

- Lack of know-how or of functioning legal institutions: Even if a country has strict laws and prohibits many practices, the enforcement of such laws is often difficult. Frequently, the necessary means to effectively prosecute misdemeanors are lacking due to resource problems, inexistent or emerging cyber-crime units, or a lack of supportive legislation, such as the storing of rendition data.[916]
- Lack or disparity of legal codes: While most crimes, such as theft, burglary, and the like are punishable offenses in almost every country of the world, some rather grave disparities still remain in the area of cyber-crime.[917]

916 Goodman, Seymour E., Pamala B. Hassebroek, Daving Kind, and Andy Azment. "International Coordination to Increase the Security of Critical Network Infrastructures", Document CNI/04. Paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures (Seoul, 20–22 May 2002).

917 Gelbstein, Eduardo and Ahmad Kamal. Information Insecurity. A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security. United Nations ICT Task Force and United Nations Institute for Training and Research (New York, November 2002). http://www.un.int/unitar/patit/dev/old%20site/curriculum/Information_Insecurity_Second_Edition_PDF.pdf.

It has, in fact, been clear for years that the existing state-centric policing and legislative structures are inadequate for regulating international networks. The WSIS declaration of principles and the policy action plan, as well as countless policy papers, repeatedly stress the need for increased international cooperation.[918] Why are international approaches crucial to the successful protection of cyberspace? The answer is rather simple and originates in the fact that like other security issues, the vulnerability of modern societies — caused by dependency on a broad spectrum of highly interdependent information systems — has global origins and implications. Specifically,

- Information infrastructures transcend territorial boundaries, so that information assets vital to the national security and the essential functioning of the economy of one state may reside outside of its sphere of influence, on the territory of other nation-states.
- Malicious actors are willing to contravene national legal frameworks and hide in the relative anonymity of cyberspace.

As a result, any adequate protection policy extending to strategically important information infrastructures will ultimately require transnational solutions. Such a solution may take the form of an international regulatory regime for the protection of cyberspace. However, so far, the international legal framework has remained rather confused and is actually an obstacle to joint action by the actors involved. At the European level, the Council of Europe Convention on Cybercrime and the European Framework Decision on Attacks Against Information Systems are currently among the most important pillars of transnational cyber-security legislation efforts. These issues are further addressed in Vol. II by Subimal Bhattacharjee.

From the National to the Global

A Canadian once said about cyber-security that it was "a Gordian knot around which many stakeholders circle, pulling on the strands that seem most promising

918 World Summit on the Information Society. "Declaration of Principles Building the Information Society: A Global Challenge in the New Millennium". Document WSIS-03/GENEVA/DOC/4-E (12 December 2003). http://www.itu.int/wsis/docs/geneva/official/dop.html.

and causing the entire thing to tighten even more snugly rather than loosen to reveal its internal structure".[919] Even though this quote dates back to 1999, it still rings true today. Cyber-security represents a major conundrum for many actors from a variety of communities, and its inner secrets are far from being revealed. We have aimed to shed some light on the issue by investigating national and international CIIP initiatives that might bring us closer to a global culture of cyber-security. On the one hand, we have found a great many approaches at national level and a great degree of diversity. On the other hand, we have identified some common themes that are of central importance in all countries. The most important of these are early warning approaches, legal issues, public-private partnerships, and the need for international cooperation.

In the majority of countries, the law-enforcement/cyber-crime perspective has emerged as the most prominent one, due to the nature of the threat, the resources that were available to the law enforcement community, and cultural and legal norms, which restrict the number of potential strategies available for selection. Thus, one key issue for all countries is the harmonization of the law to facilitate the prosecution of perpetrators of cyber-crime. The most important legislative instrument in this area is the Council of Europe Cybercrime Convention. Even though the implementation of this convention will likely make us aware of the practical difficulties of such an endeavor, the development of lowest common denominators in this field indicates a global understanding of issues.

In this domain, the basis for a global culture of cyber-security has naturally emerged from a common need on the part of the nation-states: There can be no question that the world-wide scope of the internet demands an international approach, even though each cyber-criminal is a physical entity in a physical location with an internet connection. There is a need for a common understanding of threats and needs, an understanding that can only be fostered if all relevant stakeholders find a common language to address these issues. Equipped with such a common understanding, the many stakeholders will no longer have to pull on the strands that seem most promising, but will be able to systematically untangle those strands that have hitherto kept the community from developing a global culture of cyber-security.

919 Porteous, Holly. "Some Thoughts on Critical Information Infrastructure Protection". In: Canadian IO Bulletin, 2, 4, October 1999. http://www.ewa-canada.com/Papers/IOV2N4.htm.

Appendix

A1 Countries at a Glance

Australia

Past and Present Initiatives and Policies

National Counter-Terrorism Plan (NCTP) (2003)

Organizational Overview

Public Agencies

E-Security Coordination Group (ESCG)
Department of Communications, Information Technology & the Arts (DCITA)
IT Security Expert Advisory Group (ITSEAG)
Communications Sector Infrastructure Assurance Advisory Group (CSIAAG)
Australian Government Information Management Office (AGIMO)
Information Infrastructure Protection Group (IIPG)
Defence Signals Directorate (DSD)
Information Security Group (INFOSEC)
Australian Security Intelligence Organisation (ASIO)
Australian Federal Police (AFP)
Australian High Tech Crime Centre (AHTCC)

Public Private Partnerships

Trusted Information-Sharing Network for Critical Infrastructure Protection (TISN)
Critical Infrastructure Advisory Council (CIAC)
Infrastructure Assurance Advisory Groups (IAAGs)

Early Warning and Public Outreach

Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS)

OnSecure Website
Australian Computer Emergency Response Team (AusCERT)
National Information Technology Alert Service (NITAS)

Law and Legislation
Electronic Transactions Act 1999
Cybercrime Act 2001
Security Legislation Amendment (Terrorism) Act 2002
Spam Act 2003

Austria

Past and Present Initiatives and Policies

Security and Defense Doctrine (2001)
e-Government Program (2000)
IT-Strategy of the Government (2001)
Citizen Card (2003)
ICT Security Sub-Strategy (2005)
Zentrales Ausweichsystem (ZAS) (1980)
Official Austrian Data Security Website

Organizational Overview

Public Agencies

The Austrian Parliament and the Ministries
Chief Information Officer
Ministry of Internal Affairs (BMI)
Center for the Fight against Internet Crime
Federal Agency for State Protection and Counter-Terrorism (BVT)
Ministry for Defence
Ministry for Traffic, Innovation and Technology (BMVIT)
Board of Information and Communication Technology Strategy (ICT-Board)
Government Headquarters for Information and Communication Technology Strategy
IT Security Handbook
Commission on Data Protection (DSK)

Public Private Partnerships

Center for Secure Information Technology Austria (A-SIT)

Early Warning and Public Outreach

Computer Incident Response Coordination Austria (CIRCA)

Law and Legislation

Information Security Law and Information Security Order

Data Security Law
Security Police Law
Military Competence Law
Telecommunication Law
Austrian Penal Code (StGB)
Penal Procedure (StPO)
Electronic Signature Law (SigG) 1999

Canada

Past and Present Initiatives and Policies

Canada's National Security Policy (2004)
National Critical Infrastructure Protection Strategy (underway)
Position Paper on a National Strategy for Critical Infrastructure Protection (2004)
Mitigation and Response Review (underway)
National Disaster Mitigation Strategy (NDMS) (underway)
National Emergency Response System (NERS) (underway)
Government-on-Line (GoL) (2005)
Joint Infrastructure Interdependencies Research Program (JIIRP) (underway)
Information Technology Systems Research and Development Initiative
Information-Sharing

Organizational Overview

Public Agencies

Public Safety and Emergency Preparedness Canada (PSEPC)
Integrated Threat Assessment Centre (ITAC)
Federal Provincial High-Level Forum on Emergencies
Cross-Cultural Roundtable on Security

Public Private Partnership

National Critical Infrastructure Assurance Program (NCIAP)

Early Warning and Public Outreach

Canadian Cyber Incident Response Centre (CCIRC)
Government Operations Centre (GOC)

Law and Legislation

Canadian Criminal Code Sections
The Emergencies Act 1988
The Emergency Preparedness Act 1988
C-78 - Emergency Management Act 2005
The Department of Public Safety and Emergency Preparedness Act 2005

Finland

Past and Present Initiatives and Policies

Governmental Support for the Information Society (1990)
Finland as an Information Society (2000)
Finland in eEurope (2001)
Towards a Networked Finland (2005)
Information Society Programme (2005)
Strategy for Securing the Functions Vital to Society (2003)
Security and Defence Policy (2004)
National Information Security Bodies
Advisory Committee for Information Security (ACIS) (2001)
Information Security Review (2002)
National Information Security Strategy Proposal (2002)
National Information Security Advisory Board (2004–2007)
eFinland

Organizational Overview

Public Agencies

Finnish Communications Regulatory Authority (FICORA)
National Computer Emergency Response Team (CERT-FI)
National Emergency Supply Agency (NESA)
Steering Committee for Data Security in State Administration (VAHTI)

Public Private Partnerships

National Board of Economic Defence (NBED)
Finnish Information Society Development Centre (TIEKE)
Information Society Council

Early Warning and Public Outreach

Computer Emergency Response Team Finland (CERT-FI)

Law and Legislation

Act on the National Board of Economic Defence (NBED) 1960

Emergency Powers Act 1991
Security of Supply Act 1992/2005
Finnish Penal Code
Act on Television and Radio Operations 1998
Act on Provision of Information Society Services 2002
Communications Market Act 2003
Act on the Protection of Privacy in Electronic Communications 2004

France

Past and Present Initiatives and Policies

Government Action Program for an Information Society (PAGSI) (1997)
Expression of the Needs and Identification of Security Objects (EBIOS) (1997)
State Information System Security Reinforcement Plan (2004–2007)

Organizational Overview

Public Agencies

General Secretariat for National Defense (SGDN)
Inter-Ministerial Commission for the Security of Information Systems (CISSI)
Central Directorate for Information Systems Security (DCSSI)
Security of Information Systems (SSI) Website
Information Systems Security Training Center (CFSSI)
Advisory Office
Central Office for the Fight Against Hi-Tech Crime

Public Private Partnerships

Strategic Advisory Board on Information Technologies (CSTI)
French Dependability Institute (ISDF)

Early Warning and Public Outreach

Computer Emergency Response Teams (CERTs)
CERT-RENATER
CERTA
CERT-IST (CERT-Industry, Services, and Tertiary)
CLUSIF (Club de la Sécurité des Systèmes d´Information Français)

Law and Legislation

French Penal Code 2004

Germany

Past and Present Initiatives and Policies

AG KRITIS (1997)
Situational Analysis of Threats and Hazards (2000)
Comprehensive Reports on Threats and Hazards (2001)
Kirchbach Report (2002)
Report on the IT-Security Situation in Germany (2005)
Critical Infrastructure Protection – Baseline Protection Concept (2005)
Infrastructure Analysis Studies (2002)
Campaign for „Security in the Internet" (relaunched 2003)
IT Security Guidelines (2004)
National Plan for Information Infrastructure Protection (NPSI) (2005)
Awareness and Support for the Citizen
Secure E-Government and BundOnline (2005)
e-Government Manual

Organizational Overview

Public Agencies

Federal Ministry of the Interior (BMI)
The Federal Office for Information Security (BSI)
Federal Office for Civil Protection and Disaster Response (BBK)
German Emergency Preparedness Information System (deNIS)
The Federal Criminal Police Agency (BKA)
Federal Ministry of Economics and Technology (BMWi)
Federal Network Agency
Other ministries involved

Public Private Partnership

Initiative D21
Working Group on Infrastructure Protection (AKSIS)

Early Warning and Public Outreach

CERT-Bund
Mcert

CERT-Network
IT Crisis Response Centre

Law and Legislation
Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations
Information and Telecommunications Services Act 1997
Electronic Signature Act 2001/2005
Act on the Utilization of Teleservices
Teleservices Data Protection Act
German Penal Code

India

Past and Present Initiatives and Policies

National Task Force on IT and Software Development (1998)
Information Technology Action Plan (1998)
National e-Governance Plan (NeGP) (2003–2007)
Core Group on Standards for e-Governance

Organizational Overview

Public Agencies

National Information Board (NIB)
National Information Security Coordination Cell (NISCC)
National Security Council Secretariat (NSCS)
Information Infrastructure Protection Centre (IIPC)
Ministry of Communications and Information Technology (MOC): Department of Information Technologies (DIT)
Inter Ministerial Working Groups
Standardisation, Testing and Quality Certification (STQC) Directorate
Information Security Technology Development Council (ISTDC)

Public Private Partnership

Indo-US Cyber Security Forum
Indo-US High Technology Group

Early Warning and Public Outreach

Indian Computer Emergency Response Team (CERT-In)

Law and Legislation

Information Technology Act 2000 (IT Act)
Indian Penal Code

Italy

Past and Present Initiatives and Policies

Action Plan for E-Government (2000)
E-Government for Efficient Federalism (2003)
The Government's Guidelines for the Development of the Information Society (2002)
ICT Security Directive
Report on Critical Information Infrastructure Protection: The Case of Italy (2004)

Organizational Overview

Public Agencies

Working Group on Critical Information Infrastructure Protection
Ministry for Innovation and Technologies (MIT)
Committee of Ministers for the Information Society
Department for Innovation and Technologies (DIT)
National Technical Committee for ICT Security in the Public Administration
National Center for Informatics in the Public Administration (CNIPA)
Ministry of Communication
Institute for Information and Communication Technologies (ISCOM)
National Information Security Certification Body (OCSI)
Permanent Working Group on Network Security and Communications Protection
Postal and Communications Police

Public Private Partnerships

Early Warning and Public Outreach

Italian Computer Emergency Response Team (CERT-IT)
GovCERT.it
GARR-CERT
MoD-CERT

Law and Legislation
Italian Penal Code
Privacy Law

Japan

Past and Present Initiatives and Policies

Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society (1998)
Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure (2000)
Action Plan on Critical Infrastructure (2005)
e-Japan Priority Policy Programme (2001)
e-Japan Strategy II (2003)
Comprehensive Strategy on Information Security (2003)
Action Plan on Critical Infrastructure Information Security Measures (2005)

Organizational Overview

Public Agencies

Interim Committee for Essential Issues on Information Security
IT Strategic Headquarters
IT Security Office
National Information Security Center (NISC)
Information Security Policy Council (ISPC)
Ministry of Economy, Trade and Industry (METI)
Committee of Information Security Governance at METI
National Police Agency (NPA)
Cyber Forces
Ministry of Internal Affairs and Communications (MIC)

Public Private Partnerships

Early Warning and Public Outreach

National Incident Response Team (NIRT)
Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
Asia Pacific Computer Incident (Emergency) Response Team (AP-CIRT/AP-CERT)

Cyber Force
@police
Ministry of Economy, Trade, and Industry (METI)

Law and Legislation
Unauthorized Computer Access Law 1999
Law on Electronic Signatures and Certification Services 2000
Basic Law on Formation of an Advanced Information and Telecommunication Network Society 2001 (IT Basic Law)

Republic of Korea

Past and Present Initiatives and Policies

Report on the Status of the Critical Information Infrastructure (2001)
e-Korea Vision 2006 (Third Master Plan for Informatization Promotion) (2002–2006)
First Master Plan of Informatization Promotion (1996)
Cyber Korea 21 (1999)
Mid to Long-Term Roadmap for Realizing a Safe u-Korea (2005–2008)

Organizational Overview

Public Agencies

National Cyber Security Center (NCSC)
Internet Crime Investigation Center (ICIC)
Korea Information Security Agency (KISA)
Korea Spam Response Center (KSRC)
Korea IT Security Evaluation Center (KISEC)
Information Infrastructure Protection Division
National Security Research Institute (NSRI)
Electronics & Telecommunications Research Institute (ETRI)
Telecommunication Infrastructure Protection Committee

Public Private Partnerships

National Information Security Alliance (NISA)
Financial Information Security Alliance
Information Security Practice Alliance
Korea Information Security Industry Association (KISIA)

Early Warning and Public Outreach

National Cyber Security Center (NCSC)
Korea Internet Security Center (KISC, KrCERT/CC)
Information Sharing & Analysis Centre (ISAC)

Law and Legislation

Information Security Promotion Systems

National Cyber Security Management Regulation 2005
National Information Infrastructure Protection Act 2001
E-Signature and Certification
Protection of Telecommunication Networks and Information Systems
Cyber Attacks

Malaysia

Past and Present Initiatives and Policies

National IT Agenda (NITA) (1996)
National Information Technology Council (NITC) Strategic Agenda
e-Secure Malaysia 2005 International Conference
National Information Security Policy (2006)

Organizational Overview

Public Agencies

Malaysian Communications and Multimedia Commission (MCMC)
Malaysian Administrative Modernization and Management Planning Unit (MAMPU)
Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)
Government Computer Emergency Response Team (GCERT)
ICT Strategic Plan
Royal Malaysia Police
Technology Crime Investigation Unit
Forensic Computer Laboratory
Ministry of Science, Technology and Innovation (MOSTI)
National Information Security Week
ICT Policy Division
Ministry of Energy, Water and Communications (MECM)

Public Private Partnerships

Information Sharing Forum (ISF)

Early Warning and Public Outreach

National ICT Security and Emergency Response Center (NISER)
Malaysian Computer Emergency Response Team (MyCERT)

Law and Legislation

Computer Crimes Act 1997
Communications and Multimedia Act (CMA) 1998

The Netherlands

Past and Present Initiatives and Policies

The Digital Delta (1999)
Defense Whitepaper (2000)
Infodrome Initiative and BITBREUK (2000)
KWINT-Manifest (2001)
KWINT Report and Memorandum (2001)
Vulnerability of the Internet (2001)
Platform Electronic Commerce in the Netherlands (ECP.NL)
KWINT Program (2002–2005)
Veilige Elektronische Communicatie (VEC) (2006–2008)
Quick Scan on Critical Products and Services (2002)
Anti-Terrorism Plan
Protection of the Dutch Critical Infrastructure (2002–2004)
Critical Infrastructure Strategic Consultation Group (SOVI) (2005)

Organizational Overview

Public Agencies

Ministry of the Interior and Kingdom Relations
Ministry of Economic Affairs (EZ)
Directorate-General for Energy and Telecommunications
General Intelligence and Security Service (AIVD)
National High Tech Crime Center (NHTCC)

Public-Private Partnerships

Platform Electronic Commerce in the Netherlands (ECP.NL)
National Continuity Plan for Telecommunications (NACOTEL)
National Continuity Consultation Platform Telecommunications (NCO-T)

Early Warning and Public Outreach

CERT-NL (part of SURFnet)
GOVCERT.NL

Hacking Emergency Response Team (HERT) and National High-Tech Crime Centre

Law and Legislation
Computer Crime Laws 1999
Telecommunications Law
Dutch Criminal Code

New Zealand

Past and Present Initiatives and Policies

CIIP within the Defence Policy Framework (2000)
Report on Protecting New Zealand's Infrastructure from Cyber-Threats (2000)
Towards a Centre for Critical Infrastructure Protection (CCIP) (2001)
Manual on Security in the Government Sector (2002)
Security Policy and Guidance Website
Standards New Zealand (SNZ)

Organizational Overview

Public Agencies

Domestic and External Secretariat (DESS)
Officials Committee for Domestic and External Security Co-ordination (ODESC)
Interdepartmental Committee on Security (ICS)
Centre for Critical Infrastructure Protection (CCIP)
Government Communications Security Bureau (GCSB)
NZ Government Information Technology Security Manual NZSIT 400
E-Government Unit

Public Private Partnerships

New Zealand Security Association (NZSA)
Computer Society's Special Interest Group on Security (NZCS SigSec)

Early Warning and Public Outreach

AusCERT

Law and Legislation

Crimes Amendment Act 2003: Crime involving computers

Norway

Past and Present Initiatives and Policies

Defense Review 2000
Defense Policy Commission 2000
Commission on a Vulnerable Society (1999–2000)
Green Paper on NOU (2000:24) — A Vulnerable Society (2000)
ICT Vulnerability Project (1999)
eNorway (eNorge) 2005 Action Plan (2002)
Safety and Security of Society (2002)
National Strategy for Information Security (2003)

Organizational Overview

Public Agencies

Directorate for Civil Protection and Emergency Planning (DSB)
Norwegian National Security Authority (NSM)
National Information Security Co-ordination Council (KIS)
Commission for the Protection of Critical Infrastructures in Norway

Public Private Partnerships

Center for Information Security (SIS)
Warning System for Digital Infrastructure (VDI)

Early Warning and Public Outreach

UNINETT CERT

Law and Legislation

Norwegian Penal Code

Russia

Past and Present Initiatives and Policies

Information Security Doctrine of the Russian Federation (2000)
National Security Concept
Program Electronic Russia (2002–2010)
Electronic Moscow (2002)
International Cooperation

Organizational Overview

Public Agencies

Security Council of the Russian Federation
Federal Security Service of the Russian Federation (FSB)
Computer and Information Security Directorate
Federal Guard Service of the Russian Federation
Special Communication and Information Service
Federal Agency for Government Communications and Information (FAPSI)
Federal Technical and Export Control Service
Ministry of Information Technologies and Communications

Public Private Partnerships

Russian Association of Networks and Services (RANS)
PRIOR
Russian Development Gateway

Early Warning and Public Outreach

Russian Computer Emergency Response Team (RU-CERT)
Russian Institute of Public Networks (RIPN)
Russian Backbone Network (RBNet)

Law and Legislation

Electronic Digital Signature (EDS) Law
Russian Criminal Code 1996/2004
Draft Information Security Act

Singapore

Past and Present Initiatives and Policies

National Emergency System (NEST)
National Critical Infrastructure Assurance (NCIA) (2002)
Singapore's National Security Strategy (2004)
Infocomm Security Masterplan (2005–2007)
National Authentication Infrastructure
Business Continuity Readiness Assessment Framework
National Cyber-Threat Monitoring Centre (NCMC)
Vulnerability Study of National Critical Infrastructures

Organizational Overview

Public Agencies

Infocomm Development Authority of Singapore (IDA)
Ministry of Information, Communications and the Arts (MICA)
Infocomm Security Division (iSec)
National Infocomm Security Committee (NISC)
Technology Crime Division (TCD) / Singapore Police Force
Criminal Investigation Department (CID)

Public Private Partnerships

National Infocomm Competency Centre (NICC)
Information Technology Standards Committee (ITSC)
Governmentware IT Security Seminar Series

Early Warning and Public Outreach

Singapore Computer Emergency Response Team (SingCERT)
Asia Pacific Security Incident Response Coordination Working Group (APSIRC-WG)
National Cyberthreat Monitoring Centre (NCMC)

Law and Legislation

Computer Misuse Act (CMA) 1993/1998
Computer Misuse (Amendment) Act 2003
Electronic Transactions Act 1998

Sweden

Past and Present Initiatives and Policies

Commission on Vulnerability and Security (1999–2001)
Bill on Swedish Security and Preparedness Policy (2002)
Committee on Information Assurance in the Swedish Society (2002 –2006)

Organizational Overview

Public Agencies

Ministry of Defense
Swedish Emergency Management Agency (SEMA)
Information Assurance and Analysis Department
Committee on Joint Radio Communication for Public Safety and Security
SEMA/Information Assurance Council
Cabinet Office Working Group on Information Operations
Swedish Defense Materiel Administration (FMV) & the Certification Body for IT Security (CSEC)
Swedish National Defense Radio Establishment (FRA)/The Information Security Technical Support Team
Swedish Armed Forces
Center for Asymmetric Threat Studies (CATS)
The Swedish Defense Research Agency (FOI)
Critical Infrastructure Studies Unit (CISU)
Ministry of Industry, Employment, and Communications
Swedish National Post and Telecom Agency (PTS)
Department of Network Security
Department of Justice
Swedish National Police Board (NPB)
Swedish Security Service (SÄPO)

Public Private Partnership

Swedish Emergency Management Agency (SEMA)
Industry Security Delegation (NSD)

Swedish Information Processing Society (DFS)

Early Warning and Public Outreach
The Swedish IT Incident Centre (SITIC)

Law and Legislation
Swedish Penal Code 1962
Personal Data Act 1998
Electronic Communications Act 2003

Switzerland

Past and Present Initiatives and Policies

Strategic Leadership Exercise (1997)
Strategy for the Information Society Switzerland (1998)
Security Policy Report (2000)
Concept of Information Assurance (2000)
Exercise INFORMO (2001)
Information Assurance Policy (2002)
Risk Analysis InfoSurance Foundation (2002)
Risk Analysis Federal Office for National Economic Supply (2004)

Organizational Overview

Public Agencies

Federal Strategy Unit for Information Technology (ISB)
Special Task Force on Information Assurance (SONIA)
Reporting and Analysis Center (MELANI)
Federal Office for Communication (OFCOM)
Federal Office for National Economic Supply (NES)
ICT Infrastructure Unit
Federal Office of IT, Systems and Telecommunication (FOITT)
Coordination Unit for Cybercrime Control (CYCO)
Federal Department of Defense, Civil Protection, and Sports (DDPS)

Public Private Partnerships

InfoSurance Association
Federal Office for National Economic Supply (NES): ICT Infrastructure Unit (ICT-I)
CLUSIS

Early Warning and Public Outreach

Reporting and Analysis Center (MELANI)
Special Task Force on Information Assurance (SONIA)
Computer Emergency Response Team SWITCH-CERT

Law and Legislation

Swiss Penal Code

United Kingdom

Past and Present Initiatives and Policies

e-commerce@its.best.uk (1999)
Competitiveness White Paper (1998)
UK Online Strategy
Progress Report on Electronic Security (2003)
CIIP Policy Guidelines
Information Assurance Governance Framework – Working in partnership for a secure and resilient UK information infrastructure (2005)

Organizational Overview

Public Agencies

Home Secretary
National Infrastructure Security Co-ordination Centre (NISCC)
Cabinet Office
Civil Contingencies Secretariat (CCS)
Central Sponsor for Information Assurance (CSIA)
Communications Electronics Security Group (CESG)
Government Communications Headquarters (GCHQ)
Department of Trade and Industry (DTI)
Home Office
Ministry of Defence (MoD)
Police
National High Tech Crime Unit (NHTCU)
Security Service
Security Service's National Security Advice Centre (NSAC)
Central Sponsor for Information Assurance (CSIA)
Civil Contingencies Secretariat (CCS)
Emergency Planning College

Public Private Partnerships

NISCC's Public-Private Partnerships
Warning, Advice, and Reporting Points (WARPs)

Information Assurance Advisory Council (IAAC)

Early Warning and Public Outreach
Unified Incident Reporting and Alert Scheme (UNIRAS)
Ministry of Defence Computer Emergency Response Team (MODCERT)
ITsafe: IT Security Awareness for Everyone
GetSafeOnline

Law and Legislation
Telecommunications (Fraud) Act 1997
Data Protection Act 1998
Electronic Communications Bill 2000
Terrorism Act 2000
Computer Misuse Act 1990
Police and Justice Bill 2006

United States

Past and Present Initiatives and Policies

Presidential Commission on Critical Infrastructure Protection (PCCIP) (1996)
Presidential Decision Directives (PDD) 62 and 63 (1998)
National Plan for Information Systems Protection (2000)
Homeland Security Executive Orders (2001)
Homeland Security Presidential Directive/HSPD-7 (2003)
National Strategies
National Strategy for Homeland Security (2002)
National Strategy to Secure Cyberspace (2003)
The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003)
National Infrastructure Protection Plan (NIPP) (2005/2006)

Organizational Overview

Public Agencies

Early Days
Critical Infrastructure Assurance Office (CIAO)
National Infrastructure Protection Center (NIPC)
Department of Homeland Security (DHS)
Directorate for Information Analysis and Infrastructure Protection (IAIP)
Homeland Security Council
US Department of State
International CIP Interagency Working Group
Congressional Focus
House Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity
Government Accountability Office (GAO)
Defense Community
Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD/NII)
Computer Crime and Intellectual Property Section (CCIPS)

Public Private Partnerships

Office of Private Sector, Department of Homeland Security
Information Sharing and Analysis Centers (ISACs)
InfraGard
National Cyber Security Alliance (NCSA)
Partnership for Critical Infrastructure Security (PCIS)
Cyber Incident Detection Analysis Centre (CIDDAC)
National Cyber Security Partnership (NCSP)
Institute for Information Infrastructure Protection (I3P)

Early Warning and Public Outreach

Federal Bureau of Investigation (FBI)
Directorate for Information Analysis and Infrastructure Protection (IAIP)
National Cyber Security Division (NCSD)
National Cyber Alert System
Federal Computer Incident Response Center (FedCIRC)
CERT Coordination Center (CERT/CC), Carnegie Mellon University
US-CERT
Internet Security Alliance
Information Sharing and Analysis Centers (ISACs)
OnGuardOnline.gov

Law and Legislation

Federal Advisory Committee Act (FACA) 1972
Computer Fraud and Abuse Act (CFAA) 1986
Homeland Security Act 2002
Critical Infrastructure Information Act: Procedures for Handling Critical Infrastructure Information
Freedom of Information Act (FOIA)
Terrorism Risk Insurance Act 2002

European Union (EU)

Initiatives and Policies
Critical Infrastructure Protection in the Fight Against Terrorism (2004)
Green Paper on a European Programme for CIP (EPCIP) (2005)
Critical Infrastructure Warning Information Network (CIWIN)
European Network and Information Security Agency (ENISA)

Research & Development
Information Society Technologies (IST) FP6 and FP7
European Security Research Programme (ESRP)
Critical Information Infrastructure Research Co-ordination (CI2RCO)

Law and Legislation
Data Protection Directive 1995
Directive on Electronic Signature 1999
Directive on Privacy Protection in the Electronic Communications Sector 2002
Framework Directive 2002
Council Framework Decision on Attacks Against Information Systems 2005
Directive on Data Retention 2005

Group of Eight (G8)

G8 Senior Expert Group; Lyon/Roma Group
Okinawa Charter on Global Information Society (2000)
G8 Principles for Protecting Critical Information Infrastructures (2003)
Council of Europe Cybercrime Convention (2001)
Best Practices for Network Security, Incident Response and Reporting to Law Enforcement (2004)
High-Tech Crime Sub-Group Activities
International CIIP Directory
Communiqué on CIIP

North Atlantic Treaty Organisation (NATO)

Senior Civil Emergency Planning Committee (SCEPC)
Planning Boards and Committees (PB&Cs)
Civil Communication Planning Committee (CCPC)
North Atlantic Council's Action Plan on Cyber Defense
Civil Protection Committee (CPC)
Ad Hoc Group on Critical Infrastructure Protection (AHG on CIP)
Industrial Planning Committee (IPC)
Food and Agriculture Planning Committee (FAPC)
Civil Aviation Planning Committee (CAPC)
Planning Board for Inland Surface Transportation (PBIST)
Planning Board for Ocean Shipping (PBOS)

Organisation for Economic Co-operation and Development (OECD)

Working Party on Information Security and Privacy (WPISP)
Committee for Information, Computers and Communications Policy (ICCP)
OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002)
"Culture of Security" Website (2003)
OECD Forums and Workshops

United Nations (UN)

UN Institute for Disarmament Research (UNIDIR) Workshop (1999)
UN General Assembly Resolutions
Combating the criminal misuse of information technologies (2000/2001)
Creation of a global culture of cybersecurity (2002)
Creation of a global culture of cybersecurity and the protection of critical information infrastructure (2003)
UN ICT Task Force
UN and the World Summit on the Information Society (WSIS) (2003; 2005)
International Telecommunication Union (ITU)
ITU WSIS Thematic Meeting on Cybersecurity (2005)
World Communication Day

The World Bank Group

Global Information and Communication Technologies Department (GICT)
Information Technology Security Handbook
Information for Development Program (infoDev)
Technology Risk Checklist

A2 Bibliography

Australia

Attorney-General's Department. Protecting Australia's National Information Infrastructure. Report of the Interdepartmental Committee on Protection of the National Information Infrastructure (Canberra, December 1998).

Australian Government. Protecting Australia against Terrorism. http://www.pmc.gov.au/publications/protecting_australia/docs/protecting_australia.pdf.

Commonwealth Department of Communications, Information Technology and the Arts (DOCITA). E-Commerce beyond 2000 (Canberra, 2000). http://www.iwar.org.uk/e-commerce/resources/au/beyond2k_final_report.pdf.

Commonwealth Department of Communications, Information Technology and the Arts (DOCITA). A Strategic Framework for the Information Economy. Identifying Priorities for Action (Canberra, December 1998).

Commonwealth of Australia, Information Security Group. Australian Communications-Electronic Security Instruction 33 (ACSI 33).

Etter, Barbara. "The Australasian Policing Response to Electronic Crime". Australasian Centre for Policing Research to the FBI Global Economic Threats Conference (FBI Academy, Quantico, Virginia (USA), July 9–13 2001).

KPMG/National Support Staff. Critical Infrastructure Project. Phase 2. Information Technology Report. Predict Defence Infrastructure Core Requirements Tool (PreDICT) (April 2000).

National Counter-Terrorism Plan (2nd ed.), September 2005 (Commonwealth of Australia, 2005). http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/(5738DF09EBC4B7EAE52BF217B46ED3DA)~NCTP_Sept_2005.pdf/$file/NCTP_Sept_2005.pdf.

Rathmell, Andrew. Trip Note, Australian Business-Government Task Force on Critical Infrastructure, (26–27 March 2002).

Austria

Bundesheerreformkommission. Endbericht (Vienna, 2004).

Hollosi, Arno. Sicherheit mit offenen Standards für die Verwaltung (Vienna 2002).

Pankratz, Thomas. "Information warfare - Eine Bedrohung der wired society". In: Gärtner, Heinz and Höll, Otmar. Comprehensive Security (Vienna 2001).

Resolution by the Austrian Parliament. Security and Defence Doctrine: Analysis. Draft expert report of 23 January 2001.

Stabsstelle IKT-Strategie des Bundes. Österreichisches IT-Sicherheitshandbuch (Mai 2003). http://www.cio.gv.at/securenetworks/sihb.

Unger, Walter J. and Heinz Vetschera. "Cyber War und Cyber Terrorismus als neue Formen des Krieges". In: Österreichische Militärische Zeitschrift, No. 2 (2005).

Unger, Walter J. "Angriff aus dem Cyberspace I-III". In: Truppendienst No. 2 (2004), pp. 143–147; No.3 (2004), pp. 271–5; No. 4 (2004).

Zivilschutz aktuell, No. 4 (1999), p. 13- 19.

Canada

Canada, Privy Council Office. Securing an Open Society: Canada's National Security Policy (April 2004). http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf.

Canadian Security Intelligence Service (CSIS). Protection of the Canadian Critical Infrastructure (17 July 2001).

Charters, David. The Future of Canada's Security and Defence Policy: Critical Infrastructure Protection and DND Policy and Strategy. Research Paper of the Council for Canadian Security in the 21st Century.

Dependability Development Support Initiative (DDSI). Global Overview - Countries, International and Inter-Governmental Organisations (Version April 2002).

Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection (November 2004). http://www.ocipep.gc.ca/critical/nciap/positionpap_e.asp.

Grenier, Jacques. "The Challenge of CIP Interdependencies". Conference on the Future of European Crisis Management (Uppsala, Sweden, 19–21 March 2001).

Harlick, J.E. "Understanding Critical Infrastructure Protection". Presentation at the PfP Seminar on Critical Infrastructure Protection and Civil Emergency Planning — New Concepts for the 21st Century (Stockholm, 17–18 November 2003).

National Contingency Planning Group. Canadian Infrastructures and their Dependencies (March 2000).

"National Critical Infrastructure Protection Program". In: Memo Quarterly Newsletter (Yukon Government and Emergency Preparedness Canada, Vol. 7, Winter 2001).

ÖCB (ed.). International CEP Handbook: Civil Emergency Planning in the NATO/EACP Countries 1999–2000 (Stockholm, 2000).

Purdy, Margaret. Cyber-Sabotage for Government. Speech at the Ottawa Congress Centre (Ottawa, 20 February, 2001).

Finland

Act on the Protection of Privacy in Electronic Communications (516/2004). http://www.mintc.fi/www/sivut/dokumentit/viestinta/tieto/Sahköisen_viestinnan_tietosuojalaki_20041213_en.pdf.

Dependability Development Support Initiative (DDSI). European Dependability Policy Environments, Country Report Finland (Version April 2002).

Finnish Communications Regulatory Authority (FICORA). Annual Report 2004.

Finnish Communications Regulatory Authority (FICORA). Information Security Review related to the National Information Security Strategy (May 2002). http://www.ficora.fi/englanti/document/review.pdf.

Hagman, Rauni. "Finnish Communications Regulatory Authority (FICORA). ICT Security — Finland's Strategy and Action Plan". International Northern eDimension Forum (Pori, 11–12 November 2002). http://www.pori.fi/ned2002/esitykset/hagman_p.pdf.

Information Society Advisory Board. Finland as an Information Society. Report of the Information Society Advisory Board to the Government (Helsinki 2000).

Ministry of Defence. Finnish Security and Defence Policy 2001. Report by the Government to Parliament on 13 June 2001.

Ministry of Transport and Communications. Finland in eEurope. Summary (March 2001).

National Information Security Advisory Board. Creating a Safer Information Society (2004). http://www.mintc.fi/oliver/upl501-NISAB%20report%20(lowres).pdf.

Proposal of the Advisory Committee for Information Security. National Information Security Strategy Proposal (25 November 2002). http://www.ficora.fi/englanti/document/infos.pdf.

The Amendment of the Security of Supply Act (688/2005). http://www.finlex.fi/fi/esitykset/he/2005/20050044.

The Finnish Governmen. Finnish Security and Defence Policy (2004). http://www.defmin.fi/chapter_images/2574_2160_English_White_paper_2004%5B1%5D.pdf.

The Finnish Government. Information Society Programme (April 2005). http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/11233297000000607/default/tietoyhteiskuntaojelma_en_2005.pdf.

The Information Society Council. Towards a Networked Finland (February 2005). http://www.tietoyhteiskuntaohjelma.fi/tietoyhteiskuntaneuvosto/en_GB/information_society_council/_files/11233297000012864/default/TietoYnRap-Eng-7-6-05.pdf.

France

Dependability Development Support Initiative (DDSI). European Dependability Policy Environments, Country Report France (September 2002).

Haut Comité Francais pour la Défense Civile. Livre Blanc HCFDC: 20 ans, 20 constats et propositions (2003).

Premier Ministre, Service Central de la Sécurité des Systèmes d'Information. Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS). Technical Guide - English Version, Version 1.02 (February 1997).

Présentation des nouvelles orientations de l'Etat en sécurité des systèmes d'information. Séminaire DCSSI-AFNOR, 27 March 2003. http://www.ssi.gouv.fr/fr/actualites/afnor-dcssi-270303/pdf/AFNOR270303.pdf.

Prime Minister's Office. State Information System Security Reinforcement Plan (2004–2007) (10 March 2004). http://www.ssi.gouv.fr/site_documents/PRSSI/PRSSI-en.pdf.

Service d'Information du Gouvernement. Four years of Government measures to promote the information society (August 2001).

Germany

Act on the Protection of Personal Data Used in Teleservices (Teleservices Data Protection Act – Teledienstedatenschutzgesetz, TDDSG) (22 July, 1997, amended last by Article 3 of the Bill on Legal Framework Conditions for Electronic Commerce).

Act on the Utilization of Teleservices (Teleservices Act – Teledienstegesetz TDG) (22 July, 1997, amended last by Article 1 of the Bill on Legal Framework Conditions for Electronic Commerce).

AG KRITIS. Informationstechnische Bedrohungen für Kritische Infrastrukturen in Deutschland. Kurzbericht der Ressortarbeitsgruppe KRITIS (Entwurfsversion 7.95, Dezember 1999).

Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung. Flutkatastrophe 2002 (2nd Edition 2003).

Blattner-Zimmermann, Marit. „Kritische Infrastrukturen im Zeitalter der Informationstechnik". Seminar on Information Warfare (Lucerne, 22 November 2001).

Bundesministerium des Innern. Schutz Kritischer Infrastrukturen – Basisschutzkonzept (Berlin, August 2005). http://www.bmi.bund.de/cln_012/nn_122052/Internet/Content/Common/Anlagen/Broschueren/2005/

Basiskonzept__kritische__Infrastrukturen,templateId=raw,property=publicationFile.pdf/Basiskonzept_kritische_Infrastrukturen.

Bundesministerium des Innern. Co-ordination and Advisory Board of the Federal Government for Information Technology (KBSt). Berlin-Bonn Information Network (IVBB) (November 2002). http://www.kbst.bund.de/Anlage303608/pdf_datei.pdf.

Bundesministerium des Innern. Zweiter Gefährdungsbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bevölkerung bei Grosskatastrophen und im Verteidigungsfall (Berlin, October 2001).

Bundesministerium für Bildung und Forschung. „Online – Offline: IT in Education". Innovationen Wissensgesellschaft (August 2000).

Dependability Development Support Initiative (DDSI). European Dependability Policy Environments, Country Report Germany (Version April 2002).

Ennen, Günther. „CERT-Bund – eine neue Aufgabe des BSI". In: KES Zeitschrift für Kommunikations- und EDV-Sicherheit. Bundesamt für Sicherheit in der Informationstechnik (BSI) (Bonn, June 2001), pp. 35–41.

Federal Office for Information Security (BSI). IT Security Guidelines: IT Baseline Protection in brief (Bonn: 2004). http://www.bsi.bund.de/english/gshb/guidelines/guidelines.pdf.

Federal Office for Information Security (BSI). The IT Security Situation in Germany in 2005 (2005). http://www.bsi.de/english/publications/securitysituation/lagebericht2005_englisch.pdf.

Fischer, Wolfgang, Brigitta Krüger, Niels Lepperhoff, and Regina Eich. Was treibt die Entwicklung des Internet voran? Programmgruppe Systemforschung und Technologische Entwicklung (STE) (Jülich, August 2001).

Hutter, Reinhard. „Cyber-Terror: Risiken im Informationszeitalter". In: Aus Politik und Zeitgeschichte Vol. 10/11 (2002), pp. 31–39.

Kühn, Klaus Dieter. „Katastrophenresistente Infrastrukturen". In: Bevölkerungsschutz Vol. 4 (2001), pp. 46–47.

Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations. Bundesgesetzblatt (Part 1, 21 May 2001) (Unofficial version for industry consultation).

Möhring, Michael. Informationsgesellschaft (Universität Koblenz-Landau: Institut für Wirtschafts- und Verwaltungsinformatik, 2001).

Welzel, Carolin. "Vom Kalten Krieg zum Cyberwar: eBusiness, eGovernment — eWar?". In: politik-digital (19 April 2001).

Zentralstelle für Zivilschutz. Leistungspotenziale im Zivilschutz. Deutsches Notfallvorsorge-Informationssystem (Februar 2003). http://www.denis.bund.de/imperia/md/content/intern/1.pdf.

India

Chandrashekhar, Shri R. Presentation "On The National E-Governance Plan — Approach & Key Components". National e Governance Plan – Workshop with States and UTs, (New Delhi, 11–12 March 2005). http://www.mit.gov.in/plan/cmmp.asp.

Department of Information Technology. Annual report 2004–2005 (no date). http://www.mit.gov.in/annualreport2004-05.zip.

Mishra, Vineeta. "Critical sectors to be Y2K ready in time: govt report". In: India Times, 19 October 1999. http://www.apnic.net/mailing-lists/s-asia-it/archive/1999/10/msg00050.html.

National Task Force on Information Technology and Software Development. Information Technology Action Plan, Preamble (4 July 1998). http://it-taskforce.nic.in/prem.htm.

Saini, Mukesh. Presentation at the Indo-US Cyber-Security Forum in Washington, DC, 9–10 November 2004.

Italy

Dependability Development Support Initiative (DDSI). Dependability Overview: National Dependability Policy Environments (2002).

Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche Informatizzate. Protezione delle Infrastrutture Critiche Informatizzate — La realtà Italiana (Ottobre 2003).

Minister for Innovation and Technologies. The Government's guidelines for the development of the Information Society (June 2002).

Ministero per l'innovazione e le tecnologie. Le politiche governative in tema sicurezza (no date).

Japan

Basic Law on the Formation of an Advanced Information and Telecommunications Network Society. http://www.kantei.go.jp/foreign/it/it_basiclaw/it_basiclaw.html.

Comprehensive Strategy on Information Security: Executive Summary. Chapter 1.2 New Dimensions of Risks Confronting Society as a Whole. http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf.

E-Japan Priority Policy Program (29 March 2001). http://www.kantei.go.jp/foreign/it/network/priority-all/1.html.

Hayami, Yutaka. "Realizing a World-Class 'Highly Reliable Society'". Presentation held on 25 November 2004. http://www.aavar.org/2004web/AVAR2004/Presentations/ps011.ppt.

Information Security Policy Council (ISPC). Action Plan on Critical Infrastructure (13 December 2005).

IT Strategic Headquarters. e-Japan 2002 Program. Basic Guidelines Concerning the IT Priority Policies in FY2002 (26 June 2001). http://www.kantei.go.jp/foreign/it/network/0626_e.html.

Law Concerning Electronic Signatures and Certification Services (unofficial translation). http://www.soumu.go.jp/joho_tsusin/eng/Resources/Legislation/eSignLaw/eSignLaw.pdf.

Ministry of Internal Affairs and Communications. Information and Communications in Japan. Stirring of u-Japan.White Paper 2005. http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2005/2005-index.html.

Outline of the First Follow-up of the Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society (19 May 2000) (provisional translation). http://www.kantei.go.jp/foreign/it/2000/0706outline.html.

Shimizu, Mika. "Governance for a New Security Issue: Cyber Security in Critical Infrastructure Protection." Prepared for the 2004 Annual Meeting of the American Political Science Association (2–5 September 2004).

Special Action Plan on Countermeasures to Cyber-terrorism of critical infrastructure (15 December 2000) (provisional translation). http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN009986.pdf.

Special Action Plan on Countermeasures to Cyber-terrorism of Critical Infrastructure (Summary, 15 December 2000) (provisional translation). http://www.kantei.go.jp/foreign/it/security/2001/cyber_terror_sum.html.

Yoshida, Mabito. "Information Security Policies in Japan". Presentation held at the ITU WSIS Thematic Meeting on Cybersecurity (Geneva, 28 June – 1 July 2005). http://www.itu.int/osg/spu/cybersecurity/presentations/session7_yoshida.pdf.

Republic of Korea

Korean Information Security Agency (KISA). Report on the status of the Critical Information Infrastructure (12 January 2001).

Lim, Chaeho. Creating Trust in Critical Network Infrastructures: Korean Case Study (20 May 2002) (slides). http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.14.pdf.

Lim, Chaeho. Creating Trust in Critical Network Infrastructures: Korean Case Study. Paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures (Seoul, Republic of Korea, 20–22 May 2002). http://www.itu.int/osg/spu/ni/security/docs/cni.05.doc.

Ministry of Information and Communication. e-Korea Vision 2006: The Third Master Plan for Informatization Promotion 2002–2006 (April 2002).

Yang-Shin, Cha. Korea's Approach to Network Security (21 Mai 2002). http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.21.pdf.

Malaysia

Anti-Spam Activities in Malaysia — Current Situation: Regulatory Environment and Future Developments. Presentation held at the ITU Global Symposium for Regulators (Geneva 8–10 December 2004) (no name). http://www.itu.int/ITU-D/treg/Events/Seminars/2004/GSR04/documents/NurAbdullah.pdf.

Bistamam Siru Abdul Rahman. Malaysia's Approach to Network Security. Presentation held at ITU Workshop on "Creating Trust in Critical Network Infrastructures", (Seoul, May 2002). http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.19.pdf.

Malaysia Communications and Multimedia Act 1998. http://www.mcmc.gov.my/mcmc/the_law/ViewAct.asp?cc=4446055&lg=e&arid=900722.

Malaysian Administrative Modernisation and Management Planning Unit, Prime Minister's Department (MAMPU). Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMis) (January 2002). http://www.mampu.gov.my/mampu/bm/program/ict/mymis/mymis.htm.

Sani, Rozana. Safeguarding Critical Data. Government agencies need to carry out close scrutiny on their operational (Malaysia, February 2005).

The Netherlands

De Bruin, Ronald. „From Research to Practice: A Public-Private Partnership Approach in the Netherlands on Information Infrastructure Dependability". In: Dependability Development Support Initiative (DDSI) Workshop (28 February, 2002).

Dutch Ministry of Transport, Public Works and Water Management; Dutch Ministry of Economic Affairs. Internet Vulnerability (July 2001).

Infodrome. De Overheid in de Informatiesamenleving: Mission September 1999 (September 1999).

Luiijf, Eric, M. Klaver and J. Huizenga. The Vulnerable Internet: A Study of the Critical Infrastructure of (the Netherlands Section of) the Internet (The Hague, 2001).

Luiijf, Eric, M. Klaver. In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society (Translation of he Dutch Infodrome essay „BITBREUK", de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij) (Amsterdam, March 2000).

Luiijf, Eric. „Critical Info-Infrastructure Protection in the Netherlands". ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead (Zurich, 8–10 November 2001).

Luiijf, Eric. „Information Assurance and the Information Society". In: Gattiker, Urs E., Pia Pedersen and Karsten Petersen (Eds.). EICAR 1999 Best Paper Proceedings (Aalborg, 1999).

Luiijf, Eric. „Information Assurance under Fire". Information Assurance and Data Security, SMI Conference (London, 2–3 February 2000).

Luiijf, Eric. „Netherlands Defense Information Operations Policy". Seminar on Information Warfare (Lucerne, 22 November 2001).

Ministerie van Defensie, Defensienota 2000 (1999).

Stratix / TNO-FEL. The Reliability of the Netherlands Internet: Consequences and Measures. Report of Project Phase 3: Review of International Activities and Possible Actions (English translation of "De Betrouwbaarheid van het Internet: Gevolgen en Maatregelen. Project KWINT – Rapportage Fase 3 (17 October 2000, Version 2.2).

New Zealand

Cabinet Paper. Centre for Critical Infrastructure Protection (13 August 2001). http://www.ccip.govt.nz/about-ccip/cabinet-paper.htm.

Department of the Prime Minister and Cabinet. Security in the Government Sector (2002). http://www.security.govt.nz/sigs/index.html.

Domestic and External Security Secretariat. Securing our Nation's Safety: How New Zealand manages its security and intelligence agencies (December 2000).

E-Government Unit, State Services Commission. Protecting New Zealand's Infrastructure from Cyber-Threats (8 December 2000). http://www.ccip.govt.nz/about-ccip/niip-report-final.htm.

E-Government Unit, State Services Commission. Towards a Centre for Critical Infrastructure Protection (11 June 2001). http://www.ccip.govt.nz/about-ccip/ccip-final-report.htm.

Minister of Defence. The Government's Defence Policy Framework (June 2000). http://www.executive.govt.nz/minister/burton/defence/index.html.

Norway

Dagfinn Buset. "Civil Protection in Norway". Presentation held at the Workshop on Critical Infrastructure Protection and Civil Emergency Planning: Dependable Structures, Cybersecurity, and Common Standards (Zurich, 9–11 September 2004). http://www.eda.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/cybsec/buset.html.

Dependability Development Support Initiative (DDSI). European Dependability Policy Environments, Country Report Norway (Version April 2002).

Dependability Development Support Initiative (DDSI). Public-Private Co-operation: Business Governmental Actions Towards Achieving a Dependable Information Infrastructure in Europe. Issues and background paper for the DDSI workshop on Public-Private Co-operation (Stockholm, 6–7 June 2002).

Hagen, Janne Merete and Håvard Fridheim. "Cost-Effectiveness Analysis of Measures to Reduce Vulnerabilities in the Public Telecommunication System". Paper presented at the 16 ISMOR, The Royal Military College of Science, Norwegian Defence Research Establishment (United Kingdom, 1–3 September 1999).

Henriksen, Stein. "National Approaches to CIP Norway". ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead (Zurich, 8–10 November 2001).

Hovden, Jan. Public Policy and Administration in a Vulnerable Society (Norwegian University of Science and Technology and the Norwegian Academy of Science and Letter, Centre for Advanced Study, June 2001). http://www.delft2001.tudelft.nl/paper%20files/paper1074.doc.

Jervas, Gunnar, Ian Dennis and Richard Conroy (eds.). New Technology as a Threat and Risk Generator. Can Countermeasures Keep up with the Pace? (Stockholm, March 2001).

Krohn Devold, Kristin. The Government's Defence Challenges and Priorities. The Defence Minister's New Year Address to the Oslo Military Society (Oslo, 7 January 2002). http://odin.dep.no/fd/engelsk/aktuelt/taler/statsraad_a/010011-090053/index-dok000-b-n-a.html.

Ministry of Defence. Society's Security and Preparedness. Fact Sheet (March 2002).

Ministry of Industry, Employment and Communication. An Information Society for All. Fact Sheet No. 2000.018 (March 2000).

Ministry of Justice and Police. Statement on Safety and Security of Society. Report No. 17 to the Storting (2000–2001).

Ministry of Trade and Industry. Information and Infrastructure Protection – a Norwegian View (no date).

Ministry of Trade and Industry. Society's vulnerability due to its ICT-dependence (Abridged version of the main report, Oslo, October 2000).

Nicander, Lars. „The Swedish Initiative on Critical Infrastructure Protection" ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead (Zurich, 8–10 November, 2001).

Nilsson, Jerry, Sven Erik Magnusson, Per-Olof Hallin and Bo Lenntorp. Vulnerability Analysis and Auditing of Municipalities (Lucram: Lund University).

Norges offentlige utredninger (2000:24) Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet. Statens forvaltningstjeneste Informasjonsforvaltning (Oslo, 2000).

SEMA guidelines for emergency planning for 2006 (summary). http://www.krisberedskapsmyndigheten.se/3404.epibrw.

SEMA guidelines for emergency planning for 2007 (summary). http://www.krisberedskapsmyndigheten.se/templates/Page____5730.aspx.

Svendsen, Per-Kare. Internet Rights Country Report – Norway (January 2000). http://www.apc.org/english/rights/europe/countries/norway.html.

Russia

Albats, Yevgenia. "Information Security Doctrine Redux". In: The Moscow Times (14 September 2000). http://www.themoscowtimes.com/stories/2000/09/14/007.html.

Baker and McKenzie. Legal Alert. Electronic Digital Signature Law. http://www.bakernet.com/ecommerce/Russia-E-Signature-Alert.doc.

Bennet, Gordon. FAPSI - The Federal Agency of Government Communications & Information. http://www.agentura.ru/english/dosie/brit/fapsi.

Doctrine of the Information Security of the Russian Federation. Approved by the President of the Russian Federation, Vladimir Putin (9 September 2000) No. Pr-1895. http://www.medialaw.ru/e_pages/laws/project/d2-4.htm.

Federal Target Program "Electoral Russia (years 2002 — 2010)". Approved by the Decree of the Government of the Russian Federation from January 28, 2002 No. 65. http://www.developmentgateway.org/download/182707/erussia_final_en_jr28-02.doc.

Filippov, Sergey. Policy for ICT Adoption in Moscow ("Electronic Moscow" Programme). http://www.telecities.nl/call_for_papers/paper_sergey_filippov_-_electronic_moscow.pdf.

GeoPowers. Sicherheitskonzept Russland: Wunschdenken? (7 February 2000). http://www.geopowers.com/Machte/Russland/russland.html.

Ignatyev, Mikhail B. "Analysis of the Threat of Cyberattacks to Major Transportation Control Systems in Russia." In: Terrorism: Reducing Vulnerabilities and Improving Responses - U.S.-Russian Workshop Proceedings (2004). http://www.nap.edu/openbook/0309089719/html/85.html#pagetop.

Kremer, Arkadiy. "Cyber Security in Russia". Presentation held at ITU-Cybersecurity Symposium, Florianopolis (Brazil, 4 October 2004). http://www.itu.int/ITU-T/worksem/cybersecurity/presentations/CsecS2-p2-kremer.ppt.

Leigh, Ian. Information Security Doctrine of the Russian Federation (no date). http://www.isn.ethz.ch/news/dossier/ssg/pubs/books/FluriSulakshin/05A_LEIGH.pdf.

Ministry of Information Technologies and Communications of the Russian Federation. Regulation on the RF Ministry for communications and informatization. http://english.minsvyaz.ru/site.shtml?id=17&page=1.

Naumov, Victor. Liability for computer crime in Russia (Computer Crime Research Center (online), 6 April 2004). http://www.crime-research.org/analytics/Liability_for_computer_crime_in_Russia.

Nikiforov, Ilya. Legal Protection of Software in Russia. International Considerations. http://freeweb.supereva.com/pdenicto/protectsw.htm?p.

Reuters. Russia, China Working on Cyber Warfare (21 June 2001). http://www.greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=005YM3.

Russian Federation. Law of the Russian Federation on Information, Informatisation and Information Protection (25 January 1995). http://www.datenschutz-berlin.de/gesetze/internat/fen.htm.

Russian Intelligence-Related Documents. National Information Policy and Practice. http://www.fas.org/irp/world/russia/docs/arf_p2.htm.

Russian Intelligence-Related Legal Documents. On the Russian Federation Security Council. http://www.fas.org/irp/world/russia/docs/edict_1024.htm.

Seminar E-Government in Russland (Universität Koblen-Landau, Institut für Wirtschafts- und Verwaltungsinformatik). http://www.uni-koblenz.de/~kgt/PM/SemB/Russland.ppt.

Soldatov, Andrei. FSB Reform: Changes Are Few and Far between. http://www.agentura.ru/english/press/about/jointprojects/mn/fsbreform.

Statute on the Federal Security Service of the Russian Federation and Structure of Federal Security Service Agencies. Approved by Presidential Edict No 960 of 11 (August 2003). http://www.fas.org/irp/world/russia/fsb/statute.html.

The National Academies Press. Terrorism: Reducing Vulnerabilities and Improving Responses: U.S - Russian Workshop Proceedings (2004). http://books.nap.edu/books/0309089719/html/index.html.

Thomas, Timothy L. Russian Views on Information Based Warfare. http://www.shaneland.co.uk/ewar/docs/dissertationsources/russiansource1.pdf.

Thomas, Timothy L. Information Security Thinking: A Comparison of U.S., Russian and Chinese Concepts (July 2001). http://fmso.leavenworth.army.mil/documents/infosecu.htm.

Singapore

Asia-Pacific Conference on Cybercrime and Information Security (Seoul, 11–13 November 2002). Country Report on Singapore. http://www.unescap.org/icstd/cybercrime%20meeting/Presentations/Session%203%20-%20country%20and%20org.%20reports/Singapore/Singapore%20written%20report.doc.

Costa, Valerie D. Singapore's Internet Policy. Workshop on Internet Governance at the National Level (Geneva, 19 July 2005). http://www.wgig.org/docs/Singapore%20Internet%20Policy%2019%20Jul%2005.ppt.

IDSS Commentaries (37/2004). Defending Singapore's Vital Infrastructure Against Terrorism. By Arabinda Acharya, Institute of Defence and Strategic Studies (Singapore, 2 September 2004). http://www.pvtr.org/pdf/IDSS372004.pdf.

Infocomm Development Authority of Singapore (IDA). Singapore Gears Up for Cyber Security: Three-year Infocomm Security Masterplan Unveiled (Singapore, 22 February 2005). http://www.ida.gov.sg/idaweb/marketing/infopage.jsp?infopagecategory=&infopageid=I3280&versionid=3.

Leong, Clement. Security Initiatives in the Computerisation of the Singapore Government. http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/13-Homeland-Security-Singapore_R2GVIV_0Z5RDZ-i34KpR.htm.

National Security Coordination Centre. The Fight Against Terror - Singapore's National Security Strategy (Singapore 2004). http://www.pmo.gov.sg/NSCS/FightAgainstTerror.pdf.

Sweden

Coherent strategy for the society's information assurance (Sammanhållen strategi för samhällets IT-säkerhet, rapport Statskontoret rapportserie (1998).

Security related to electronic identification (Säkerhet med elektronisk identifiering, rapport i Statskontorets rapportserie (1999).

SEMA document 0160/2003. Account of what measures that have been accomplished to take over the responsibilities from the working group on Information Operations (Redovisning av åtgärder för att överta arbetsuppgifter från Ag IO 0160/2003).

The Swedish Commission on Vulnerability and Security. Vulnerability and Security in a New Era — A Summary (SOU 2001:41, Stockholm, 2001).

The Swedish ICT Commission. Basic Protection in Computer Hardware and Software. The Observatory for Information Security (2001).

The Swedish ICT Commission. General Guide to a Future-Proof IT Infrastructure. Observatory for IT Infrastructure. Report 37/2001 (Stockholm, 2001).

Wallstrom, Peter. "Methods for Infrastructure Protection". MIS Training, InfowarCon '99 (London, 1999).

Weissglass, Gösta (ed.). "Planning a High-Resilience Society". Papers and Proceedings from the Lövånger Symposium, 18–20 August 1993 (Umeå, 1994).

Wik, Manuel W. „The Swedish Commission on Vulnerability and Security. Under Leadership of Special Investigator Åke Pettersson". ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead (Zurich, 8–10 November, 2001).

Switzerland

Bircher, Daniel. „Informationsinfrastruktur — Verletzliches Nervensystem unserer Gesellschaft". In: Neue Zürcher Zeitung, 7 July 1999.

Carrel, Laurent F. Bericht des Projektleiters über die Strategische Führungsausbildung (SFU) 97 (Bern, 1 July 1998).

Generalsekretariat VBS (ed.). Risikoprofil Schweiz. Umfassende Risikoanalyse Schweiz (Draft, Bern, August 1999).

Groupe de Réflexion. Für eine Informationsgesellschaft in der Schweiz. Zuhanden des Schweizerischen Bundesrates (Bern, June 1997).

Haefelfinger, Rolph L. "The Swiss Perspective on Critical Infrastructure". Presentation at the PfP Seminar on Critical Infrastructure Protection and Civil Emergency Planning — New Concepts for the 21st Century (Stockholm, 17–18 November 2003).

Informatikstrategieorgan Bund ISB. Einsatzkonzept Information Assurance Schweiz. Melde- und Analysestelle Informationssicherheit (MELANI), Sonderstab Information Assurance (SONIA). Schlussbericht vom 30. November 2001 (Zollikon, 2001).

Informatikstrategieorgan Bund ISB. Verletzliche Informationsgesellschaft. Herausforderung Informationssicherung (Bern, October 2002). http://www.isb.admin.ch/imperia/md/content/sicherheit/schutz-infrastruktur/information_assurance/pia_d.pdf.

InfoSurance/Wirtschaftliche Landesversorgung/Informatikstrategieorgan Bund. Sektorspezifische Risikoanalysen — Methodischer Leitfaden, 2002.

ISPS News (Infosociety.ch). Press Release: Gemeinsam die Cyber-Kriminalität bekämpfen. Bundesrat genehmigt Konvention des Europarats.

Koordinationsgruppe Informationsgesellschaft (KIG). Konzept "Information Assurance" (Bern, May 2000).

OFCOM. 5th Report of the Information Society Coordination Group (ISCG) to the Federal Council (June 2003).

Rytz, Ruedi and Jürg Römer. "MELANI – An Analysis Centre for the Protection of Critical Infrastructures in the Information Age". Workshop

on Critical Infrastructure Protection (CIP) (Frankfurt a. M., 29–30 September 2003).

Rytz, Ruedi. Sonderstab Information Assurance - ein paar Gedanken (Bern, 11 September 2001).

Schweizerische Bundeskanzlei. Information Assurance: Die Verletzlichkeit der schweizerischen Informationsgesellschaft (Bern, 19 May 1998).

Schweizerische Bundeskanzlei. INFORMO 2001: Strategische Führungsausbildung. Dokumentation für Teilnehmende und Medienschaffende (Bern, 2001).

Schweizerische Bundeskanzlei. Strategische Führungsübung 1997 — Kurzdokumentation über die SFU 97 (Bern, 1997).

Security through Cooperation - Report of the Federal Council to the Federal Assembly on the Security Policy of Switzerland (Bern, June 1999).

Sibilia, Ricardo. Informationskriegführung. Eine schweizerische Sicht (Institut für militärische Sicherheitstechnik (IMS), Nr. 97–6, Zurich, 1997).

Spillmann, Kurt R., Stefan Libiszewski and Andreas Wenger. „Die Rückwirkungen der Informationsrevolution auf die schweizerische Aussen- und Sicherheitspolitik". NFP 42 Synthesis, Nr. 11 (Bern, Schweizerischer Nationalfonds, 1999).

Strategy of the Federal Council for an Information Society in Switzerland (Bern, 18 February 1998).

Trappel, Josef. Informationsgesellschaft Schweiz — Bestandesaufnahme und Perspektiven. Europäisches Zentrum für Wirtschaftsforschung und Strategieberatung (Basel, 1997).

Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung (BinfV) vom 23. Februar 2000 (Bern, 2000). http://www.admin.ch/ch/d/sr/1/172.010.58.de.pdf.

Wigert, Isabelle. "Der Schutz kritischer Informationsinfrastrukturen in der Schweiz: Eine Analyse von Akteuren und Herausforderungen." In: Wenger, Andreas (Hg.). Bulletin 2005 zur schweizerischen Sicherheitspolitik (Zurich: Center for Security Studies 2005), pp. 97–121. http://www.css.ethz.ch/publications/bulletin.

United Kingdom

Monthly Report from the e-Minister and e-Envoy (3rd March 2003). http://archive.cabinetoffice.gov.uk/e-envoy/reports-pmreports-2003/$file/3march03.htm.

Parsons, T. J. "Protecting Critical Information Infrastructures. The co-ordination and development of Cross-sectoral research in the UK". Plenary Address at 'The Future of European Crisis Management (Uppsala, Sweden, March 2001).

Performance and Innovation Unit Report. e-commerce@its.best.uk (September 1999). http://www.strategy.gov.uk/downloads/su/ecomm/ec_body.pdf.

United States

Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. Information Assurance Workforce Improvement Program (DoD 8570.01-M, 19 December 2005). http://www.dtic.mil/whs/directives/corres/pdf/d85701_081104/d85701p.pdf.

Belcher, Tim and Elad Yoran. Internet Security Threat Report: Attack Trends for Q3 and Q4 2001 (Alexandria, January 2002).

Bendrath, Ralf. "Critical Infrastructure Protection in the United States". ETH-ÖCB-CRN Workshop on Critical Infrastructure Protection in Europe: Lessons Learned and Steps Ahead (Zurich, 8–10 November 2001).

Brown, Evelyn. "Energy Systems Expertise is Key to Critical Infrastructure Center." In: Logos (No. 17, vol. 2, Fall 1999).

Buehring, Bill. Natural Gas Security Issues Related to Electric Power Systems (28 November 2001). http://wpweb2k.gsia.cmu.edu/ceic/presentations/Buehring.pdf.

Bush, George W. Executive Order 13228. Establishing the Office of Homeland Security and the Homeland Security Council (Washington, 8 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13228.htm.

Bush, George W. Executive Order 13231. Critical Infrastructure Protection in the Information Age (Washington, 16 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

Clinton, William J. Defending America's Cyberspace: National Plan for Information Systems Protection. An Invitation to a Dialogue. Version 1.0 (Washington, 2000).

Clinton, William J. Executive Order 13010 on Critical Infrastructure Protection (Washington, 15 July 1996). http://www.fas.org/irp/offdocs/eo13010.htm.

Clinton, William J. Protecting America's Critical Infrastructures: Presidential Decision Directive 63 (Washington, 22 May 1998). http://www.fas.org/irp/offdocs/pdd-63.htm.

Clinton, William J. Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities (Washington, January 2001). http://www.fas.org/irp/offdocs/pdd/CIP_2001_CongRept.pdf.

Cyber Security — Full Committee Hearing on Cyber Security – How Can We Protect American Computer Networks From Attack? (Washington, 10 October 2001). http://www.house.gov/science/full/oct10/full_charter_101001.htm.

Dacey, Robert F. Critical Infrastructure Protection: NIPC Faces Significant Challenges in Developing Analysis, Warning, and Response Capabilities, before the Subcommittee on Technology, Terrorism, and Government Information, Senate Committee on the Judiciary. GAO-01-769T (Washington, 22 May 2001). http://www.iwar.org.uk/cip/resources/gao/d01769t.pdf.

Davis, John. Research and Development for Critical Infrastructure Protection (Washington, 5 September 1997).

Department of Homeland Security. Draft National Infrastructure Protection Plan (NIPP) Base Plan (2 November, 2005). http://www.fas.org/irp/agency/dhs/nipp110205.pdf.

Erica B. Russell. "International and Interagency Critical Infrastructure Protection Coordination". Presentation at the PfP Seminar on Critical Infra-

structure Protection and Civil Emergency Planning — New Concepts for the 21st Century (Stockholm, 17–18 November 2003).

Fisher, R., J. Peerenbaum. "Interdependencies: A DOE Perspective". 16th Annual Security Technology Symposium & Exhibition. Session IV: Infrastructure Interdependencies: The Long Pole in the Tent (Williamsburg, Virginia, 28 June 2000).

Fisher, R. J. Peerenbaum. "Lessons Learned from Industry Vulnerability Assessments and September 11th". US Department of Energy Assurance Conference (Arlington, 12–13 December 2001).

Government Accountability Office (GAO). Critical Infrastructure Protection. Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilites (GAO-05-434, May 2005). http://www.gao.gov/new.items/d05434.pdf.

Government Accountability Office (GAO). Information Security: Federal Agencies Need to Improve Controls over Wireless Networks (GAO-05-383, May 2005). http://www.gao.gov/new.items/d05383.pdf.

Government Accountability Office (GAO). Report to the Congressional Requesters, Information Security. Emerging Cybersecurity Issues Threaten Federal Information Systems (GAO-05-231, May 2005). http://www.gao.gov/new.items/d05231.pdf.

Government Electronics and Information Technology Association (GEIA). Information Assurance and Critical Infrastructure Protection: A Federal Perspective (2001).

Hearing before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism and Government Information. Improving Our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center (Washington, 25 July 2001). http://www.iwar.org.uk/cip/resources/nipc-oversight/hr072501st.htm.

House Science Committee: October 17, 2001 - Full Committee Hearing on Cyber Terrorism – A View From the Gilmore Commission (Washington, 17 October, 2001).

Kneso, Genevieve J. Federal Research and Development for Counter Terrorism: Organization, Funding and Options (CRS Congressional Research Service, Report for Congress November 2001).

League, Sarah Jane. "Critical Infrastructure Assurance Office: Protecting America's Infrastructures". InfowarCon '99 (London, 1999).

Little, Richard G., Paul B. Pattak, and Wayne A. Schroeder (eds.). Use of Underground Facilities to Protect Critical Infrastructures. Summary of a Workshop (National Academy Press: Washington, 1998).

Marwick, Peat. Vulnerability Assessment Framework 1.1. Prepared under contract for the Critical Infrastructure Assurance Office (October 1998).

Moteff, John D. and Paul Parfomak. Critical Infrastructure and Key Assets: Definition and Identification (CRS Congressional Research Service, Report for Congress Updated 1 October, 2004). http://www.fas.org/sgp/crs/RL32631.pdf.

Moteff, John D. Critical Infrastructures: Background, Policy, and Implementation (CRS (Congressional Research Service, Report for Congress, Updated 4 February, 2002). http://www.fas.org/irp/crs/RL30153.pdf.

Moteff, John D. Critical Infrastructures: Background and Early Implementation of PDD-63 (RL30153, Updated 12 September, 2000). http://www.cnie.org/nle/crsreports/science/st-46.cfm.

Office of the Undersecretary for Defense. Protecting the Homeland - Report of the Defense Science Board Task Force on Defensive Information Operations 2000 Summer Study (Executive Summary, Vol. I, March 2001).

Oversight Hearing on Information Technology. Essential Yet Vulnerable: How Prepared Are We for Attacks. Subcommittee on Governmental Efficiency, Financial Management and Intergovernmental Relations (26 September, 2001). http://www.iwar.org.uk/cip/resources/house-sep-26-01/witnesses.htm.

Power, Richard. "2001 CSI/FBI Computer Crime and Security Survey." In: Computer Security Issues & Trends (Vol. 1, 2001).

Proceedings of the Infrastructure Interdependencies Research and Development Workshop. Hosted by the Department of Energy, Office of Critical

Infrastructure Protection, and the White House, Office of Science and Technology Policy (Mc Lean, 12–13 June 2000).

Ryan, Julie. The Infrastructure of the Protection of the Critical Infrastructure (1998). http://www.iwar.org.uk/cip/resources/pdd63/pdd63-article.htm.

Sandia National Laboratories. Modeling of Interdependencies. Critical Infrastructure Surety (no date). http://www.sandia.gov/Surety/Facts/Modeling.htm.

Scalingi, Paula. Critical Infrastructure Protection Activities, Department of Energy (March 2001). http://www.naseo.org/events/outlook/2001/presentations/scalingi.pdf.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-30 (Washington: U.S. Government Printing Office, January 2002).

Stoneburner, Gary. Computer Security. Underlying Technical Models for Information Technology Security. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-33 (Washington: U.S. Government Printing Office, December 2001). http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf.

The Department of Homeland Security. Information Analysis and Infrastructure Protection (no date). http://www.whitehouse.gov/deptofhomeland/sect6.html.

The President's Commission on Critical Infrastructure Protection (PCCIP). Critical Foundations: Protecting America's Infrastructures (Washington, October 1997).

The White House. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Washington, February 2003). http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf.

The White House. The National Strategy to Secure Cyberspace (Washington, February 2003). http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

The White House. Homeland Security Presidential Directive/HSPD-7 (Washington, 17 December 2003). http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

United States General Accounting Office (GAO). Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities (GAO-01-323, 25 April 2001).

United States Government Accountability Office (GAO). Critical Infrastructure Protection and Improving Information Sharing with Infrastructure Sectors (GAO-04-780, July 2004). http://www.gao.gov/new.items/d04780.pdf.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT, 2001). http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf.

US Critical Infrastructure Assurance Office. Practices for Securing Critical Infrastructure Assets (Washington, January 2000). http://www.iwar.org.uk/cip/resources/prac.pdf.

US Senate Committee on Governmental Affairs. Hearing on: How Secure is Our Critical Infrastructure? (Washington, 12 September, 2001). http://www.iwar.org.uk/cip/resources/senate-sep-12-01.

US Subcommittee on Oversight and Investigations Hearing. Protecting America's Critical Infrastructures: How Secure Are Government Computer Systems? (Washington, 5 April 2001). http://energycommerce.house.gov/107/action/107-13.pdf.

White Paper on PDD-63. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (Washington, 22 May 1998). http://www.cybercrime.gov/white_pr.htm.

European Union (EU)

Commission of the European Communities. Critical Infrastructure Protection in the Fight against Terrorism (Brussels, 20 October 2004), COM (2004)702 final. http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf.

Commission of the European Communities. Green Paper on a European Programme for Critical Infrastructure Protection (Brussels, 17 November 2005), COM(2005) 576 final.

Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems. http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/esignatures_en.pdf.

Directive 2002/21/EC of the EU Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive). http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_108/l_10820020424en00330050.pdf.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications). http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector. http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf.

Esterle, Alain, Hanno Ranck and Burkard Schmitt (edited by Burkard Schmitt). Information security. A new challenge for the EU. Chaillot Paper no. 76 (Paris, March 2005). http://www.iss-eu.org/chaillot/chai76.pdf.

Europe's Information Society. Legislation in Force. http://europa.eu.int/information_society/policy/ecomm/info_centre/documentation/legislation/index_en.htm.

European Network and Information Security Agency (ENISA). Work Programme 2005: "Information Sharing is Protecting". (Brussels 25 February 2005). http://www.enisa.eu.int/doc/pdf/management_board/decisions/work_programme_2005.pdf.

European Network and Information Security Agency (ENISA). ENISA Inventory of CERT Activities in Europe (Version 1.0, December 2005). http://www.enisa.eu.int/doc/pdf/deliverables/enisa_cert.pdf.

European Network and Information Security Agency (ENISA). Who is Who Directory on Network and Information Security (Version 1.0, December 2005). http://www.enisa.eu.int/doc/pdf/deliverables/ENISA_Who-is-Who-Directory_v1.0.pdf.

European Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. http://europa.eu.int/scadplus/leg/en/lvb/l14012.htm.

European Union task force to study IT critical infrastructure. InfoSec News, 19 April 2005. http://www.attrition.org/pipermail/isn/2005-April/001454.html.

Official Journal of the European Union. Commission Decision of 22 April 2005 establishing the European Research Advisory Board (2005/516/EC).

Status of implementation of Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. http://www.europa.eu.int/comm/justice_home/fsj/privacy/law/implementation_en.htm.

Group of Eight (G8)

"Critical Information Infrastructure Protection Work in the G8". In: NISCC Quarterly (January 2005). http://www.niscc.gov.uk/niscc/docs/re-20050401-00470.pdf?lang=en.

Dependability Development Support Initiative (DDSI). Dependability Overview – International Organisations and Dependability-Related Activities (Version April 2002).

Deutsches Auswärtiges Amt. The G8 Lyon Group (December 2004). http://www.auswaertiges-amt.de/www/en/aussenpolitik/vn/lyon_group_html.

G8 Information Centre. G8 Conference and the Protection of Critical Infrastructures Paris (Paris, 24 –26 March, 2003). http://www.g7.utoronto.ca/summit/2003evian/press_statement_march24_2003.html.

G8 Information Centre. G8 Conference on Dialogue Between the Public Authorities and Private Sector on Security and Trust in Cyberspace: Final Press Release (Paris, 15 – 17 May, 2000). http://www.g8.utoronto.ca/crime/paris2000.htm.

G8 Information Centre. Okinawa Charter on Global Information Society (Okinawa, 22 July 2000). http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm.

Setola, Roberto. Comments on G8 initiatives about CIIP. http://www.eda.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/cybsec.ContentPar.0086.UpFile.tmp/xy_yymmdd_0123456789_l.pdf.

UK Home Office. Challenges Associated with Emerging Technologies For Law Enforcement: Wireless Local Area Networks (WLANs) (November, 2004). http://www.homeoffice.gov.uk/documents/G8-WLANBstPrcNov04.pdf?view=Binary.

UN General Assembly Resolution 58/199. Creation of a global culture of cybersecurity and the protection of critical information infrastructures (30 January 2004). http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.

United States Department of Justice. G8 Principles for Protecting Critical Information Infrastructures (May 2003). http://www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf.

United States Department of Justice. Meeting of G8 Justice and Home Affairs Ministers: Best Practices for Network Security, Incident Response and Reporting to Law Enforcement (Washington, 11 May, 2004). http://www.usdoj.gov/ag/events/g82004/G8_Best_Practices_Network_Security.pdf.

Organisation for Economic Co-operation and Development (OECD)

Dependability Development Support Initiative (DDSI). Dependability Overview – International Organisations and Dependability-Related Activities (Version April 2002).

Organisation for Economic Co-operation and Development (OECD). Culture of Security. http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase.

Organisation for Economic Co-operation and Development (OECD). Information Security and Privacy. http://www.oecd.org/topic/0,2686,en_2649_34255_1_1_1_1_37409,00.html.

Organisation for Economic Co-operation and Development (OECD). Information and Communications Policy. http://www.oecd.org/department/0,2688,en_2649_34223_1_1_1_1_1,00.html.

Organisation for Economic Co-operation and Development (OECD). OECD Governments Launch Drive to Improve Security of Online Networks (7 August 2002). http://www.oecd.org/documentprint/0,2744,en_2649_34255_1946997_1_1_1_37409,00.html.

Organisation for Economic Co-operation and Development (OECD). OECD Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security (2002). http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf.

Organisation for Economic Co-operation and Development (OECD)/Working Party on Information Security and Privacy. The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries (DSTI/ICCP/REG(2002)1FINAL, 16 December 2005). http://www.oecd.org/dataoecd/16/27/35884541.pdf.

United Nations (UN)

Dependability Development Support Initiative (DDSI). International Organisations and Dependability-related Activities (Version 31 May 2002). http://www.ddsi.org/Documents/CR/DDSI_International_organisations.pdf.

Gelbstein, Eduardo and Ahmad Kamal. Information Insecurity – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security (New York, 2002). https://unp.un.org/details.aspx?entry=E04291#.

International Telecommunication Union (ITU). ITU Initiatives related to cybersecurity. http://www.itu.int/osg/spu/cybersecurity/ituevents.html.

International Telecommunication Union (ITU). Chairman's Report Version 2. ITU WSIS Thematic Meeting on Cybersecurity. ITU Headquarters (Geneva, 28 June-1 July 2005). http://www.itu.int/osg/spu/cybersecurity/chairmansreport.pdf.

International Telecommunication Union (ITU) (10 June, 2005). WSIS Thematic Meeting on Cybersecurity: Harmonizing National Legal A Chairman's Report Version 2. ITU WSIS Thematic Meeting on Cybersecurity. ITU Headquarters (Geneva, 28 June-1 July 2005) pp. 19–20. http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf.

UN Information and Communication Technologies Task Force (21 April, 2004). Headquarters to the Host Seminar on Policy, Security Issues in Information Technologies on 23 April. http://www.unicttaskforce.org/perl/documents.pl?id=1352.

UN General Assembly Resolution 55/63 and 56/121 (23 January 2002). Combating the criminal misuse of information technologies.

UN General Assembly Resolution 57/239 (31 January 2003). Creation of a global culture of cybersecurity. http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf.

UN General Assembly Resolution 58/199 (30 January 2004). Creation of a global culture of cybersecurity and the protection of critical information infrastructures. http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.

World Summit on the Information Society (WSIS). Outcome Documents (Declaration of Principles, Action Plan, Tunis Commitment, and Tunis Agenda). http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160|2266|2267.

World Summit on the Information Society (WSIS). Tunis Agenda. http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

World Bank Group

The International Bank for Reconstruction and Development/The World Bank (infoDev). Information Technology Security Handbook (Washington 2003). http://www.infodev-security.net/handbook.

The World Bank. Electronic Security: Risk Mitigation in the Financial Transactions. Public Policy Issues (June 2002). http://www.digitaldefense.net/white_papers/Risk_Mitigation_in_Financial_Transactions_version_2.pdf.

The World Bank. Technology Risk Checklist (May 2004, Version 7.3). http://www.infragard.net/library/pdfs/technologyrisklist.pdf.

A3 Important Links

Australia

Attorney-General's Department
(http://www.ag.gov.au)

Australian Computer Emergency Response Team (AusCERT)
(http://www.auscert.org.au)

Australian Government: Department of Defence (http://www.dsd.gov.au)

Australian Government: Information Management Office
(http://www.agimo.gov.au)

Australian High Tech Crime Centre (AHTCC) (http://www.ahtcc.gov.au)

Australian Security Intelligence Organization (ASIO)
(http://www.asio.gov.au)

Defense Science and Technology Organization (DSTO)
(http://www.dsto.defence.gov.au)

Prime Minister of Australia (http://www.pm.gov.au)

Trusted Information Sharing Network for Critical Infrastructure Protection
(TISN) (http://www.cript.gov.au)

Austria

Austrian Citizen Card/Österreichische Bürgerkarte
(http://www.buergerkarte.at/index.html)

Austrian Data Protection Commission (http://www.dsk.gv.at/indexe.htm)

Chief Information Office Austria (http://www.cio.gv.at)

Computer Incident Response Co-ordination Austria (CIRCA)
(http://www.circa.at/index.html)

Electronic Signatures/Aufsichtsstelle für elektronische Signaturen
(http://www.signatur.rtr.at)

Federal Chancellery/Bundeskanzleramt (http://www.bka.gv.at)

Federal Ministry of Transport, Innovation and Technology/ Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) (http://www.bmvit.gv.at)

Ministery of Internal Affairs/Bundesministerium für Inneres (http://www.bmi.gv.at)

Zentrum für sichere Informationstechnologie Austria (A-SIT) (http://www.a-sit.at)

Canada

Canada's National Computer Emergency Response Team (http://www.cancert.ca)

Canadian National Research Council (NRC) (http://www.nrc.ca)

Canadian Security Intelligence Service: Integrated Threat Assessment Centre (http://www.csis-scrs.gc.ca/en/itac/itac.asp)

Communication Research Centre (CRC) (http://www.crc.ca)

Department of National Defense (http://www.dnd.ca)

Federal Association of Security Officials (http://www.faso-afrs.ca)

Government-on-Line (GoL) (http://www.gol-ged.gc.ca)

Institute for Information Technology (IIT) (http://iit-iti.nrc-cnrc.gc.ca)

Public Safety and Emergency Preparedness Canada (http://www.psepc.gc.ca)

Treasury Board Secretariat (http://www.tbs-sct.gc.ca)

Finland

CERT-FI (http://www.ficora.fi/ruotsi/tietoturva/certfi.htm)

eFinland (http://e.finland.fi)

Finnish Communications Regulatory Authority (FICORA) (http://www.ficora.fi)

Finnish Government (http://www.valtioneuvosto.fi/vn/liston/base.lsp?k=en)

Finnish Information Society Development Center (http://www.tieke.fi)

Ministry of Defence (http://www.defmin.fi)

National Emergency Supply Agency (NESA) (http://www.nesa.fi)

France

Agence pour le Développement de l'Administration Électronique (http://www.adae.gouv.fr/adele)

Club de la Sécurite des Systèmes d'Information Français (CLUSIF) (https://www.clusif.asso.fr/index.asp)

Computer Emergency Response Team (CERTA) (http://www.certa.ssi.gouv.fr)

Computer Emergency Response Team Industry, Services, and Trade (CERT-IST) (http://www.cert-ist.com)

Direction for Security of Information Systems (DCSSI) (http://www.ssi.gouv.fr/fr/dcssi/index.html)

Le Portail Société de l'Information Internet gouv.fr (http://www.internet.gouv.fr)

National Network of Telecommunications for Technology, Education, and Research (GIP RENATER) (http://www.renater.fr)

Security of Information Systems (SSI) (http://www.ssi.gouv.fr/fr/index.html)

Strategic Advisory Board on Information Technologies (CSTI) (http://www.csti.pm.gouv.fr)

Germany

Arbeitskreis Schutz von Infrastrukturen/ German Group on Infrastructure Protection (AKSIS) (http://www.aksis.de)

CERT-Bund (http://www.bsi.bund.de/certbund/index.htm)

DCERT (http://www.dcert.de)

Deutsche Telekom AG (http://www.telekom.de)

DFN-CERT (http://www.cert.dfn.de)

Federal Intelligence Service/Bundesnachrichtendienst (BND) (http://www.bundesnachrichtendienst.de)

Federal Law Enforcement Agency/BKAonline - Bundeskriminalamt (http://www.bka.de)

Federal Ministry of Economic and Technology/Bundesministerium für Wirtschaft und Technologie (http://www.bmwi.de)

Federal Ministry of Education and Research/Bundesministerium für Bildung und Forschung (BMBF) (http://www.bmbf.de)

Federal Ministry of Justice/Bundesministerium für Justiz (http://www.bmj.bund.de)

Federal Ministry of the Interior/Bundesministerium des Innern: Wissensmanagement (http://www.wmsbundonline.de)

Federal Network Agency (http://www.bundesnetzagentur.de)

Federal Office for Civil Protection and Disaster Response/Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (http://www.bbk.bund.de)

Federal Office for Information Security/Bundesamt für Sicherheit in der Informationstechnik (BSI) (http://www.bsi.de)

Federal Police/Bundespolizei (http://www.bundespolizei.de)

German Association for Information Technology, Telecommunications and New Media/Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) (http://www.bitkom.org)

German Association for IT Security/Deutsche Gesellschaft für IT-Sicherheit: IT-Sicherheit für den Mittelstand (Mcert) (http://www.mcert.de)

German Bundestag (http://www.bundestag.de)

German CERT-Verbund (http://www.cert-verbund.de)

German Emergency Preparedness Information System (deNIS) (http://www.denis.bund.de)

Government Disaster Relief Organisation/Technisches Hilfswerk (THW) (http://www.thw.de/english)

Guideline to the Information and Communication Services Acts/Informations- und Kommunikationsdienste-Gesetz (http://www.iid.de/iukdg)

Initiative D21 (http://www.initiatived21.de)

Initiative on the Information Society in Germany/Initiative Informationsgesellschaft Deutschland (http://www.iid.de)

Security in the Internet/Sicherheit im Internet (http://www.sicherheit-im-internet.de)

India

Department of Information Technology (DIT) (http://www.mit.gov.in)

Electronic Governance Division, Department of Information Technology (http://egov.mit.gov.in)

Indian Computer Emergency Response Team (CERT) (http://www.cert-in.org.in)

Ministry of Communications and Information Technology (http://www.moc.gov.in)

National Association of Software and Service Companies (NASSCOM) (http://www.nasscom.org)

National Informatics Centre (NIC), Department of Information Technology (DIT) (http://home.nic.in)

National Task Force on IT and Software Development (http://it-taskforce.nic.in)

Standardisation, Testing and Quality Certification (STQC) Directorate, Department of Information Technology (DIT) (http://www.stqc.nic.in)

Italy

Computer Emergency Response Team Italy (CERTIT) (http://security.dsi.unimi.it)

Department of Informatics and Communications at the University of Milan/Dipartimento di Informatica e Comunicazione (http://www.dico.unimi.it)

GARR-CERT (http://www.cert.garr.it)

Incident Response Italy (http://www.iritaly.org)

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM) (http://www.iscom.gov.it)

Minister for Innovation and Technologies (http://www.innovazione.gov.it/eng)

Ministry of Communication (http://www.comunicazioni.it/en)

National Centre for Informatics in the Public Administration (CNIPA) (http://www.cnipa.gov.it)

Organismo di Certificazione della Sicurezza Informatica (http://www.ocsi.gov.it)

State Police/Polizia di Stato (http://www.poliziadistato.it/pds/english)

Japan

@Police/National Police Agency's Commitment to Information Security (http://www.cyberpolice.go.jp/english)

Asia Pacific Computer Emergency Response Team (APCERT) (http://www.apcert.org)

Information and Communications Statistics Database (http://www.johotsusintokei.soumu.go.jp/english/index.html)

IT Security Office, Cabinet Secretariat (http://www.bits.go.jp/en)

Japan Computer Emergency Response Team Coordination Center (JPCERT CC) (http://www.jpcert.or.jp/english)

Japan Information Processing Development Corporation (JIPDEC) (http://www.jipdec.jp/eng)

Ministry of Economy, Trade and Industry (METI) (http://www.meti.go.jp/english)

Ministry of Economy, Trade and Industry (METI), Information Policy (http://www.meti.go.jp/english/policy/index_information_policy.html)

Ministry of Internal Affairs and Communications (MIC) (http://www.soumu.go.jp/english)

National Information Security Center (http://www.bits.go.jp/active/general/kijun01.html)

National Police Agency (NPA): Japan Countermeasure against Cybercrime Homepage (http://www.npa.go.jp/cyber/english/index.html)

Prime Minister of Japan and His Cabinet (http://www.kantei.go.jp/foreign/index-e.html)

Republic of Korea

Electronics and Telecommunications Research Institute (ETRI) (http://www.etri.re.kr/www_05/e_etri)

Korea Information Security Agency (KISA) (http://www.kisa.or.kr/index.jsp)

Korea Information Security Agency (KISA), Common Criteria Evaluation (http://www.kisa.or.kr/kisae/kisec/jsp/kisec_6010.jsp)

Korea Information Security Industry Association (KISIA) (http://www.kisia.or.kr/new)

Korea Informatization PromotionCommittee (http://www.ipc.go.kr/ipceng/index.jsp)

Korea Internet Security Center (http://www.certcc.or.kr/english/vision.htm)

Ministry of Science and Technology (MOST) (http://www.most.go.kr)

National Cyber Security Center (http://www.ncsc.go.kr/eng)

National Information Security Alliance (NISA) (http://www.nisa.or.kr/link_2.php)

National Security Research Institute (NSRI) (http://www.nsri.re.kr/kor/index.html)

Supreme Prosecutor's Office (http://www.icic.sppo.go.kr)

Malaysia

E-Secure Malaysia (http://www.esecuremalaysia.org.my)

Malaysia Communications and Multimedia Commission (MCMC) (http://www.cmc.gov.my)

Malaysian Administrative Modernization and Management Planning Unit (MAMPU) (http://www.mampu.gov.my)

Malaysian Computer Emergency Response Team (MyCERT) (http://www.mycert.org.my)

Ministry of Energy, Water and Communications (MEWC) (http://www.ktkm.gov.my)

Ministry of Science, Technology and Innovation (MOSTI) (http://www.mosti.gov.my/MostePortal/website/index.jsp)

National ICT Security & Emergency Response Centre (NISER) (http://www.niser.org.my)

The Netherlands

Government-wide Computer Emergency Response Team (GOVCERT.NL) (http://www.govcert.nl)

infodrome (http://www.infodrome.nl)

KWINT (http://www.kwint.org)

Ministry of Economic Affairs/Ministerie van Economische Zaken (http://www.minez.nl/index.jsp)

Ministry of Health, Welfare and Sport (http://www.minvws.nl/en)

Ministry of the Interior and Kingdom Relations (http://www.minbzk.nl)

Ministry of Transport, Public Works and Water Management/Ministerie van Verkeer en Waterstaat (http://www.minvenw.nl)

National Alerting Service/Waarschuwingsdienst (http://www.waarschuwingsdienst.nl)

National High Tech Crime Center (NHTC) (http://www.nhtcc.nl/index_en.html)

SURFnet Computer Security Incident Response Team (http://cert-nl.surfnet.nl/home-eng.html)

The General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) (https://www.aivd.nl/)

The Platform for Electronic Business in the Netherlands (ECP.nl) (http://www.ecp.nl/index.php)

TNO Web (http://www.tno.nl)

New Zealand

Australian Computer Emergency Response Team (AusCERT) (http://www.auscert.org.au)

Centre for Critical Infrastructure Protections (http://www.ccip.govt.nz)

Department of the Prime Minister and Cabinet (http://www.dpmc.govt.nz)

E-Secure-IT Alert and Early Warning Service (http://www.cologic.co.nz)

Government Communications Security Bureau (http://www.gcsb.govt.nz)

Government security policy and guidance website (http://www.security.govt.nz)

Ministry of Defence (http://www.defence.govt.nz)

New Zealand Computer Society (http://www.nzcs.org.nz)

Standards New Zealand (http://www.standards.co.nz)

State Services Commission (http://www.ssc.govt.nz/display/home.asp)

Norway

Center for Information Security (SIS) (http://www.norsis.no/indexe.php)

Directorate for Civil Protection and Emergency Planning/Direktoratet for Sivilt Beredskap (DSB) (http://www.dsb.no)

Ministry of Trade and Industry (http://odin.dep.no/nhd/engelsk)

National Telecommunications and Information Administration (http://www.ntia.doc.gov)

Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime/Okokrim (http://www.okokrim.no)

Norwegian National Security Authority/Nasjonal sikkerhetsmyndighet (http://www.nsm.stat.no/index.html)

The Norwegian Network for Research & Education - Computer Emergency Response Team (http://cert.uninett.no)

Russia

Computer Security Incident Response Team (CSIRT). (http://www.cert.ru/index_eng.html)

E-Russia (http://www.e-rus.ru)

Federal Security Service (FSB)(http://www.fsb.ru)

MediaLaw.ru (http://www.medialaw.ru/e-index.html)

Ministry of the Interior (http://eng.mvdrf.ru/)

Russian Association for Networks and Services (RANS) (http://www.rans.ru/eng/directions)

Russian Backbone Network (RBNet) (http://www.ripn.net:8082/rbnet/en/description.html)

Russian E-Development Partnership (http://russia-gateway.ru/en)

Russian Institute for Public Networks (http://www.ripn.net)

Russian Security Council (http://www.kremlin.ru/eng/articles/institut04.shtml)

State Technical Commission (http://www.globalsecurity.org/intell/world/russia/gtk.htm)

Singapore

Infocomm Development Authority of Singapore (IDA) (http://www.ida.gov.sg)

Information Technology Standards Committee (ITSC) (http://www.itsc.org.sg)

Ministry of Home Affairs (MHA) (http://www2.mha.gov.sg)

National Infocomm Competency Centre (NICC) (http://www.nicc.org.sg/index.aspx)

Singapore Computer Emergency Response Team (SingCERT) (http://www.singcert.org.sg)

Singapore Police Force (http://www.spf.gov.sg)

Sweden

Ministry of Defense/Försvars Departementet (http://forsvar.regeringen.se)

Swedish Alliance for Electronic Businesses (GEA) (http://www.gea.nu)

Swedish Armed Forces (http://www.mil.se/?lang=E)

Swedish Defense Material Administration (FMV) (http://www.fmv.se)

Swedish Defense Research Agency (FOI) (http://www.foi.se/english)

Swedish Emergency Management Agency (SEMA) (http://www.krisberedskapsmyndigheten.se)

Swedish IT Incident Centre (SITIC) (http://www.sitic.se)

Swedish National Defense College (http://www.fhs.mil.se)

Swedish National Defense Radio Establishment (FRA) (http://www.fra.se/english.shtml)

Swenskt Näringsliv: Confederation of Swedish Enterprise (http://www.svensktnaringsliv.se)

The National Board of Psychological Defence (http://www.psycdef.se/english)

Switzerland

Center for Security Studies, ETH Zurich (http://www.css.ethz.ch)

CLUSIS (Association Suisse de la Sécurité des Systèmes d'Information) (http://www.clusis.ch)

Comprehensive Risk Analysis and Management Network (CRN) (http://www.isn.ethz.ch/crn)

Federal Department of Defence, Civil Protection and Sports/Eidgenössisches Departement für Verteidigung, Bevölkerungschutz und Sport (DDPS) (http://www.vbs.admin.ch/internet/vbs/en/home.html)

Federal Office for Communication (OFCOM)/Bundesamt für Kommunikation (BAKOM) (http://www.bakom.ch/en/index.html)

Federal Office for National Economic Supply/Bundesamt für Wirtschaftliche Landesversorgung (BWL) (http://www.bwl.admin.ch)

Federal Office for Police (FOP)/Bundesamt für Polizei (http://internet.bap.admin.ch)

Federal Strategy Unit for Information Technology/Informatikstrategieorgan Bund (ISB) (http://internet.isb.admin.ch/internet/index.html?lang=de)

Information and Communication Management Research Group (http://www.ifi.unizh.ch/ikm/research.html)

Information Society Coordination Group (http://www.isps.ch)

InfoSurance Association (http://www.infosurance.ch)

International Relations and Security Network (ISN) (http://www.isn.ethz.ch)

National Emergency Operations Center/Nationale Alarmzentrale (NAZ) (http://www.naz.ch)

Reporting and Analysis Centre/Melde- und Analysestelle Informationssicherung (MELANI) (http://www.melani.admin.ch)

Strategic Leadership Training/Strategische Führungsausbildung (http://www.admin.ch/ch/d/bk/sfa/index.html)

Swiss Coordination Unit for Cybercrime Control (CYCO)/Koordinationsstelle Internet-Kriminalität (KOBIK) (http://www.cybercrime.admin.ch)

Swiss Education and Research Network (SWITCH) (http://www.switch.ch/about)

Swiss Federal Office of Information Technology and Telecommunication (FOITT)/Bundesamt für Informatik und Telekommunikation (BIT) (http://www.efd.admin.ch/e/dasefd/aemter/bit)

SWITCH-CERT Computer Emergency Response Team (http://www.switch.ch/cert)

Symposium on Privacy and Security (http://www.privacy-security.ch)

United Kingdom

British Computer Society (BCS) (http://www.bcs.org/bcs)

Cabinet Office (http://www.cabinet-office.gov.uk)

Communications-Electronics Security Group (http://www.gchq.gov.uk/about/cesg.html)

Department of Trade and Industry (http://www.dti.gov.uk)

Forum of Incident Response and Security Teams (FIRST) (http://www.first.org)

Get Safe Online (http://www.getsafeonline.org)

Home Office (http://www.homeoffice.gov.uk)

Internet Watch Foundation (IWF) (http://www.iwf.org.uk)

IT Security Awareness for Everyone (ITSafe) (http://www.itsafe.gov.uk)

MI5 The Security Service (http://www.mi5.gov.uk)

Ministry of Defense Computer Emergency Response Team (http://www.mod.uk/cert)

National Computing Centre (NCC) (http://www.ncc.co.uk/index.cfm)

National Infrastructure Security Co-ordination Centre (NISCC) (www.niscc.gov.uk)

Prime Minister's Strategy Unit (http://www.strategy.gov.uk)

UK Online (http://www.direct.gov.uk/Homepage/fs/en)

Unified Incident Reporting and Alert Scheme (UNIRAS) (http://www.uniras.gov.uk)

United States

Federal Bureau of Investigation (FBI) (http://www.fbi.gov)

Federation of American Scientists (http://www.fas.org)

Financial Services Information Sharing and Analysis Center (FS-ISAC) (http://www.fsisac.com)

Government Accountability Office (GAO) (http://www.gao.gov/index.html)

Information Society Website of the European Union (http://europa.eu.int/information_society/index_en.htm)

Information Technology - Information Sharing and Analysis Center (IT-ISAC) (https://www.it-isac.org)

InfraGard (http://www.infragard.net)

Institute for Information Infrastructure Protection (I3P) (http://www.thei3p.org)

Internet Security Alliance (http://www.isalliance.org)

National Coordinating Center for Telecommunications (http://www.ncs.gov/ncc)

National Cyber Security Partnership (NCSP) (http://www.cyberpartnership.org/init.html)

North American Electric Reliability Council (NERC) (http://www.nerc.com)

Office of Science and Technology Policy (http://www.ostp.gov)

OnGuard Online (http://onguardonline.gov/index.html)

Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE) (http://www.cert.org/octave)

Research Themes under the 7th Framework Programme, European Commission (http://europa.eu.int/comm/research/future/themes/index_en.cfm)

Security Research, European Commission (http://www.europa.eu.int/comm/enterprise/security/index_en.htm)

Sixth Framework Programme of the European Commission (http://europa.eu.int/comm/research/fp6/index_en.cfm?p=0)

Stay Safe Online (http://www.staysafeonline.info)

Surface Transportation Information Sharing and Analysis Center (ST-ISAC) (http://www.surfacetransportationisac.org)

United States Computer Emergency Readiness Team (http://www.us-cert.gov)

United States Department of Defense (http://www.defenselink.mil/nii/index.html)

White House (http://www.whitehouse.gov)

European Union (EU)

Center for Democracy and Technology (http://www.cdt.org)

Community Research & Development Information Service (CORDIS) (http://cordis.europa.eu.int/en/home.html)

Computer Emergency Response Team (CERT) Coordination Center (http://www.cert.org)

Critical Information Infrastructure Research Co-ordination Project (CI2RCO) (http://www.ci2rco.org/index.asp)

Department of Homeland Security (http://www.dhs.gov/dhspublic/)

eEurope Standards (http://www.e-europestandards.org)

European Commission Directorate-General's Joint Research Centre (JRC) (http://www.jrc.cec.eu.int)

European Commission, Data Protection, Legislative Documents (http://www.europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm)

European Network and Information Security Agency (ENISA) (http://www.enisa.eu.int)

European Telecommunications Standards Institute (http://www.etsi.org)

Group of Eight (G8)

G8 Information Centre (http://www.g8.utoronto.ca)

North Atlantic Treaty Organisation (NATO)

North Atlantic Treaty Organization (NATO) (http://www.nato.int)

Organisation for Economic Co-operation and Development (OECD)

Organisation for Economic Co-operation and Development (OECD) (http://www.oecd.org)

United Nations (UN)

International Telecommunication Union (ITU) (http://www.itu.int/home/index.html)

United Nations (http://www.un.org)

United Nations Information and Communication Technologies Task Force (http://www.unicttaskforce.org)

World Bank Group

Information for Development Program (infoDev) (http://www.infodev.org)

International Bank for Reconstruction and Development/The World Bank (infoDev), (http://www.infodev-security.net)

World Bank (http://www.worldbank.org)

World Bank Global Information and Communication Technologies (GICT) (http://info.worldbank.org/ict/index.cfm)

Miscellaneous

4Law (http://www.4law.co.il)

Cybercrime Law: A Global Survey of Cybercrime Legislation (http://www.cybercrimelaw.net)

Dependability Development Support Initiative (DDSI) (http://www.ddsi.org)

Global Business Dialogue on Electronic Commerce (http://www.gbde.org)

A4 List of Experts

Australia

Alex Webling, Attorney-General's Department, Australian government (2006)
Patrick Drake-Brockman, Attorney-General's Department, Australian government (2006)
Adam Cobb, Director Stratwise Strategic Intelligence (2004)
Ivan Timbs, National Office for the Information Economy (NOIE) (2002)

Austria

Thomas Pankratz, Austrian Federal Ministry of Defense, Bureau for Security Policy (2004 + 2006)
Otto Hellwig, Former Official of the Federal Chancellery (2004 + 2006)
Gerald Trost, Stabsstelle IKT-Strategie des Bundes, Federal Chancellery of the Republic (2004 + 2006)
Nieves Kautny, University of Vienna (2006)
Ralph Schöllhammer, University of Vienna (2006)

Canada

Claudia Zuccolo, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
Janet Bax, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
Phil Beahen, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
Robert Corley, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
Peter Hill, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
Andrew McAllister, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)

Craig Oldham, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
Julie Spallin, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
Suki Wong, Public Safety and Emergency Preparedness Canada (PSEPC) (2006)
Louise Forgues, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2004)
Shannon Hiegel, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2004)
Dan Lambert, Solicitor General (2004)
Paul Pagotto, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2004)
Jacques L. Grenier, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2002)
Colin Knight, Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) (2002)

Finland

Ilkka Kananen, National Emergency Supply Agency (NESA) (2004 + 2006)
Veli-Pekka Kuparinen, National Emergency Supply Agency (NESA) (2004 + 2006)
Hannu Sivonen, National Emergency Supply Agency (NESA) (2006)
Mika Purhonen, National Emergency Supply Agency (NESA) (2004)
Markku Haranne, Ministry of the Interior, Rescue Services Unit (2004)

France

Isabelle Valentini, Secretary-General for National Defense (SGDN) (2006)

Germany

Susanne Jantsch, Consultant (2002 + 2004 + 2006)

Thomas Beer, Industrieanlagen-Betriebsgesellschaft (IABG) (2004)
Dirk Reinermann, Federal Office for Information Security (BSI) (2004)
Stefan Ritter, Federal Office for Information Security (BSI) (2004)
Willi Stein †, Federal Office for Information Security (BSI), (2004)
Christine Schwarz-Hemmert, Industrieanlagen-Betriebsgesellschaft (IABG) (2002)
Ralf Bendrath, Political Scientist (2002)
Jörn Brömmelhörster, Consultant (2002)

India

Subimal Bhattacharjee, Argus Integrated Systems (2006)
Luthra & Luthra Law Offices (2006)

Italy

Roberto Setola, Working Group for Critical Information Infrastructure Protection (2004 + 2006)
Paolo Donzelli, Prime Minister's Office - Dept. for Innovation and Technologies (2006)
Tommaso Palumbo, Postal and Communication Police (2006)
Sandro Bologna, Italian National Agency for New Technologies, Energy and the Environment (ENEA) (2004)
Giovanna Dondossola, CESI (2004)

Japan

Mika Shimizu, Osaka School of International Public Policy (2006)
Japanese experts from the
Ministry of Internal Affairs and Communication (MIC) (2006)
Ministry of Foreign Affairs (MOFA) (2006)
National Police Agency (NPA) (2006)
Cabinet Secretariat (2006)
Ministry of Economy, Trade and Industry (METI) (2006)

Republic of Korea

Seok-Koo Yoon, Director National Cyber Security Center (NCSC) (2006)

Netherlands

Eric Luiijf, TNO Defense, Security and Safety (2002 + 2004 + 2006)
Ronald de Bruin, KWINT, ECP.nl (2002 + 2004)

New Zealand

Mike Harmon, Centre for Critical Infrastructure Protection (CCIP) (2004 + 2006)
Richard Byfield, Centre for Critical Infrastructure Protection (CCIP) (2006)

Norway

Stein Henriksen, Directorate for Civil Protection and Emergency Planning (DSB) (2002 + 2004 + 2006)
Laila Berge, Ministry of Justice and the Police (2006)
Dagfinn Buset, Ministry of Justice and the Police (2006)
Roger Steen, Directorate for Civil Protection and Emergency Planning (DSB) (2002 + 2004)
Kjetil Sørli, Directorate for Civil Protection and Emergency Planning (DSB) (2004)
Cort Archer Dreyer, Ministry of Trade and Industry (2002)
Havard Fridheim, Norwegian Defence Research Establishment (FFI) (2002)
Arthur Gjengstö, Secretary to the Norwegian Commission on the Vulnerability of Society (2002)

Russia

Anatoly Streltsov, professor at the Institute of Information Security, Lomonosov Moscow State University (2006)

Martin Wählisch, Humboldt University Berlin (2006)

Singapore

Experts from the Ministry of Home Affairs (MHA) (2006)

Sweden

Linda Englund, Swedish Emergency Management Agency (SEMA) (2006)
Henrik Christiansson, Swedish Defence Research Agency (FOI) (2004)
Georg Fischer, Swedish Defence Research Agency (FOI) (2004)
Jan Lundberg, Swedish Emergency Management Agency (SEMA) (2002 + 2004 + 2006)
Lars Nicander, Swedish National Defence College (2002 + 2004)
Sara Siri, Swedish Emergency Management Agency (SEMA) (2004)
Peter Stern, Swedish Emergency Management Agency (SEMA) (2002)
Peter Wallström, Cell Network (2002)
Peter Westrin, FOI, Swedish Defence Research Agency (2002)
Manuel W. Wik, Swedish National Defence College (2002)

Switzerland

Ruedi Rytz, Federal Strategy Unit for Information Technology (ISB) (2002 + 2004 + 2006)
Michel Dufour, Dufour Consulting (2002 + 2004 + 2006)
Anton Lagger, Federal Office for National Economic Supply (2004 + 2006)
Marc Henauer, Federal Office of Police/DAP (2004 + 2006)
Gérald Vernez, General Staff of the Swiss Armed Forces (2006)
Riccardo Sibilia, armasuisse (2006)
Oliver Vaterlaus, AWK Group (2006)
André Schmid, InfoSurance Foundation (2004)
Kurt Haering, Director Foundation InfoSurance (2002)
Ueli Haudenschild, Federal Office for National Economic Supply (2002)
Thomas Köppel, Former Official of the Federal Office of Police (2002)

United Kingdom

John Neil Park, National Infrastructure Security Coordination Centre (NISCC) (2004 + 2006)
Ted Barry, National Infrastructure Security Coordination Centre (NISCC) (2004)
Stephen Cummings, National Infrastructure Security Coordination Centre (NISCC) (2004)

United States

Scott C. Algeier, Executive Director IT-ISAC (2002 + 2006)
Erica B. Russel, Deputy Coordinator for International Critical Infrastructure Protection Policy, Department of State (2006)
John A. McCarthy, Critical Infrastructure Protection Project, George Mason University School of Law (2004)
Emily Frye, Critical Infrastructure Protection Project, George Mason University School of Law (2004)

European Union (EU)

Marcelo Masera, European Commission, Joint Research Centre (2006)
Ronald De Bruin, European Network and Information Security Agency (ENISA) (2006)
Martin Wählisch, Humboldt University Berlin (2006)

Group of Eight (G8)

Harry Hoverd, Home Office, United Kingdom (2006)
North Atlantic Treaty Organization (NATO)
Evert G. J. Somer, NATO Headquarters (2006)
Silla A. Jonsdottier, NATO Headquarters (2004)

Organization for Economic Cooperation and Development (OECD)

Peter Lübkert, Organization for Economic Cooperation and Development (OECD) (2006)

Anne Carblanc, Organization for Economic Cooperation and Development (OECD) (2006)
Laurent Bernat, Organization for Economic Cooperation and Development (OECD) (2006)

United Nations (UN)

Robert Shaw, International Telecommunication Union (ITU) (2006)
Christine Sund, International Telecommunication Union (ITU) (2006)

The Center for Security Studies at ETH Zurich (Swiss Federal Institute of Technology) was founded in 1986 and specializes in the fields of international relations and security policy. The Center coordinates and develops the Comprehensive Risk Analysis and Management Network (CRN), a Swiss-Swedish initiative for open dialog on risks and vulnerabilities that is aimed at enhancing knowledge of the causes, interactions, probabilities, and costs of risks in modern societies.

The International Critical Information Infrastructure Protection (CIIP) Handbook is a joint effort within the CRN partner network, which currently includes: The Swedish Emergency Management Agency (SEMA), Sweden; the Directorate for Civil Protection and Emergency Planning (DSB), Norway; the Federal Office for National Economic Supply (NES), Federal Department of Economic Affairs, Switzerland; and the Swiss Federal Department of Defense, Civil Protection, and Sports (DDPS), Switzerland.

The CIIP Handbook focuses on national governmental efforts to protect critical information infrastructure and provides an overview of CII protection practices in a range of countries and international organizations (Vol. I). Vol. II offers more in-depth analysis of key issues related to CIIP.