International Organizations

The threats to CIP/CIIP do not respect functional or geographic boundaries, and 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-operation effort: strong international partnerships between governments and critical infrastructure owners and operators are becoming essential. 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.

This section gives an overview of CIIP efforts of the following international organizations: The *European Union* (EU), the *G8 Group*, the *North Atlantic Treaty Organization* (NATO), the *Organization for Economic Cooperation and Development* (OECD), and the *United Nations* (UN).

European Union (EU)

The EU is a key player at the international level concerning CIIP. CIIP, the Information Society, and Information Security are increasingly recognized as key issues. The EU is supporting these issues and investigating them by

- Considering its various aspects and impacts on citizenship, education, business, health, and communications;
- Supporting relevant programs and initiatives, such as the eEurope Action Plan, Information Society Technologies Research, eContent, eSafety, the Internet Action Plan, etc.[1]

The following sections give a short overview of important steps taken by the EU in the past.

"eEurope 2002 – An Information Society for all"

The program "*eEurope 2002 – An Information Society for all*" was launched by the EU on 8 December 1999. It is a key initiative within the EU's strategy for modernizing the European economy.[2] The EU has identified a tremendous economic and social potential offered by new information and communication technologies. The "eEurope 2002 action plan" was launched to ensure that everyone in Europe is able to benefit from the new technological develop-

[1] http://europa.eu.int/information_society/index_en.htm.

[2] http://www.etsi.org/eeurope/home.htm.

ments. The plan outlines eleven main action lines for the future (including e-Security).[3]

As the information society becomes more and more important to business and society, the EU regards ensuring the security of CI/CII as an important task. To this end, the EU argues that the Internet must be available to everyone at all times without time interruptions. Furthermore, the Internet must be protected against hacker and virus attacks. The EU believes that the full development of the information society cannot take place until security issues are addressed. Information security, which includes CIIP, has become a key component of the EU's vision for the so-called "*Next Generation Internet*". Hence, it is included among the policy priorities for "*eEurope 2005*", which are: modern online services such as e-Government, e-Learning, online Health services, a dynamic e-Business environment, widespread availability of broadband access at competitive prices, and finally, a *secure information infrastructure.*[4]

"eEurope 2005: An Information Society for all"

The action plan "*eEurope 2005: An Information Society for all*" was adopted in June 2002. It is an extension of the successful "*eEurope 2002*" initiative.[5] With the "*eEurope 2005*" initiative, the EU clearly recognizes information security to be more than a purely technological challenge. The EU states that information security is mainly dependent on human behavior, on the knowledge of threats, and on the management of these threats. Hence, the social and political aspect of information security is stressed. Since information security embraces a number of policy fields such as privacy, civil rights, law enforcement, international trade, and defense, the EU promotes a "holistic approach" concerning CIIP.[6] This means that an effective CIIP approach depends on the cooperation of all actors involved (public, private, individual) and on a multi-dimensional approach to establishing protective measures (including technical aspects, social and political aspects, and legal aspects.)

Implementing Information Security in Europe

In order to fulfill the goals of the action plans, the EU has initiated and supports different implementation activities (publications, setting of standards). One of these activities was the establishment of a special *EU Forum on*

[3] http://www.e-europestandards.org.

[4] http://europa.eu.int/information_society/eeurope/2005/index_en.htm.

[5] http://www.e-europestandards.org.

[6] http://europa.eu.int/information_society/eeurope/2005/all_about/security/print_en.htm.

Cybercrime. The Forum aims to raise awareness, promote best practices for security within the EU, identify counter-crime tools and procedures to combat computer-related crime, and to develop early warning and crisis management systems.[7]

In June 2001, the *European Commission* issued a communication entitled "*Network and Information Security: Proposal for a European Policy Approach*", including recommendations directed toward the *European Standardization Bodies* for the further development of their activities.[8]

A joint group of the *European Committee for Standardization* (CEN) and the *European Telecommunications Standards Institute* (ETSI) was set up in October 2001 and issued a draft report of network and information security recommendations, which were finalized in July 2003.[9]

European Network and Information Security Agency (ENISA)

On 11 February 2003, the *European Commission* presented a proposal for "*Establishing the European Network and Information Security Agency*" (ENISA). With the decision on 5 June 2003 to set up ENISA as a legal entity, the EU reinforced its efforts to enhance European coordination on information security. The agency has advisory and coordinating functions concerning data-gathering and data analysis on information security. Furthermore, the agency serves as a centre of expertise and excellence for the EU member states and EU institutions. The agency helps to establish broader cooperation between the key players and to ensure the interoperability of networks and information systems by promoting security standards.[10] The ENISA agency will become operational on 1 January 2004.[11] This will be a major step towards improving CIIP at the international level.

The Sixth Framework Program FP6 IST

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 knowledge society as agreed at the Lisbon Council of 2000, the Stockholm Council of 2001, the Seville Council of 2002, and reflected in the eEurope Action Plan. The IST component within

[7] http://cybercrime-forum.jrc.it/default.

[8] http://www.etsi.org/frameset/home.htm?/public-interest/Network_Information_Security.htm.

[9] Ibid.

[10] http://europa.eu.int/abc/doc/off/bull/en/200301/p103146.htm.

[11] http://www.terena.nl/tech/task-forces/tf-csirt/meeting9/vietsch-nisa.pdf and http://europa.eu.int/information_society/eeurope/2002/news_library/documents/nisa_en.pdf.

FP6 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. Among the strategic objectives of IST FP6 are: "Towards a global dependability and security framework", "Semantic-based knowledge systems", "Networked business and government", "eSafety for road and air transport", "eHealth", "Cognitive systems", "Embedded systems", "Improving risk management", and "eInclusion". As in FP5, the focus of the 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.

Group of Eight (G8)

Since 1995, the G8 has become more and more involved in issues relating to cybercrime, 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 catalogue of 40 operative recommendations. These recommendations were approved at the G8 summit in Lyon in 1996. The so-called *Lyon Group* was the first international political forum to fully recognize the significance of high-tech crime. The work of the Lyon Group has an impact beyond the G8 member states and their efforts concerning CIIP. One of the main tasks of the Lyon Group is to establish best-practice guides.[12]

A next 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*".[13] 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 cybercrime.[14]

[12] http://www.auswaertiges-amt.de/www/en/aussenpolitik/vn/lyon_group_html.

[13] http://www.g8.utoronto.ca/crime/paris2000.htm.

[14] Ibid.

Okinawa Charter on Global Information Society

The *Okinawa Charter on Global Information Society* was published in July 2000.[15] The Charter states that ICT is one of the most potent forces shaping the 21st century, enabling many communities to address social and economic challenges with greater efficiency and imagination.[16] 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. The G8 is determined to continue to engage industry and other stakeholders to protect critical information infrastructures.[17]

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.[18] The eleven clearly defined CIIP Principles were adopted on 5 May 2003 by the *G8 Justice and Interior Ministers*. They cover the following topics:

- The establishment of warning networks;
- Raising awareness about CIIP and their interdependencies;
- Promoting partnerships;
- Maintaining crisis communication networks;
- Facilitating the tracing of attacks;
- Training and exercising;
- Having appropriate laws and trained personnel;
- International co-operation;
- Promoting appropriate research.[19]

With the adoption of these principles, the G8 member states suggested that the emergence of a new "security culture" should encourage them to strengthen

[15] http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm.

[16] DDSI, Dependability Overview – *International Organisations and Dependability-Related Activities* (2002), p. 36.

[17] Ibid., p. 4.

[18] www.g7.utoronto.ca/summit/2003evian/press_statement_march24_2003.html.

[19] "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.

international co-operation, 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 main lines of actions, etc.[20] The eleven principles are intended to guide national responses to CIIP. However, to this end it is crucial that the principles be communicated to all concerned parties.

*North Atlantic Treaty Organization (NATO)**

The *Ministerial Guidance for NATO Civil Emergency Planning* (CEP) for 2003–2004 includes several references to critical infrastructure protection. The *Senior Civil Emergency Planning Committee* (SCEPC) has stated that it sees a need for exploratory and definitional work on the problems that may result from attacks on critical infrastructures.[21] Moreover, the SCEPC has tasked the *Planning Boards and Committees* (PB&Cs) with exploring the general aspects of critical infrastructure, as well as the social consequences of the non-availability of critical infrastructure, including transportation assets.[22]

Civil Communication Planning Committee (CCPC)

The *Civil Communication Planning Committee* (CCPC) is responsible for reviewing existing and planned electronic public and non-public communications infrastructures, services, associated facilities, postal services, and any related services with a view to determining their suitability 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';[23]
- 'CEP consequences of disruption of critical postal infrastructure';[24]

[20] "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.

[*] This chapter was written by Silla Jonsdottir, NATO Headquarters, Brussels.

[21] EAPC(SCEPC)N(2002)51, §12.6.

[22] EAPC(SCEPC)N(2002)51, §13.8.

[23] EAPC(CCPC)D(2002)8.

[24] EAPC(CCPC)D(2003)2.

- 'New risks and threats to civil telecommunications';[25]
- 'CEP requirements for coordinated national telecommunications regulatory measures';
- 'New risks and threats to the postal services'.[26]

In addition, the CCPC has contributed to the *North Atlantic Council's Action Plan on Cyber Defense*. Several other studies are underway, 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 and opportunities for NATO CEP in information society developments'.

Civil Protection Committee (CPC)

In 2001, the *Civil Protection Committee* (CPC) set up an *Ad Hoc Group* (AHG) to work on issues related to CIP. One of the first tasks of the AHG was to develop and circulate to the CPC a critical infrastructure mapping survey, which invited nations to indicate how they were structurally organized to deal with critical infrastructure protection, and their state of readiness in terms of planning and infrastructure mapping.[27] A report on the analysis of the mapping survey was endorsed by the CPC in October 2002 and forwarded to the SCEPC.[28] Subsequently, the CPC developed and approved a working definition for critical infrastructure, which was endorsed by the SCEPC on 4 November 2002.[29]

On 10 September 2003, the CPC approved a paper developed by the AHG that attempts to explain the CIP concept and its link with CEP.[30] The *Concept Paper* also proposes a way forward for work to be carried out by the CPC in this field. Attached to the Concept Paper is a road map detailing immediate, mid-term, and long-term actions. Also attached is a scenario that attempts to further explain the concept, and a glossary of frequently-used CIP terms. On 6 November 2003 the SCEPC endorsed the Concept Paper prepared by the CPC AHG.

[25] EAPC(CCPC)WP(2002)1, REV1.
[26] EAPC(CCPC)D(2003)1.
[27] EAPC(CPC)N(2002)6.
[28] EAPC(CPC)D(2002)4.
[29] EAPC(SCEPC)D(2002)14, REV1.
[30] EAPC(CPC)WP(2003)3.

Industrial Planning Committee (IPC)

The 2003 *Industrial Planning Committee* (IPC) Seminar was held in Slovakia on 8–9 September 2003 and 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 Slovakian 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" and "Protecting Critical Infrastructure during Disasters". The results of the subsequent group discussions will be summarized in a report soon to be published.

After this seminar and based on a questionnaire circulated in April 2003[31] and replies to it,[32] the IPC agreed at its meeting in September 2003 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)

In its work program, the *Food and Agriculture Planning Committee* (FAPC) looks at how CIP impacts on food, agriculture, and water production. In particular, the FAC looks at threats, risks, and vulnerabilities affecting the water sector. The FAPC is considering setting up a multi-disciplinary training seminar in 2005, 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, Telecommunications, and Energy Committees will be approached to encourage cross-discipline co-operation in planning and response.

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

[31] EAPC(IPC)N(2003)6.

[32] EAPC(IPC)WP(2003)2.

effective. These will soon be released in a report. 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 all 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.[33] 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. The report was discussed during the PBIST meeting on 17 November 2003.

Planning Board for Ocean Shipping (PBOS)

At the behest of the 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. An updated progress report, which was endorsed by the PBOS on 24 September 2003, will be submitted to the SCEPC in autumn of 2004.

Coordination

The 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 underway and/or planned within their respective areas of interest, in addition to fostering closer cooperation and coordination.

[33] EAPC(PBIST)D(2003)8.

Organization for Economic Cooperation and Development (OECD)

The *Organization for Economic Cooperation and Development* (OECD) is becoming more and more involved in the issue of CIIP. The OECD is committed to the fight against cybercrime 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.[34] There is a consensus among the member states 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 policymaking in these areas to help build trust online.[35] In addition, the *Committee for Information, Computer and Communications Policy* (ICCP) analyses the broad policy framework underlying the e-Economy, information infrastructures, and the information society.[36]

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 better counter cyberterrorism, 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*"[37]. These guidelines are designed to develop a "culture of security" among the government, businesses, and users with respect to the rapid worldwide expansion of network communication systems.

The guidelines are not binding. However, they are the result of a consensus between OECD governments and of discussions involving representatives of the information technology industry, business users, and civil society.[38] The OECD invites governments in other countries to adopt a similar approach to CIIP. Furthermore, the private sector representatives are asked to im-

[34] DDSI, Dependability Overview – *International Organisations and Dependability-Related Activities* (2002), p. 67.

[35] http://www.oecd.org/topic/0,2686,en_2649_34255_1_1_1_1_37409,00.html.

[36] http://www.oecd.org/department/0,2688,en_2649_34223_1_1_1_1_1,00.html.

[37] http://www.oecd.org/documentprint/0,2744,en_2649_33703_15582250_1_1_1_37409,00.html.

[38] http://www.oecd.org/documentprint/0,2744,en_2649_34255_1946997_1_1_1_37409,00.html.

prove security aspects 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.

In December 2003, the OECD has launched a *"Culture of Security" Web site* as part of the 30-member country Organizations' initiative to promote a global culture of security. This site primarily provides member and non-member governments with an international information-exchange tool on initiatives to implement the *OECD Guidelines* and serves as a portal to relevant Web sites as a first step towards creating a global culture of security.[39]

OECD Global Forums

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 security of information systems and networks, as well as the need for the OECD to implement the *OECD Security Guidelines* (see above). Furthermore, the importance of the preparation for the *World Summit on the Information Society* (WSIS) in December 2003 in Geneva (Switzerland) was also stressed. 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.

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.[40]

[39] http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase

[40] http://www.oecd.org/document/14/0,2340,en_2649_34255_8165070_1_1_1_37409,00.html.

United Nations (UN)

Issues related to CIIP have been discussed by different *United Nations* (UN) bodies since the end of the 1980s. However, formal CIIP efforts are a more recent phenomenon. Several steps have since been undertaken towards better work coordination. Among these are initiatives taken by UN institutes, UN resolutions, and the establishment of *UN Task Forces* with a focus on CIIP.

UN Institute for Disarmament Research

An important step was the organization of a workshop in July 1999 by the *UN Institute for Disarmament Research* 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 Revolutions in Military Affairs (RMA) and the proliferation of offensive tools for attacking information systems and networks were discussed in Geneva. There was a consensus among the participants that the vulnerability of national and international information infrastructures to cyberattacks was increasing, and that international co-operation 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.[41] Hence, it is crucial to achieve cooperation between public and private actors as well as between nations.

UN Resolutions about ICT

In December 2000, the 55th *UN General Assembly* issued Resolution 55/63 on "*Combating the criminal misuse of information technologies*".[42] This was a next important step in the efforts of the UN concerning CIIP. This resolution emphasizes 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 co-operation among countries and between the public and private sectors was stressed once again. The resolution also mentions the *Cyber Crime Convention* of the Council of Europe and the work done by the G8 as crucial milestones in the international field.[43]

[41] 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.

[42] UN General Assembly Resolution 55/63 (22 January 2001). http://ods-dds-ny.un.org/doc/UNDOC/GEN/N00/563/17/PDF/N0056317.pdf?OpenElement.

[43] Ibid.

The UN Information & Communications Technologies 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.[44] 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*".[45] This publication depicts the problem of information insecurity in general, provides possible solutions for prevention and response to security incidents (including standards and best practices).[46]

UN Resolution to Improve Cybersecurity

The US intends to propose a resolution at the *UN General Assembly* to highlight key elements needed for an effective cybersecurity environment. The US is convinced that, no matter what steps individual nations take to safeguard their own CII, a global approach is required for CIIP. Therefore, the US intends to encourage other nations to join in its efforts to protect CII. With this resolution, the US seeks to encourage as many other nations as possible to establish own national CIIP programs with the help of the governments, the public sector, and the public.[47]

It is hoped that this resolution will strengthen public-private partnerships, promote international cooperation in CIIP, and improve future efforts for national and international information-sharing and incident-reporting.

[44] http://www.unicttaskforce.org/about/principal.asp.

[45] Gelbstein, Eduardo and Ahmad Kamal. *Information Insecurity – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security* (New York, 2002). http://www.unicttaskforce.org/community/documents/764021661_unicttf_infosec.pdf.

[46] Ibid.

[47] http://www.state.gov/p/io/rls/fs/2003/24184.htm.

Center for Security Studies, ETH Zurich
Volume 2, Zürich 2004.

The International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

edited by
Andreas Wenger and Jan Metzger